

MEGATREND REVIJA

MEGATREND REVIEW

2 | 2025

MEGATREND REVIJA MEGATREND REVIEW

2/2025



Megatrend univerzitet, Beograd
Megatrend University, Belgrade

MEGATREND REVIJA • MEGATREND REVIEW

№ 2/2025

Izdavački savet / Publishing Council:

Predsednik izdavačnog saveta / President of the Publishing Council:

Professor Mića JOVANOVIĆ, PhD

Članovi iz inostranstva / International Members:

Professor Jean-Jacques CHANARON, PhD, Grenoble Ecole de Management, France Academician

Professor Vlado KAMBOVSKI, Macedonian Academy of Sciences and Arts, Skopje, North Macedonia

Professor Žarko LAZAREVIĆ, PhD, Institute for Contemporary History, Ljubljana, Slovenia

Professor Norbert PAP, PhD, University of Pécs, Hungary

Professor Sung Jo PARK, PhD, Free University, Berlin, Germany

Professor Budimir STAKIĆ, emeritus Slobomir P Univerzitet, Republika Srpska

Professor Srdjan LALIĆ, Ekonomski fakultet Brčko, Univerzitet Istočno Sarajevo,

Professor Maria POPOVIĆ, Univerzitet Adriatik, Crna Gora

Professor Jovica VASILJEVIĆ, Internacionalni univerzitet Brčko, BiH

Članovi iz Srbije / Members from Serbia:

Professor Miljojko BAZIĆ, PhD – Megatrend University, Belgrade

Professor Dragan NIKODIJEVIĆ, PhD – Megatrend University, Belgrade

Professor Milivoje PAVLOVIĆ, PhD – Megatrend University, Belgrade

Professor Jelena LUTOVAC, Megatrend Univerzitet, Srbija,

Professor Milan STAMATOVIĆ, PhD – Metropolitan University, Belgrade

Professor Nenad KAPOR, Megatrend University, Belgrade

Professor Miloš LUTOVAC, Beogradska akademija poslovnih i umetničkih strukovnih studija, Srbija

Associate Professor Milinko VELIČKOVIĆ, PhD, Megatrend University

Marijana ZIMONJIĆ, PhD, Megatrend University, Belgrade

Izdaje / Published by:

Megatrend univerzitet, Beograd / Megatrend University, Belgrade

Štampa / Printed by:

Tercija DOO, Bor

ISSN 1820-3159

UDK / UDC 33

Svi članci su recenzirani od strane dva recenzenta.

All papers have been reviewed by two reviewers.

Adresa redakcije / Editorial Address:

Megatrend revija / Megatrend Review

Bulevar maršala Tolbuhina 8

11070 Novi Beograd, Srbija

Tel.: (381 11) 220 31 50

Fax: (381 11) 220 30 47

E-mail: megatrendrevija@megatrend.edu.rs

<http://megatrendreview.megatrend.edu.rs>

Redakcija / Editorial Board:

Glavni urednik / Editor-in-chief:

Professor Vesna BALTEZAREVIĆ, PhD

Pomoćnik glavnog urednika/ Assitant to the Editor in Chief:

Mirjana TOPIC

Članovi iz inostranstva / International Members:

Professor Zijad BEĆIROVIĆ, IFIMES, Ljubljana, Slovenia

Professor Vladimir DAVIDOV, PhD – Institute for Latin America, Russian Academy of Sciences, Moscow, Russia

Dr. Christophe de JAEGER, Institute de Jaeger, France

Researcher Yury V. KULINTSEV, PhD – North-East Asian Strategic Issues and SCO Center, Institute of Far Eastern Studies, Russian Academy of Sciences, Moscow, Russia

Professor Jana LENGHARDTOVÁ, PhD – The University of Economics, Bratislava, Slovakia Professor Maria de MONSERRAT LLAIRO, PhD – Faculty of Economic Sciences, Buenos Aires University, Argentina

Research Professor Domenico MORRONE, PhD – LUM Jean Monnet University, Bari – Casamassima, Italy

Professor Kevin V. OZGERCIN, PhD, Department of Politics, Economics & Law, The State University of New York, USA Senior Fellow & the Head of the Stockholm Center for South Asian and Indo-Pacific Affairs (SCSA-IPA), PhD, New Delhi, India

Professor Tatjana BURZANOVIĆ, Fakultet za dizajn i multimediju, Univerzitet Donja Gorica, Podgorica, Montenegro

Asst. Professor Natasha SARAFOVA, Faculty of Philology, Goce Delcev University, Štip, North Macedonia

Članovi iz Srbije: / Members from Serbia:

Professor Tatjana CVETKOVSKI, PhD, Faculty of Business Studies, Megatrend University, Belgrade

Professor Vladan PAVLOVIĆ, PhD, Faculty of Economics, Kosovska Mitrovica, University of Priština

Professor Vladimir RISTANOVIĆ, PhD, Research associate, Institute for European Studies, Belgrade

Professor Olja MUNTILAK IVANOVIĆ, PhD, Faculty of Sciences, The Department of Geography, Tourism and Hotel Management, University of Novi Sad, Novi Sad

Professor Slobodan POPOVIĆ, Fakultet za ekonomiju i inženjerski menadžment, Univerzitet Privredna akademija, Srbija

Professor Svetislav LUTOVAC, Faculty of Law, Megatrend University, Belgrade

Professor Nada TORLAK, Faculty of Culture and Media, Megatrend University, Belgrade

Professor Zorana MIHAJLOVIĆ, Faculty of Law, Megatrend University, Belgrade

“Megatrend review” is the leading scholarly journal of national importance,
according to the classification M51 clasiffied by CEON, and M52 classified
by the Ministry of Science of the Republic of Serbia

* * *

“Megatrend Review” is registered
in The International Bibliography of the Social Sciences (IBSS)
produced by the London School of Economics and Political Science
– Pro Quest Michigan USA.

* * *

“Megatrend Review” is registered and published
in EBSCO's (EBSCO Publishing Inc.) Database "Business Source Complete":
<http://www.ebscohost.com/titleLists/bth-journals.xls>

* * *

“Megatrend Review” is registered
in GESIS "Knowledge Base SSEE", Leibniz Institute for the Social Science:
<http://www.cee-socialscience.net/journals/>

The Library of Congress Catalog

Megatrend review: the international review of applied economics.

LC Control No.: 2007201331

Type of Material: Serial (Periodical)

Uniform Title: Megatrend Revija. English.

Main Title: Megatrend review : the international review of applied economics.

Published/Created: Belgrade : ill. ; 24 cm.

Description: v. : Megatrend University of Applied Sciences, [2004]-
Year 1, no. 1 ('04)-

ISSN: 1820-4570

CALL NUMBER: HB1 .M44

CIP – Каталогизација у публикацији

Народна библиотека Србије, Београд

33

MEGATREND revija = Megatrend Review / glavni urednik Vesna Baltezarević.

- God. 1, br. 1 (2004)- . - Beograd : Megatrend univerzitet, 2004- (Bor : Tercija). - 24 cm

Tekst na srp. i engl. jeziku. - Preuzeo je: Megatrend review = ISSN 1820-4570. - Drugo izdanje na drugom medijumu: Megatrend revija (Online) = ISSN 2560-3329. - Ima izdanje na drugom jeziku: Megatrend review = ISSN 1820-4570

ISSN 1820-3159 = Megatrend revija

COBISS.SR-ID 116780812

Sadržaj – Contents

EKONOMIJA

STEFAN MILOJEVIĆ OD TRADICIONALNOG DO STRATEGIJSKOG UPRAVLJAČKOG RAČUNOVODSTVA: IZAZOVI I PRILIKE	1
NIKOLA KOVINIĆ UTICAJ STRANIH DIREKTNIH INVESTICIJA NA KLJUČNE MAKROEKONOMSKE VARIJABLE U REPUBLICI SRBIJI I ZEMLJAMA REGIONA	15
STEFAN MILOJEVIĆ FORENZIČKO RAČUNOVODSTVO U DIGITALNOM OKRUŽENJU: TRENDOWI I PROMENE	39

MENADŽMENT I MARKETING

MARKO STANOJEVIĆ, DANILO IZGAREVIĆ INTEGRATION OF ARTIFICIAL INTELLIGENCE IN CORPORATE INFORMATION SECURITY SYSTEMS	51
MARIJANA ZIMONJIĆ, MILINKO VELIČKOVIĆ TRANSFORMACIJA UPRAVLJANJA LJUDSKIM RESURSIMA KROZ VEŠTAČKU INTELIGENCIJU	61
ANĐELKA RAČIĆ ETIČKI ASPEKT U CIVILNOM VAZDUHOPLOVSTVU I TRANSPORTU (CARGO) USLUGE	75
ALBINA KECMAN, VLADIMIR STANKOVIĆ ULOGA LJUDSKIH RESURSA U KONKURENTNOSTI I EKONOMSKOM RASTU	95
MARKO STANOJEVIĆ, DANILO IZGAREVIĆ THE ROLE OF HUMAN RESOURCE MANAGEMENT IN ENHANCING CORPORATE INFORMATION SECURITY CULTURE	105
ANĐELKA RAČIĆ ETIKA POSLOVANJA U CIVILNOM VAZDUHOPLOVSTVU	115
SNJEŽANA GLUMAC LOURENCO, LAYTH NESSEEF INVESTICIONO PONAŠANJE U ERI ODRŽIVOSTI I SKLONOST INVESTITORA KA ZELENIM KOMPAIJAMA	133

PRAVO

ALEKSANDRA NIKOLOVA MARKOVIĆ CONTEMPORARY CHALLENGES AND PERSPECTIVES FOR THE DEVELOPMENT OF INTERNATIONAL AVIATION LAW	149
ALEKSANDRA NIKOLOVA MARKOVIĆ ANALYSIS OF THE LEGAL REGULATION OF THE REPUBLIC OF SERBIA ON CIVIL AVIATION AND ITS COMPLIANCE WITH INTERNATIONAL REGULATIONS	159

POLITIKA I BEZBEDNOST

IVANA BALTEZAREVIĆ, VESNA BALTEZAREVIĆ, RADOŠLAV BALTEZAREVIĆ AI-DRIVEN SOCIAL BOTS IN POLITICAL CAMPAIGNS AND THEIR ROLE IN SHAPING OPINION, MANIPULATION AND MOBILISATION	169
DANILO IZGAREVIĆ, MIRJANA RISTIĆ, MARKO STANOJEVIĆ DARK WEB FORENSICS, INFORMATION SECURITY, AND THE INVESTIGATION OF ILLICIT DIGITAL FOOTPRINTS	181
BOJAN ZIMONJIC, JOVICA VASILJEVIC ULOGA INFORMACIONIH TEHNOLOGIJA U UNAPREĐENJU BEZBEDNOSTI CIVILNOG VAZDUHOPLOVSTVA	193
DEJANA RADOVIĆ, DRAGAN NIKOLIĆ DIPLOMATIC ACTIVITIES AND THE INFLUENCE OF THE ENGLISH LANGUAGE ON LOCAL TERMINOLOGY IN SECURITY AND CORPORATE CONTEXTS	209
MIRJANA RISTIĆ, DANILO IZGAREVIĆ, MARKO STANOJEVIĆ DIGITAL FORENSICS AND INFORMATION SECURITY IN THE ERA OF ARTIFICIAL INTELLIGENCE – EXPLORING NEW APPROACHES AND ETHICAL IMPLICATIONS	221
DEJAN V. KOŽOVIĆ, DRAGAN Ž. ĐURĐEVIĆ SIGURNOST ADS-B AVIO SISTEMA: ANALIZA LJUDSKIH FAKTORA	231
DRAGAN NIKOLIĆ, DEJANA RADOVIĆ ENGLISH LANGUAGE PROFICIENCY AS A STRATEGIC TOOL IN INTERNATIONAL RELATIONS AND CORPORATE SECURITY	245
VLADIMIR LOVIĆ, MILOŠ AZDEJKOVIĆ IZAZOVI DIGITALNOG OKRUŽENJA: MEDJUNARODNOPRAVNI, GEOPOLITIČKI I BEZBEDNOSNI ASPEKTI	255
SPISAK RECENZENATA / LIST OF REVIEWERS	273
OSNOVNE INFORMACIJE O ČASOPISU I UPUTSTVO ZA AUTORE	275
GENERAL INFORMATION ON THE JOURNAL AND THE INSTRUCTIONS FOR AUTHORS	285

OD TRADICIONALNOG DO STRATEGIJSKOG UPRAVLJAČKOG RAČUNOVODSTVA: IZAZOVI I PRILIKE

Sažetak: *Upravljačko računovodstvo se razvilo od tradicionalne funkcije do savremenog sistema informisanja koji podržava strateško odlučivanje, kreiranje vrednosti i upravljanje organizacionim performansama. Promena uloge upravljačkih računovođa rezultat je dinamičnog poslovnog okruženja, digitalne transformacije, potrebe za bržim i pouzdanijim informacijama, kao i rastućih zahteva menadžmenta za analitičkom podrškom. Ključni izazovi uključuju potrebu za razvojem novih kompetencija računovođa, usklađivanje različitih izvora podataka, obezbeđivanje kvaliteta i relevantnosti informacija, kao i balansiranje uloga kontrolinga, analitike i strateškog savetovanja. Preporučuje se primena upravljačkog računovodstva kao podrške upravljačkim procesima, jer poboljšava konkurentsku prednost i generiše vrednost za organizaciju.*

Ključne reči: *upravljačko računovodstvo, strategija, odlučivanje, organizacija*

* Fakultet poslovne ekonomije, Univerzitet Educons, Sremska Kamenica, Srbija.
E-mail: stefan.milojevic@educons.edu.rs

UVOD

Sa pojavom ekonomske aktivnosti, čovek je morao da registruje i činjenice te strane njegovog života. Tako je i nastalo računovodstvo. Ono se preko rasta i širenja proizvodne aktivnosti čoveka postepeno širilo. Tako su formirane tri glavne oblasti računovodstva: finansijsko računovodstvo, upravljačko računovodstvo i poresko računovodstvo (Frolova et al., 2021). Pod dominantnom ulogom ekonomskog pozitivizma i male grupe moćnih američkih članova akademske zajednice, sistem informisanja upravljačkog računovodstva se razvijao u skladu sa finansijskim računovodstvom (Malmi & Granlund, 2009).

Računovodstvo je fenomen koji se menja i isprepleteno je sa samim menadžmentom. „Računovodstvo predstavlja informacioni most koji povezuje top menadžment profitno orijentisane organizacije sa ekonomskim transakcijama koje se u njoj odvijaju i rezultatima donetih strateških odluka“ (Milojević, 2025: 3). Primenjene nauke i koncepti se kontinuirano razvijaju i redefinišu računovodstvo (Dahal, 2019).

Upravljačko računovodstvo definisano prema CIMA citatu (1996) glasi: „proces identifikacije, merenja, prikupljanja, analize, pripreme, tumačenja i komunikacije informacija koje menadžment koristi za planiranje, procenu i kontrolu unutar entiteta i za obezbeđivanje odgovarajuće upotrebe i odgovornosti za svoje resurse“. Upravljačko računovodstvo nastavlja da se razvija u skladu sa tim kako se preduzeća suočavaju sa novim problemima koje treba rešiti, a važno je istaći i činjenicu da se prakse upravljačkog računovodstva koje su korišćene početkom 1900-ih, primenljive i danas. Upravljačko računovodstvo je podsistem računovodstva koji igra vitalnu ulogu u poslovnom okruženju (Filippova, 2023). Alati upravljačkog računovodstva imaju široku primenu i kod porodičnih preduzeća (Hiebl & Mayrleitner, 2019), posebno u delu koji se odnosi na olakšanu komunikaciju između članova porodične firme i eksternog savetnika (Leotta et al., 2023).

Uticaj procesa globalizacije i integrisane internacionalizacije tržišta na način poslovanja savremenih korporacija je veliki i zahteva sofisticirane informacije, te tako i razvoj sistema upravljačkog računovodstva. Računovodstvo je učestvovalo u dizajniranju i implementaciji mnogih promena u praksi upravljanja organizacijama (Burchell et al., 1980). Stoga se računovodstveni sistemi mogu posmatrati kao ogledala društva i organizacija u kojima su uključeni i oni se za razliku od nekih drugih sistema kontinuirano nadograđuju (Knežević et al., 2012). Računovodstvo i revizija su profesije koje su najviše pogođene procesom digitalne transformacije. S jedne strane, veštačka inteligencija je unapredila efikasnost poslovnih procesa i podršku menadžmentu, dok je s druge strane sve izraženija zabrinutost za budućnost ovih profesija (Costa & Pinho, 2025). Široka automatizacija i smanjenje

potrebe za pojedinim tradicionalnim poslovima već uveliko utiču i na ove dve profesije. Drugim rečima, digitalizacija i tehnologije veštačke inteligencije imaju visok potencijal da transformišu oblast upravljačkog računovodstva, kao i ulogu računovođa (Abbas, 2025). Izazovi se odnose na smanjene mogućnosti zapošljavanja u računovodstvenoj profesiji i nove zahteve za veštinama kojima se profesija mora prilagoditi (Matejić et al., 2025). U dinamičnom i izazovnom okruženju, masovno povećanje količine znanja koje pojedinci generišu putem novih informacionih tehnologija će zahtevati napredne veštine i sposobnosti za upravljanje tim znanjem (Beke-Trivunac et al., 2025).

Prvi deo rada ukazuje na evoluciju upravljačkog računovodstva. Nakon toga, drugi deo rada se bavi transformacijom uloge upravljačkog računovođe. Strategijska dimenzija upravljačkog računovodstva je predmet obuhvatanja u trećem delu rada. Na kraju slede zaključna razmatranja.

1. Evolucija upravljačkog računovodstva

Računovodstvo predstavlja živi sistem, te je kao takvo i evoluiralo i steklo moderne karakteristike. Ujedno predstavlja uslužnu funkciju. Od računovodstva se očekuje da pruži relevantne informacije koje će pomoći menadžerima na različitim nivoima u organizaciji da razlikuju ukupne organizacione ciljeve i da im pomognu u donošenju mudrih odluka. U sadašnjoj fazi, automatizacija i digitalizacija su čvrsto ukorenjene u našim životima, menjajući ne samo naše navike i preferencije, već i druge aspekte naših života. Na osnovu analize ekonomske literature, zaključuje se da se aktivnost računovođa svodi na formiranje računovodstvenih politika, tumačenje događaja i klasifikaciju činjenica ekonomske aktivnosti preduzeća. Profesija „računovođa“ u našem uobičajenom smislu biće stvar prošlosti, zamenjena kvalifikovanim stručnjacima sa funkcijama finansijskog supervizora.

Za razliku od konvencionalnog finansijskog računovodstva, upravljačko računovodstvo se koristi za opisivanje modernog koncepta računovodstva kao alata upravljanja, koje često ima i strategijsku dimenziju. Sistem informisanja upravljačkog računovodstva deluje u dva pravca (1) obezbeđivanje informacija koje podržavaju donošenje mudrih ekonomskih odluka i (2) motivacija korisnika da deluju u skladu sa organizacionim ciljevima (Horngren, 1995). Uočeno je da su organizacije koje posluju u konkurentnijim okruženjima obično koristile veći broj sistema upravljačkog računovodstva (Libby & Waterhouse, 1996), kao i da intenzitet konkurencije utiče na promene upravljačkog računovodstva kroz organizacionu strukturu (Waweru, 2008). Pored toga, nalazi Waweru & Uliana (2008) su pokazali da su organizacije koje su stavljale veliki naglasak na strategije diferencijacije,

prijavile značajne promene u svojim sistemima upravljačkog računovodstva i kontrole. Sistemi upravljačkog računovodstva su konceptualizovani kao zavisni od organizacione strukture i konteksta. Ovo može uticati na promene na dva načina: ili ih podsticati ili ometati njihovu brzinu (Libby & Waterhouse, 1996).

Promene u tehnologiji i organizacionim procedurama u menadžmentu imaju značajan uticaj na upravljačko računovodstvo. Naime, informaciona tehnologija je bila najvažniji pokretač nedavnih promena u upravljačkom računovodstvu (Dung & Lien, 2024). Brza digitalna transformacija je podstakla modifikacije upravljačkih procesa. Nove tehnologije omogućavaju finansijskim stručnjacima da se više fokusiraju na upravljačko računovodstvo (Milacic & Zarkovic, 2025). Sa brzim razvojem interneta, era veštačke inteligencije postala je trend u današnjem društvu, uvodeći inteligentnu revoluciju u raznim industrijama. To će u velikoj meri uticati i na tradicionalne metode rada i pristupe finansijskih računovođa od kojih se očekuje generisanje validnih informacija za eksterne korisnike.

Primena tehnologije veštačke inteligencije ne samo da može poboljšati efikasnost finansijskih računovođa, već i promovisati prelazak sa finansijskog računovodstva na upravljačko računovodstvo. Stoga je način korišćenja veštačke inteligencije za pomoć finansijskim stručnjacima u radu upravljačkog računovodstva neizbežan uslov za razvoj inteligentnog doba, koje postavlja veće zahteve za upravljačko računovodstvo. Da bi računovodstvo u punoj meri odgovorilo na izazove koje predstavljaju velike količine informacija i njihova složenost, potrebno je da integriše tehnološke promene. Generalno, na osnovu ove pozadine, proces razvoja preduzeća mora transformisati model finansijskog upravljanja, omogućavajući tehničkim aspektima prikupljanja i organizacije podataka da se kreću ka pravicima koji podstiču snažniji napredak i veću efikasnost. Važno je kreirati strategije za korišćenje veštačke inteligencije kako bi se finansijskim računovođama pomoglo da steknu veštine upravljačkog računovodstva, postignu transformaciju finansijskih stručnjaka u upravljačke računovođe i pruže podršku za razvoj. Nesporna je činjenica da tehnologije zasnovane na veštačkoj inteligenciji dramatično menjaju aktivnost i ulogu stručnjaka u računovodstvu. To zahteva nove paradigme u funkciji razumevanja novih realnosti.

2. Transformacija uloge upravljačkog računovođe

Ovo doba zahteva profesionalce u sa odgovarajućom ravnotežom između tehničkih veština i širine znanja kako bi bili kompatibilni sa tekućom transformacijom. Isto važi i za finansijske i upravljačke računovođe. U skoro svim dimenzijama profesionalnog radnog okruženja, današnje upravljačke računovođe doživljavaju

promene. Naime, pritisci tržišne konkurencije su iznedrili izazove u prilagođavanju savremene prakse u upravljačkom računovodstvu kako bi reagovali na promenljive potrebe u turbulentnom okruženju. Organizacije se danas suočavaju sa brojnim opcijama i izazovima, tako da im je neophodno da se upravljačke računovođe uključe i rade na bilo kom nivou kao deo tima (Kamal, 2015).

Pozicija savremenih upravljačkih računovođa je da dodatno nose način unapređenja i proširenja organizacione vizije i od njih se zahteva da se pojave kao komercijalni poslovni partneri i agenti promena. Upravljačke računovođe mogu i treba da široko budu uključene u organizacione aktivnosti. Upravljačke računovođe su sada važne u oblikovanju budućih poslovnih strategija. Ova nova uloga je inicirana veštačkom inteligencijom, ažuriranim kontrolnim tablama i sistemima poslovne inteligencije (Khan et al., 2025). Ističe se da računovođe sada moraju biti vešte po pitanju upotrebe podataka, njihovom timskom obradom sa ljudima iz drugih odeljenja, kao i da koriste strategijsko razmišljanje. Ipak, nije sve bez problema; ljudima su potrebne nove veštine, neki se plaše da se prilagode, a tehnologiju je u nekim slučajevima teško integrisati. Uprkos raznim izazovima, istaknute publikacije, kao što je primera radi, "Harvard Business Review", takođe su skrenule pažnju menadžera širom sveta na mnoge tehnike i procese upravljačkog računovodstva strategijske orijentacije.

Ključna vrednost veštačke inteligencije je da ona može poboljšati, a u nekim slučajevima čak i zameniti ljudsko donošenje odluka i delovanje (Davenport & Ronanki, 2018). Naime, sistemi veštačke inteligencije obavljaju složene zadatke i donose sofisticirane procene i odluke. Korišćenje veštačke inteligencije može pomoći upravljačkim računovođama u realizaciji raznih zadataka, a neki od njih jesu: budžetiranje i obračun troškova, održavanje i kontrola evidencije zaliha, upravljanje potraživanjima i najzad, očekuje se i podrška kod strateškog finansijskog planiranja (Kerr et al., 2025).

Savremeno poslovanje prožimaju brojne mogućnosti za razvoj različitih profesija, ali to za sobom povlači i neke rizike (Mitrović et al., 2022:73). Budućnost upravljačkih računovođa zavisi od toga kako se prilagođavaju i reaguju na promenljive i nove tehnologije, kao i na promene koje se tiču regulatornih i drugih faktora koji utiču na ovu profesiju. Nalazi Shields (1998) ukazuju da postoji konvergencija među evropskim zemljama u praksi upravljačkog računovodstva, posebno kada je reč o terminologiji i tehnikama, dok je uočena manja konvergencija po pitanju svrhe i stilova korišćenja tehnika. Na izbor i oblikovanje novih računovodstvenih rutina mogu uticati mnogi faktori, kao što su potreba za kontrolom troškova, promena načina planiranja i kontrole, konkurencija i dinamika tržišta, regulativa i pritisci koji dolaze od strane strukovnih udruženja i drugo. Istraživanje promena u upravljačkom računovodstvu se uglavnom odnosi na prakse u razvijenim zemljama

(Maina Waweru et al.: 676). Bez obzira na činjenicu da mnoge upravljačke računovođe u nemačkom govornom području Evrope pohađaju kurseve kontinuirane edukacije iz upravljačkog računovodstva, pružaoci takvih kurseva nemaju tako snažno društveno priznanje kao što to slučaj kada je u pitanju Ovlašćeni institut upravljačkih računovođa (The Chartered Institute of *Management Accountants* - CIMA) u Velikoj Britaniji (Heinzelmann 2016).

3. Strategijski aspekti upravljačkog računovodstva

Da bi bili kompetentni i pouzdani u organizaciji, računovođe bi trebalo da se proaktivno uključe u liderstvo, stratejsko upravljanje, operativno usklađivanje i doživotno učenje i usavršavanje. Današnje poslovno okruženje se drastično promenilo. Stavljjen je naglasak na proizvode višeg kvaliteta, niže cene i troškove, globalnu konkurenciju i zadovoljavanje i predviđanje potreba kupaca (Dahal, 2019), tako da u celini gledano, to iziskuje i nove stratejske imperativne, kao i jačanje postojećih. Strateške odluke počivaju na širim osnovama. Sve to skupa je doprinelo pojavi stratejskog upravljačkog računovodstva kao vitalnog alata za organizacije koje se kreću u dinamičnim i konkurentnim poslovnim okruženjima (Rahuman, 2025), i potrebno je da ga menadžeri percipiraju kao deo šireg organizacionog sistema. Kako Knežević et al. (2011:5) ističu, "stratejsko upravljačko računovodstvo je fokusirano na analizu podataka upravljačkog računovodstva o preduzeću i njegovoj konkurenciji radi identifikovanja i praćenja poslovne strategije".

Cilj vrhovnog menadžmenta je da kroz izveštavanje pomogne menadžmentu na svim nivoima da uspostavi planove i vrši kontrolu nad poslovanjem, što je osnova za merenje efikasnosti politika koje su uspostavljene. U tom kontekstu se ističe da upravljačko računovodstvo stratejske orijentacije pomaže donosiocima stratejskih odluka da obezbede relevantne finansijske i nefinansijske mere. Pažljivo praćenje efikasnosti upravljanja resursima je bitno za održivo poslovanje organizacije.

U visoko konkurentnom okruženju je čini se, više nego ikada bitno obezbediti informacije koje se odnose na aktivnosti konkurenata i trenutne i buduće tržišne trendove, kako bi se na najbolji način podržao proces evaluacije strategije. Upravljačko računovodstvo je po svojoj prirodi pomoćna aktivnost za donošenje odluka i kontrolu u organizaciji. Shodno tome, računovodstvo se mora povezati sa drugim oblastima, kao što je marketing, kako bi se uspostavili mehanizmi stratejskog upravljanja koji poboljšavaju organizacione performanse. Međutim, tradicionalne informacije iz upravljačkog računovodstva ne mogu se pružiti za stratejsko donošenje odluka. Fokus je pomeren od operativnog ka stratejskom. Termin „stratejsko upravljačko računovodstvo“ postoji u literaturi o upravljačkom računovodstvu

više od decenije. Međutim, ne postoji usaglašen termin strategijskog upravljačkog računovodstva u literaturi (Langfield-Smith, 2008).

Informacije koje se koriste u procesu odlučivanja su posebno relevantne za opstanak preduzeća u neprijateljskom i konkurentnom okruženju. Mogu biti deo operativnog upravljanja firmama. Čini se da je upotreba termina „strategijsko upravljačko računovodstvo“ i dalje nedovoljno razumljiva za računovođe u organizacijama, posebno kada je reč o nacionalnim okvirima. Strategijsko upravljačko računovodstvo se može posmatrati na jednostavan način, kao težnja da se upravljačkom računovodstvu u većoj meri dodeli strategijska orijentacija; ili da se sagleda kao “pružanje i analiza podataka upravljačkog računovodstva o proizvodu kompanije na tržištima, njenoj strukturi troškova i troškovima konkurenata, kao i praćenje strategijskih pozicija firme i njenih konkurenata na ovim tržištima tokom vremena” (Nik Abdullah et al., 2022). Kako Ma et al. (2022) navode, tehnike strategijskog upravljačkog računovodstva mogu u velikoj meri pomoći malim i srednjim preduzećima da racionalno raspodele ograničene resurse, i integrišu interne i eksterne informacije radi podrške menadžerima da donose adekvatne strategijske odluke.

Tehnike koje se koriste u strategijske svrhe imaju potencijal da pruže širok spektar prednosti za organizacije, a uključuju: računovodstvo konkurenata, računovodstvo kupaca, strategijski obračun troškova, strategijsko planiranje, kontrolu i upravljanje performansama, iz čega se može sagledati da je nesporna značajna uloga upravljačkog računovodstva u donošenju strategijskih odluka, planiranju i prognoziranju. Potrebno je ojačati njihovu integraciju u rad zaposlenih na nadzornim i kontrolnim pozicijama na višem i srednjem nivou menadžmenta u organizacijama (Shaqqour, 2025). Međutim, kada su u pitanju ekonomije u razvoju, nezavisno od brojnih koristi, implementacija strategijskog upravljačkog računovodstva suočava se sa brojnim izazovima. Neki od njih jesu: neadekvatno tehničko znanje, nedostatak svesti, otpor prema promenama i odsustvo regulatornih okvira koji podstiču njegovo usvajanje (Alkhafaji & Khalid, 2019).

Upravljačko računovodstvo funkcioniše kao dinamička sposobnost koja oblikuje strategiju i rast kompanije omogućavajući integrisane procese koji olakšavaju strategijsku raspodelu resursa tokom vremena, posebno unutar malih i srednjih preduzeća. Shodno tome, uključivanje tehnika analize podataka upravljačkog računovodstva može pomoći u donošenju odluka. Primera radi, podaci o tržištu mogu podržati strategijsko upravljanje. Strategijsko upravljanje je sistematski proces osmišljen da optimizuje korišćenje resursa uz usklađivanje sa organizacionim ciljevima. U suštini, poslovne strategije i politike predstavljaju formulisanje strategijskog plana za postizanje vizije, misije i ciljeva kompanije.

Najprikladniji indikator za procenu efikasnosti alata upravljačkog računovodstva koje kompanija usvaja jeste učinak. Upravljačke računovođe sve više igraju

ključnu ulogu u merenju organizacionog učinka i pružanju informacija višem menadžmentu za podršku donošenju odluka. Finansijski učinak se odnosi na sposobnost kompanije da generiše profit, dok nasuprot tome, nefinansijski učinak obuhvata metrike koje dopunjuju finansijske izveštaje i dizajnirane su da postignu dugoročne ciljeve, kao što su lojalnost kupaca, angažovanje zaposlenih i organizaciona održivost.

Upravljačko računovodstvo je neophodno za podršku strategijskom odlučivanju i organizacionoj konkurentnosti (Dung & Lien, 2024). Strategijski fokus kompanije (interni ili eksterni) značajno utiče na njegov učinak, jer su strategijsko planiranje i donošenje odluka ključni i za male i za velike organizacije. Generalno, prakse strategijskog upravljanja, kao što su postavljanje ciljeva, strategijsko planiranje, analiza finansijskih pokazatelja, upravljanje ukupnim kvalitetom i preduzetnička orijentacija, pozitivno utiču na organizacioni učinak, posebno u malim i srednjim preduzećima. Istovremeno, evaluacija i odabrana strategija su veoma relevantni za poslovni uspeh. Efikasnost sistema informisanja upravljačkog računovodstva strategijske orijentacije u smislu zadovoljenja potreba ključnih grupa informacionih adresata zavisi od toga da li je primenjen sveobuhvatni pristup njegovoj organizaciji na nivou poslovnog subjekta. Pritom je bitno uvažiti specifičnosti, kako organizacionih, tako i upravljačkih struktura entiteta.

Literatura o profesionalizaciji upravljačkog računovodstva u porodičnim firmama se u velikoj meri fokusirala na stručnjake koji nisu članovi porodice, kao što su kontrolori ili finansijski direktori, kao pokretače ovog procesa, što je donekle jednostran pogled. Važno pitanje je i istražiti kako menadžeri mogu doprineti profesionalizaciji upravljačkog računovodstva u porodičnim firmama. Iako mnoge upravljačke računovođe u nemačkom govornom području Evrope pohađaju kurseve kontinuirane edukacije iz upravljačkog računovodstva, pružaoci takvih kurseva nemaju tako snažno društveno priznanje kao, na primer, Ovlašćeni institut upravljačkih računovođa (CIMA) u Velikoj Britaniji (Heinzelmann, 2016).

Zaključak

Računovođe igraju ključnu ulogu u pružanju pouzdanih finansijskih i operativnih informacija za donošenje ekonomskih i finansijskih odluka. Ove odluke su važan element za organizaciju. Stoga, računovodstvo postaje nezaobilazan element u formiranju poslovne strategije. Uspešno upravljanje preduzećem zahteva prilagođavanje dinamičnim uslovima poslovanja u kontinuitetu. Kako se poslovni pejzaž razvijalo, računovodstvo je prevazišlo svoju tradicionalnu ulogu, postavši ključna komponenta u menadžerskom donošenju odluka.

Finansijsko računovodstvo predstavlja sistem informisanja primarno usmeren na zadovoljenje informacionih potreba eksternih korisnika, dok upravljačko računovodstvo pruža neophodne informacije koje pomažu menadžmentu u kreiranju politika i u svakodnevnom (operativnom) poslovanju. Računovodstvo kao sistem informisanja neće nestati, kao što ni sam ekonomski život neće nestati. Doći će do transformacije računovodstva zajedno sa ekonomskim životom, i nastaviće da se odvija u drugačijem, naprednijem i progresivnijem obliku. Stoga, od dinamičnih upravljačkih računovođa se u sve većoj meri zahteva fleksibilnost, odnosno da budu u poziciji da mogu da se prilagode promenama u tržišnom okruženju koje imaju veći uticaj na organizaciju.

Sa ubrzanim razvojem tehnologije i globalizacijom, došlo je do velikih promena u sferi upravljanja ljudskim resursima. Danas je upravljačko računovodstvo važan aspekt planiranja i donošenja odluka u poslovanju. Naime, u preduzećima koja koriste mnogo podataka, menadžeri očekuju mnogo više od svojih računovođa. Potrebna je šira primena naprednijih praksi i tehnika strategijskog upravljačkog računovodstva u realnom ambijentu. Od upravljačkih računovođa se očekuje da čitaju, razumeju finansijske i nefinansijske evidencije, predviđaju buduće trendove, proučavaju rizike, kao i da povezuju svaku finansijsku meru sa ciljevima kompanije.

Literatura

- Abbas, K. (2025): "Management accounting and artificial intelligence: a comprehensive literature review and recommendations for future research". *The British Accounting Review*, 101551.
- Alkhafaji, A. F. & Khalid, S. (2019): "Challenges of implementing management accounting innovations: Evidence from Nigeria". *Prometheus*, 38(4), 399-415.
- Beke-Trivunac, J., Knežević, S., Milojević, S., Mrdak, G., Adamović, M. (2025). Znanje i/ili veštine za upravljanje ograničenim ekonomskim, prirodnim i ljudskim resursima, „Znanje ili veštine“ ili „znanje i veštine“, tematski zbornik nacionalnog značaja, Alfa BK Univerzitet - Institut za strategijske studije i razvoj „Petar Karić“ i Naučno društvo za upravljanje organizacijama.
- Burchell, S., Clubb, C., Hopwood, A., Hughes, J., & Nahapiet, J. (1980): "The roles of accounting in organizations and society". *Accounting, organizations and society*, 5(1), 5-27.
- CIMA (1996): *Official Terminology*, London: CIMA.
- Costa, M., & Pinho, M. (2025): "Management accounting and the paradigm change-a journey through the age of digitalization". *Procedia Computer Science*, 263, 564-574.

- Dahal, R. K. (2019): "Changing role of management accounting in 21st Century". *Review of Public Administration and Management*, 7(3), 1-8.
- Davenport, T. H., & Ronanki, R. (2018): "Artificial intelligence for the real world". *Harvard business review*, 96(1), 108-116.
- Dung, N. T. P., & Lien, N. T. H. (2024): "Factors affecting the stages of management accounting evolution: The developing market research [Special issue]". *Journal of Governance & Regulation*, 13(2), 452–464. <https://doi.org/10.22495/jgrv13i2siart20>
- Filippova, L. (2023): "International Practice in the Organization of Management Accounting". In: Bolgov, R. *et al.* Proceedings of Topical Issues in International Political Geography. TIPG 2021. Springer Geography. Springer, Cham. https://doi.org/10.1007/978-3-031-20620-7_20
- Frolova, O. A., Milgunova, I. V., Sidorova, N. P., Kulkova, N. S., Kitaeva, E. N. (2021): "Development of Accounting in Digital Economy Era". In: Antipova, T. (eds) Integrated Science in Digital Age 2020. ICIS 2020. Lecture Notes in Networks and Systems, vol 136. Springer, Cham. https://doi.org/10.1007/978-3-030-49264-9_5
- Grinko, A., Havrylenko, N., Kostash, T., Plekan, M., & Breus, S. (2020): "Organization of a strategic management accounting in an innovative economy". *Academy of Accounting and Financial Studies Journal*, 24(5), 1-7.
- Heinzelmann, R. (2016): "Comparing professions in UK and German-speaking management accounting". *Accounting in Europe*, 13(1), 103-120.
- Hiebl, M. R. W., Mayrleitner, B. (2019): "Professionalization of management accounting in family firms: the impact of family members". *Review of Managerial Sciences*, 13, 1037–1068, <https://doi.org/10.1007/s11846-017-0274-8>
- Horngren, C. T. (1995): "Management accounting: this century and beyond". *Management Accounting Research*, 6(3), 281-286.
- Kamal, S. (2015): "Historical evolution of management accounting". *The cost and management*, 43(4), 12-19.
- Kerr, D., Smith, K. T., Smith, L. M., & Xu, T. (2025): "A Review of AI and Its Impact on Management Accounting and Society". *Journal of Risk and Financial Management*, 18(6), 340.
- Khan, M. S. U., Sophia, J., & Shetty, P. (2025): "The Evolving Role of Management Accounting in Strategic Decision-Making: A Study of Contemporary Practices in Data-Driven Enterprises", *International journal of research and scientific innovation (IJRSI)*, 12(6), DOI: <https://doi.org/10.51244/IJRSI.2025.120600133>
- Knežević, S., Barjaktarović Rakočević, S., & Đurić, D. (2011): "Upravljačko računovodstvo u funkciji sticanja konkurentske prednosti i bankarski kontroling". *Management - časopis za teoriju i praksu menadžmenta*, 16(59), 5-13.

- Langfield-Smith, K. (2008): "Strategic management accounting: how far have we come in 25 years?". *Accounting, Auditing & Accountability Journal*, 21(2), 204-228.
- Leotta, A., Rizza, C., & Ruggeri, D. (2023): "Complementing family firm and managerial views of doing business through management accounting tools". *Journal of Management Control*, 34(3), 347-376.
- Libby, T., & Waterhouse, J. H. (1996): "Predicting change in management accounting systems". *Journal of Management Accounting Research*, 8.
- Ma, L., Chen, X., Zhou, J., & Aldieri, L. (2022): „Strategic management accounting in small and medium-sized enterprises in emerging countries and markets: A case study from China". *Economies*, 10(4), 74.
- Maina Waweru, N., Hoque, Z., & Uliana, E. (2004): "Management accounting change in South Africa: Case studies from retail services". *Accounting, Auditing & Accountability Journal*, 17(5), 675-704.
- Malmi, T., & Granlund, M. (2009): "In search of management accounting theory". *European accounting review*, 18(3), 597-620.
- Matejić, T., Knežević, S., Joksimović, A., Milojević, S., & Adamović, M. (2025): "Potentials of blockchain technology application in accounting and financial reporting". *BizInfo Blace*, 16(1), 87-95. <https://doi.org/10.71159/bizinfo250010M>
- Milacic, D., & Zarkovic, S. (2025): "The role of the management accountant in leadership decision-making processes". *MEST Journal*, 13(2), 177-186.
- Milojević, S. (2025): "Forenzičko računovodstvo i oporezivanje". *Megatrend revija*, 22(1), 1-16.
- Mitrović, A., Knežević, S., & Milašinović, M. (2022): "The importance of ethics in the auditing profession in contemporary business", *Revizor - časopis za upravljanje organizacijama, finansije i reviziju*, 25, 73-79.
- Nik Abdullah, N. H., Krishnan, S., Mohd Zakaria, A. A., & Morris, G. (2022): "Strategic management accounting practices in business: A systematic review of the literature and future research directions". *Cogent Business & Management*, 9(1), 2093488. <https://doi.org/10.1080/23311975.2022.2093488>Page 3 of 21
- Rahuman, M. R. A. H. (2025): "Strategic Management Accounting Usage in the Sri Lankan Service Sector". *Journal of Economics, Finance and Accounting Studies*, 7(2), 01-17.
- Shaqqour, O. F. (2025): "The Impact of Integrating Strategic Management Accounting and Decision-Making on Financial Performance in Industrial Companies". In: Hannon, A., Mahmood, A. (eds). *Intelligence-Driven Circular Economy. Studies in Computational Intelligence*, vol 1174. Springer, Cham. https://doi.org/10.1007/978-3-031-74220-0_22
- Shields, M. D. (1998): "Management accounting practices in Europe: a perspective from the States". *Management Accounting Research*, 9(4), 501-513.

- Waweru, N. (2008): "Predicting change in management accounting systems: The effects of competitive strategy". *Global Journal of Business Research*, 2(1), 25-41.
- Waweru, N., & Uliana, E. (2008): "Predicting change in management accounting systems: a contingent approach". *Problems and Perspectives in Management*, 6(2), 72-84.

FROM TRADITIONAL TO STRATEGIC MANAGEMENT ACCOUNTING: CHALLENGES AND OPPORTUNITIES

Summary: *Management accounting has evolved from a traditional function to a modern information system that supports strategic decision-making, value creation, and organizational performance management. The changing role of management accounting is a result of the dynamic business environment, digital transformation, the need for fast and reliable information, and the growing demands of management for analytical support. Key challenges include developing new competencies for accountants, harmonising disparate data sources, ensuring quality and accurate information, and balancing roles, analytics, and control consulting. We recommend applying management accounting as a support to management processes, as it improves competitive advantage and creates value for the organization.*

Keywords: *management accounting, strategy, decision making, organization*

UTICAJ STRANIH DIREKTNIH INVESTICIJA NA KLJUČNE MAKROEKONOMSKE VARIJABLE U REPUBLICI SRBIJI I ZEMLJAMA REGIONA

Apstrakt: Makroekonomske varijable, kao pokazatelj ekonomskog stanja u jednoj zemlji, predmet su sve većeg interesovanja i one nam u značajnoj meri mogu olakšati da razumemo ekonomsku politiku koju jedna država vodi. Posmatrajući kretanje vrednosti makroekonomskih varijabli možemo videti kako i na koji način strane direktne investicije (SDI) utiču na privredu jedne zemlje. SDI predstavljaju najvažniji segment razvoja privrede, posebno zemalja u razvoju kakve su analizirane zemlje (Republika Srbija, Republika Hrvatska i Bosna i Hercegovina). Ove zemlje danas ulažu velike napore kako bi svoj investicioni ambijent učinile privlačnim za strane investitore. Privlačenje adekvatnih stranih investicija i njihovo usmeravanje u ključne privredne grane je osnov za ostvarivanje privrednog razvoja. Posebna pažnja u radu data je uticaju SDI na ključne makroekonomske varijable (bruto domaći proizvod (BDP), stopu nezaposlenosti i izvoz roba i usluga) uz kontrolu uticaja inflacije. Svi podaci u radu su obrađeni uz pomoć statističkog programa SPSS i predstavljeni su tabelarno i u obliku grafikona.

Ključne reči: strane direktne investicije, bruto domaći proizvod, stopa nezaposlenosti, izvoz roba i usluga, stopa inflacije, pandemija virusa Covid-19

* Doktorant ekonomskog fakulteta u Subotici, Univerzitet u Novom Sadu, Ekonomski fakultet u Subotici, Subotica
E-mail: nikola94np@gmail.com

1. UVOD

Veliki broj teoretičara bavio se problematikom SDI, iz čega je proizašao veliki broj definicija ovog pojma. SDI prema *Balance of Payments and International Investment Position Manual, Sixth Edition*, predstavljaju kategoriju međunarodnog investiranja, pri čemu rezident jedne ekonomije preuzima kontrolu ili ostvaruje značajan uticaj na upravljanje preduzećem koje je rezident druge ekonomije.¹ Privlačenje adekvatnih stranih investicija i njihovo usmeravanje u ključne privredne grane je osnov za ostvarivanje privrednog razvoja. SDI u svim zemljama, a posebno u zemljama u razvoju kakve su analizirane zemlje (Republika Srbija, Republika Hrvatska i Bosna i Hercegovina), imaju veliki uticaj na ostvarivanje privrednog razvoja. Ove zemlje danas ulažu velike napore kako bi svoj investicioni ambijent učinile privlačnim za strane investitore. SDI utiču na povećanje BDP i izvoza roba i usluga ali i na smanjenje broja nezaposlenih što su ključni ciljevi ekonomije svake zemlje. Takođe, one omogućavaju zemljama u razvoju da dođu do novih znanja i savremenih tehnologija.

Makroekonomske varijable odražavaju numerički deo ekonomske stvarnosti i koriste se za analizu ekonomskog okruženja. Analiza glavnih makroekonomskih indikatora je veoma važna jer ima za cilj da prikaže celokupno stanje ekonomije, da predvidi njenu stabilnost i omogući investitorima da blagovremeno reaguju na novonastale situacije.² Postoji više makroekonomskih indikatora, među kojima se posebno ističu: 1) stopa nezaposlenosti, 2) rast BDP, 3) cenovna stabilnost (stopa inflacije) i 4) platni bilans.³ Merenje ekonomske aktivnosti pomoću makroekonomskih varijabli omogućava nam uvid u efekte SDI na ekonomiju jedne zemlje.

Predmet istraživanja

Predmet istraživanja pristupnog rada je kretanje SDI u Republici Srbiji, Republici Hrvatskoj i BiH u periodu od 2013. do 2022. godine, ali i njihov uticaj na BDP, stopu nezaposlenosti i izvoz roba i usluga uz kontrolu uticaja inflacije. Takođe predmet istraživanja su i investicione odlike analiziranih zemalja.

Cilj istraživanja

Primarni cilj rada je da se prikaže kretanje i zastupljenost SDI u analiziranim zemljama u periodu od 2013. do 2022. godine i na koje makroekonomske varijable

¹ Veličković, M. (2019): *Strane direktne investicije kao faktor privrednog razvoja zemalja Zapadnog Balkana*, Doktorska disertacija, Univerzitet Edukons, Fakultet poslovne ekonomije: Sremski Karlovci, str. 45.

² Mügge, D. (2016): "Studying macroeconomic indicators as powerful ideas", *Journal of European Public Policy*, pp. 410-427.

³ Greene, J. E. (2018): *Using Macroeconomic and Structural Policies to Attain Macroeconomic Objectives*, World Scientific Book Chapters, pp. 183-212.

SDI imaju najveći uticaj i u kojim zemljama je taj uticaj najveći. Takođe cilj rada je i da se pokaže kakav je uticaj SDI na makroekonomske varijable posredstvom inflacije. Društveni cilj rada treba da ukaže na značaj SDI za privredu i društvo jedne zemlje.

Metode istraživanja

Eksplorativni metod istraživanja biće korišćen za utvrđivanje tekućih trendova i stanja, odnosno koristiće se odgovarajuća naučna i stručna literatura iz ove oblasti, kao i upotreba različitih elektronskih izvora. Uz pomoć eksplorativnog metoda moći će da se analizira i utvrdi kretanje SDI u analiziranim zemljama. Metod klasifikacije koji će se koristiti u izradi ovog rada služiće da se utvrde razlike u zastupljenosti SDI u analiziranim zemljama. Analiza svih podataka biće izvršena uz pomoć statističkog programa SPSS. Podaci koji su neophodni za sprovođenje analize biće preuzeti sa zvaničnog sajta Svetske banke za period od 2013. do 2022. godine i biće prikazani na godišnjem nivou. Kao nezavisnu varijablu koristićemo SDI, dok će zavisne varijable biti BDP, stopa nezaposlenosti i izvoz roba i usluga. Kao kontrolnu varijablu koristićemo inflaciju. Za statističku analizu podataka koristimo:

- Izračunavanje deskriptivnih statističkih mera centralne tendencije i to aritmetičku sredinu i medijanu, i mera varijabilnosti i to standardnu devijaciju, minimum i maksimum;
- Linijski dijagram za prikaz promena skorova varijabli pri protoku vremena i za poređenje istih kod više varijabli;
- Korelacionu analizu za utvrđivanje povezanosti parova varijabli izraženu Pirsonovim koeficijentom korelacije i testom značajnosti tog koeficijenta;
- Parcijalnu korelacionu analizu za koju dobijamo koeficijent korelacije i njegovu značajnost u slučaju kad se zavisnost prati uz kontrolu treće varijable koja bi mogla praviti posrednu vezu između posmatranog para. Drugim rečima, ispitujemo korelaciju kada se zanemari mogući uticaj varijable posrednika.
- Linearnu regresionu analizu za ispitivanje mogućnosti uspostavljanja linearne veze između para varijabli, značajnosti te veze i varijabiliteta koji tom vezom biva određen;
- Medijacionu analizu za ispitivanje medijacije (posredstva) medijatorske (treće) varijable pri analizi uticaja nezavisno promenljive na zavisno promenljivu i njeno bliže opisivanje uz to. U model medijacione analize uključeno je sprovođenje regresione analize uticaja:
 - nezavisno promenljive (X) na zavisno promenljivu (Y) direktno,
 - nezavisno promenljive na zavisno promenljivu indirektno, tj. u modelu sa medijatorskom varijablom (M),
 - nezavisno promenljive na medijatorsku varijablu,
 - medijatorske varijable na zavisno promenljivu.

- Za utvrđivanje značajnosti medijacije koristimo Aroian test sa test statistikom

$$|z| = \frac{B_{XM} \cdot B_{MY}}{\sqrt{B_{MY}^2 \cdot SE_{XM}^2 + B_{XM}^2 \cdot SE_{MY}^2 + SE_{XM}^2 \cdot SE_{MY}^2}}$$

čija se realizovana vrednost upoređuje sa kritičnom vrednošću 1,96 za prag značajnosti od 5%, gde u slučaju da je z po apsolutnoj vrednosti manje od 1,96 kažemo da nastala medijacija nije statistički značajna. Ovde su B koeficijenti linearne regresije, a SE standardne greške nastale pri istoj.

- Za opis varijabilnosti objašnjene posredstvom inflacije koristimo relativnu snagu medijatorskog modela koja se računa kao $(Beta_{XM} \cdot Beta_{MY}) / Beta_{D;XY}$ gde su $Beta$ standardizovani koeficijenti regresije (podeljeni sa standardnom greškom). Dobiye vrednost pomnožena sa 100 predstavlja procenat spomenute varijabilnosti.

Polazne hipoteze u istraživanju

Prilikom izrade ovog rada postavljene su osnovna hipoteza i posebne hipoteze:

Osnovna hipoteza:

SDI u značajnoj meri utiču na privredu jedne zemlje i njene ključne makroekonomske varijable.

Posebne hipoteze:

H1: „Postoji značajan direktan uticaj SDI na ključne makroekonomske varijable (BDP, stopu nezaposlenosti i izvoz roba i usluga) u analiziranim zemljama (Republici Srbiji, Republici Hrvatskoj i BiH).“

H2: „Posredstvom inflacije uticaj SDI na makroekonomske varijable se ne menja značajno u analiziranim zemljama (Republici Srbiji, Republici Hrvatskoj i BiH).“

2. ANALIZA UTICAJA STRANIH DIREKTNIH INVESTICIJA NA KLJUČNE MAKROEKONOMSKE VARIJABLE

SDI predstavljaju veoma važan element globalne ekonomije i često su vodeća komponenta strategije ekonomskog razvoja, kako u razvijenim tako i u zemljama u razvoju.⁴ U kojoj će meri SDI biti realizovane u nekoj zemlji to prvenstveno zavisi od geografskog položaja zemlje, nivoa ekonomskog i političkog rizika u zemlji i regionu, pravne sigurnosti, pristupa lokalnom i regionalnom tržištu ali i od radne

⁴ Jensen, N. M. (2003): “Democratic governance and multinational corporations: Political regimes and inflows of foreign direct investment”, *International Organization*, 57(3), str. 587.

snage i institucionalne izgrađenosti u toj zemlji.⁵ U ovom poglavlju biće prikazano kako i na koji način SDI utiču na BDP, stopu nezaposlenosti i izvoz roba i usluga uz kontrolu uticaja inflacije u Republici Srbiji, Republici Hrvatskoj i BiH. Republika Srbija i BiH konstantno rade na unapređenju svog investicionog ambijenta i prilagođavanju svoje zakonske regulative, regulativi EU, kako bi postale privlačne za strane investitore.

2.1. Uticaj stranih direktnih investicija na ključne makroekonomske varijable Republike Srbije (2013.-2022.)

Koliki je značaj SDI za Republiku Srbiju kao zemlju u razvoju, govori i činjenica da su SDI, naponi Vlade u privlačenju stranih investitora i ostvareni rezultati svakodnevna tema politike i medija u Srbiji. Jedno od osnovnih obeležja zemalja u razvoju, kakva je i Republika Srbija, jeste nizak nivo domaće akumulacije kapitala koji uslovljava potrebu za intenziviranjem priliva SDI.⁶ Zahvaljujući reformama koje je Vlada Republike Srbije sprovela u poslednjih deset godina priliv SDI je bio na zadovoljavajućem nivou. Značajan napredak ostvaren je u oblasti zdravstvene zaštite, komunikacione tehnologije, razvoju obnovljive energije ali i na polju upravljanja čvrstim otpadom.⁷ Uzlaznu liniju priliva stranih investicija u Republici Srbiji prekinula je pandemija virusa Covid-19 početkom 2020. godine kada su one opale za 0,8 milijardi evra u poređenju sa 2019. godinom.⁸ Prosečno učešće investicija u BDP Srbije iznosi oko 22% od čega stana ulaganja čine oko 5%. Prema preporuci Ujedinjenih nacija udeo investicija u BDP u zemljama kao što je Republika Srbija treba da bude najmanje 25%.⁹ Strane investitore u Republici Srbiji posebno privlači to što Vlada daje značajna sredstva investitorima u obliku subvencija i što su prema zakonu iz 2014. godine domaći i strani investitori izjednačeni. Pored toga, dalje sprovođenje reformi i približavanje EU kao i poboljšanje odnosa sa međunarodnim institucijama svakako će podsticajno delovati na budući priliv stranog kapitala.¹⁰

Najveći broj SDI dolazi iz evropskih zemalja. Italija ulaže u automobilsku industriju, tekstilnu industriju, bankarstvo i osiguranje (*Fiat, Golden Lady, Intesa*). Austrijske SDI su plasirane u telekomunikaciju, bankarstvo, nekretnine, osiguranje

⁵ Stojanović, D. (2018): "Strane direktne investicije, izvoz i ekonomski rast u Srbiji", *Poslovna ekonomija*, 12(1), str. 54.

⁶ Stojanović, D. (2018): "Strane direktne investicije, izvoz i ekonomski rast u Srbiji", *Poslovna ekonomija*, 12(1), str. 62.

⁷ U.S. Department of State (2022): *2022 Investment Climate Statements: Serbia*, Belgrade, str. 3.

⁸ UN (2021): *The impact of COVID-19 on trade and structural transformation in Serbia*, United Nation: UNECE, str. 33.

⁹ Foreign investors council (2023): *Investiciona i poslovna klima*, Bela knjiga, <https://fic.org.rs/wp-content/uploads/2022/11/06-Investiciona-i-poslovna-klima.pdf> (15.07.2023).

¹⁰ Stojanovic, D., Ilic, B., Mihajlovic, D. (2017): "Strane direktne investicije u ostvarivanju ciljeva održivog razvoja lokalnih zajednica u Srbiji", *Ecologica*, 86(1), str. 265.

i proizvodnju plastičnih materijala (*Erste bank, Uniqa insurance, Raiffeisen bank, Porsche Holding*). Grčke SDI su u najvećem broju slučajeva usmerene u sektor banкарства (*Alpha bank, EFG Eurobank*) a norveške SDI u sektor telekomunikacija (*Yettel*). Francuska ulaže u bankarstvo, reklamne agencije kao i u prehrambenu industriju (*Michelin, Tarkett, BSA, Societe General, Segur Development*). Nemačke SDI su usmerene u više oblasti i to u farmaciju, komercijalne banke, automobilsku industriju, robne kuće, obradu metala, motore i generatore i drugu električnu opremu (*Stada Hemopharm, Metro AG, Siemens AG, IGB Holding, DM Drogerie*).¹¹ Osim ovih zemalja, SDI, ali u nešto manjem procentu, dolaze i iz Mađarske, Švajcarske, Španije, Slovenije i Turske.

Analizu kretanja SDI i njihovog uticaja na BDP, stopu nezaposlenosti i izvoz roba i usluga uz kontrolu uticaja inflacije započemo deskriptivnom statističkom analizom.

Tabela 1. Vrednosti deskriptivnih statistika za varijable Republike Srbije

	N	Mean	Std. Deviation	Median	Minimum	Maximum
Strane direktne investicije	10	3.2680	1.05876	3.1900	2.01	4.60
Bruto domaći proizvod	10	50.2070	8.20289	49.5150	39.66	63.50
Stopa nezaposlenosti	10	13.9340	4.51505	13.0950	9.01	22.10
Izvoz roba i usluga	10	25.1270	7.21816	23.9200	17.92	40.30
Inflacija	10	3.5900	3.54352	2.0500	1.10	12.00

Izvor: Kalkulacija autora na osnovu podataka World Bank

Na osnovu tabele 1 možemo videti numeričke karakteristike SDI, BDP, stope nezaposlenosti, izvoza robe i usluga i stope inflacije u vidu prosečne vrednosti, standardne devijacije, medijane, minimalne i maksimalne vrednosti, izračunate na osnovu podataka u periodu od 2013. do 2022. godine.

U cilju boljeg razumevanja posmatranih kretanja u nastavku rada sprovedaćemo korelacionu analizu sa Pirsonovim koeficijentom korelacije, koeficijentom parcijalne korelacije i testovima njihove značajnosti a zatim ćemo prikazati rezultate linearne regresione analize uticaja SDI na zavisno promenljive.

Tabela 2 nam pokazuje da je u posmatranom periodu registrovana sledeća povezanost promena u iznosu SDI:

- sa BDP imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje BDP) korelaciju koja je statistički značajna ($r=0,818$; $p=0,004<0,05$),
- sa stopom nezaposlenosti imamo jaku negativnu (povećanje SDI uzrokuje smanjenje stope nezaposlenosti) korelaciju koja je statistički značajna ($r=-0,875$; $p=0,001<0,05$),

¹¹ Blue Europe (2023): *Foreign Direct Investments (FDI) in Serbia: A review*, <https://www.blue-europe.eu/analysis-en/country-analysis/foreign-direct-investments-fdi-in-serbia-a-review/> (01.08. 2023).

- sa izvozom roba i usluga imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje izvoza roba i usluga) korelaciju koja je statistički značajna ($r=0,878$; $p=0,001<0,05$).

Tabela 2. *Pirsonov koeficijent korelacije SDI u Republici Srbiji sa zavisnim varijablama i inflacijom*

		Strane direktne investicije u Srbiji
Bruto domaći proizvod	r	.818
	p	.004
Stopa nezaposlenosti	r	-.875
	p	.001
Izvoz roba i usluga	r	.878
	p	.001
Inflacija	r	.298
	p	.403

Izvor: Kalkulacija autora na osnovu podataka World Bank

Nije zabeležena statistički značajna povezanost SDI sa stopom inflacije. Naime, registrujemo slabu pozitivnu korelaciju koja nije statistički značajna ($r=0,298$; $p=0,403>0,05$).

Tabela 3. *Parcijalna korelacija SDI sa zavisno promenljivim uz kontrolu inflacije u Republici Srbiji*

Inflacija kao kontrolna varijabla		Strane direktne investicije u Srbiji
Bruto domaći proizvod	r	.845
	p	.004
Stopa nezaposlenosti	r	-.903
	p	.001
Izvoz roba i usluga	r	.933
	p	.000

Izvor: Kalkulacija autora na osnovu podataka World Bank

Iz tabele 3 možemo videti da je, kada se u posmatranom periodu kontrolišu promene koje nastaju u stopi inflacije, registrovana sledeća povezanost promena u iznosu SDI:

- sa BDP imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje BDP) korelaciju koja je statistički značajna ($r=0,845$; $p=0,004<0,05$),
- sa stopom nezaposlenosti imamo jaku negativnu (povećanje SDI uzrokuje smanjenje stope nezaposlenosti) korelaciju koja je statistički značajna ($r=-0,903$; $p=0,001<0,05$),
- sa izvozom roba i usluga imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje izvoza roba i usluga) korelaciju koja je statistički značajna ($r=0,933$; $p=0,000<0,05$).

Na osnovu ove tabele mogli smo videti da nema statistički značajnih promena u rezultatu pri kontroli inflacije.

Tabela 4. Rezultati linearne regresione analize uticaja SDI na zavisno promenljive u Republici Srbiji

Zavisno promenljiva	B	R ²	p	95.0% Confidence Interval for B	
				Lower Bound	Upper Bound
Bruto domaći proizvod	6.337	.669	.004	2.703	9.971
Stopa nezaposlenosti	-3.731	.766	.001	-5.415	-2.048
Izvoz roba i usluga	5.986	.771	.001	3.326	8.646

Izvor: Kalkulacija autora na osnovu podataka World Bank

Povećanje SDI u Republici Srbiji za 1 milijardu dolara uzrokuje povećanje BDP-a za 6,337 milijardi dolara. To povećanje je statistički značajno ($p=0,004<0,05$) i kreće se od 2,703 do 9,971 milijardi dolara u 95% slučajeva. Takođe, zaključujemo da je 66,9% varijabiliteta BDP Republike Srbije određeno promenama u iznosu SDI.

Povećanje SDI u Republici Srbiju za 1 milijardu dolara uzrokuje smanjenje stope nezaposlenosti za 3,731%. To smanjenje je statistički značajno ($p=0,001<0,05$) i kreće se od 2,048% do 5,415% u 95% slučajeva. Takođe, zaključujemo da je 76,6% varijabiliteta stope nezaposlenosti Republike Srbije određeno promenama u iznosu SDI.

Povećanje SDI u Republici Srbiju za 1 milijardu dolara uzrokuje povećanje izvoza roba i usluga za 5,986 milijardi dolara. To povećanje je statistički značajno ($p=0,001<0,05$) i kreće se od 3,326 do 8,646 milijardi dolara u 95% slučajeva. Takođe, zaključujemo da je 77,1% varijabiliteta izvoza Republike Srbije određeno promenama u iznosu SDI.

Na osnovu analiziranih podataka za period od 2013. do 2022. godine došli smo do sledećih zaključaka:

- Postavljena hipoteza: „Postoji značajan direktan uticaj SDI na ključne makroekonomske varijable (BDP, stopu nezaposlenosti i izvoz roba i usluga) u Republici Srbiji“ **se pokazala kao tačna.**
- Postavljena hipoteza: „Posredstvom inflacije uticaj SDI na makroekonomske varijable se ne menja značajno u Republici Srbiji“ **se pokazala kao tačna.**

2.2. Uticaj stranih direktnih investicija na ključne makroekonomske varijable Republike Hrvatske (2013.-2022.)

Republika Hrvatska je 2013. godina postala članica Evropske unije što je u značajnoj meri poboljšalo njenu ekonomsku poziciju. Članstvo u EU omogućava Republici Hrvatskoj lakše dolaženje do neophodnih finansijskih sredstava, lakše privlačenje stranih investitora, obezbeđivanje najefikasnijih oblika proizvodnje ali i brži izlazak na veći broj tržišta. Najveći broj SDI dolazi iz Austrije, Italije,

Holandije, Nemačke i Luksemburga i one su pretežno usmerene u oblasti finansija, nekretnina, proizvodnje ali i trgovine na veliko i malo.¹²

Kao prednosti Republike Hrvatske za SDI, pored njenog članstva u EU, navodi se i njen povoljan geografski položaj i izlazak na Jadransko more. Takođe, kao prednost navodi se i niska inflacija, obučena radna snaga koja govori strane jezike, kvalitetna telekomunikaciona i energetska infrastruktura u koju država stalno ulaže. Tokom 2015. godine izvršena je i reforma poreskog sistema. Pored ovih brojnih prednosti koje Hrvatska pruža stranim investitorima tu se pojavljuje i određeni broj nedostataka. Ovde se prvenstveno misli na visok stepen korupcije, pravosudni sistem je spor a postoji i veliki odliv kvalifikovane radne snage. Članstvo u EU koje može biti prednost, može biti i nedostatak zbog zavisnosti zemlje od ekonomske situacije Evropske unije. Kako bi obezbedila što bolje uslove za privlačenje SDI Vlada Republike Hrvatske pokrenula je projekat „Pravda za posao“ koji ima za cilj poboljšanje poslovne klime. Zakon o promociji investicija donet je 2020. godine i on omogućava povraćaj poreza i davanje novčanih donacija preduzećima koja posluju u oblasti prerađivačke industrije.¹³

Analizu kretanja SDI i njihovog uticaja na BDP, stopu nezaposlenosti i izvoz roba i usluga uz kontrolu uticaja inflacije započecemo deskriptivnom statističkom analizom.

Tabela 5. Vrednosti deskriptivnih statistika za varijable Republike Hrvatske

	N	Mean	Std. Deviation	Median	Minimum	Maximum
Strane direktne investicije	10	1.9890	1.69507	1.2800	.04	4.66
Bruto domaći proizvod	10	59.7450	6.34342	59.2850	50.74	70.69
Stopa nezaposlenosti	10	11.1800	4.44367	9.8000	6.60	17.30
Izvoz roba i usluga	10	28.8670	6.44226	26.4850	22.98	43.04
Inflacija	10	1.7400	3.39287	.9500	-1.10	10.80

Izvor: Kalkulacija autora na osnovu podataka World Bank

U tabeli 5 možemo videti numeričke karakteristike SDI, BDP, stope nezaposlenosti, izvoza robe i usluga i stope inflacije u vidu prosečne vrednosti, standardne devijacije, medijane, minimalne i maksimalne vrednosti, izračunate na osnovu podataka u periodu od 2013. do 2022. godine.

U cilju boljeg razumevanja posmatranih kretanja sprovedemo korelacionu analizu sa Pirsonovim koeficijentom korelacije, koeficijentom parcijalne korelacije i testovima njihove značajnosti a zatim ćemo prikazati rezultate linearne regresione analize uticaja SDI na zavisno promenljive.

¹² Lloyds Bank, (2023): *Foreign direct investment (FDI) in Croatia*, <https://www.lloydsbanktrade.com/en/market-potential/croatia/investment> (10. 08. 2023).

¹³ Ibid.

Tabela 6. *Pirsonov koeficijent korelacije SDI u Republici Hrvatskoj sa zavisnim varijablama i inflacijom*

		Strane direktne investicije u Hrvatskoj
Bruto domaći proizvod	r	.837
	p	.003
Stopa nezaposlenosti	r	-.488
	p	.152
Izvoz roba i usluga	r	.701
	p	.024
Inflacija	r	.464
	p	.177

Izvor: Kalkulacija autora na osnovu podataka World Bank

Tabela 6 nam pokazuje da je u posmatranom periodu registrovana sledeća povezanost promena u iznosu SDI:

- sa BDP imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje BDP) korelaciju koja je statistički značajna ($r=0,837$; $p=0,003<0,05$),
- sa stopom nezaposlenosti imamo umerenu negativnu (povećanje SDI uzrokuje smanjenje stope nezaposlenosti) korelaciju koja nije statistički značajna ($r=-0,488$; $p=0,152>0,05$),
- sa izvozom roba i usluga imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje izvoza roba i usluga) korelaciju koja je statistički značajna ($r=0,701$; $p=0,024<0,05$).

Nije zabeležena statistički značajna povezanost SDI sa stopom inflacije. Naime, registrujemo umerenu pozitivnu korelaciju koja nije statistički značajna ($r=0,464$; $p=0,177>0,05$).

Tabela 7. *Parcijalna korelacija SDI sa zavisno promenljivim uz kontrolu inflacije u Republici Hrvatskoj*

Inflacija kao kontrolna varijabla		Strane direktne investicije u Hrvatskoj
Bruto domaći proizvod	r	.864
	p	.003
Stopa nezaposlenosti	r	-.359
	p	.342
Izvoz roba i usluga	r	.667
	p	.050

Izvor: Kalkulacija autora na osnovu podataka World Bank

Iz tabele 7 možemo videti da je, kada se u posmatranom periodu kontrolišu promene koje nastaju u stopi inflacije, registrovana povezanost promena u iznosu SDI:

- sa BDP imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje BDP) korelaciju koja je statistički značajna ($r=0,864$; $p=0,003<0,05$),

- sa stopom nezaposlenosti imamo umerenu negativnu (povećanje SDI uzrokuje smanjenje stope nezaposlenosti) korelaciju koja nije statistički značajna ($r=-0,359$; $p=0,342>0,05$).
- sa izvozom roba i usluga imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje izvoza roba i usluga) korelaciju koja je statistički značajna ($r=0,667$; $p=0,050<0,05$).

Na osnovu ove tabele mogli smo videti da nema statistički značajnih promena u rezultatu pri kontroli inflacije.

Tabela 8. Rezultati linearne regresione analize uticaja stranih direktnih investicija na zavisno promenljive

Zavisno promenljiva	B	R ²	p	95.0% Confidence Interval for B	
				Lower Bound	Upper Bound
Bruto domaći proizvod	3.132	.700	.003	1.461	4.802
Stopa nezaposlenosti	-1.280	.238	.152	-3.145	.586
Izvoz roba i usluga	2.663	.491	.024	.452	4.874

Izvor: Kalkulacija autora na osnovu podataka World Bank

Povećanje SDI u Republici Hrvatskoj za 1 milijardu dolara uzrokuje povećanje BDP-a za 3,132 milijardi dolara. To povećanje je statistički značajno ($p=0,003<0,05$) i kreće se od 1,461 do 4,802 milijardi dolara u 95% slučajeva. Takođe, zaključujemo da je 70% varijabiliteta BDP Republike Hrvatske određeno promenama u iznosu SDI.

Povećanje SDI u Republici Hrvatskoj za 1 milijardu dolara uzrokuje smanjenje stope nezaposlenosti za 1,280%. To smanjenje nije statistički značajno ($p=0,152>0,05$) i kreće se od -0,586% do 3,145% u 95% slučajeva. Takođe, zaključujemo da je 23,8% varijabiliteta stope nezaposlenosti Republike Hrvatske određeno promenama u iznosu SDI.

Povećanje SDI u Republici Hrvatskoj za 1 milijardu dolara uzrokuje povećanje izvoza roba i usluga za 2,663 milijardi dolara. To povećanje je statistički značajno ($p=0,024<0,05$) i kreće se od 0,452 do 4,874 milijardi dolara u 95% slučajeva. Takođe, zaključujemo da je 49,1% varijabiliteta izvoza Republike Hrvatske određeno promenama u iznosu SDI.

Na osnovu analiziranih podataka za period od 2013. do 2022. godine došli smo do sledećih zaključaka:

- Postavljena hipoteza: „Postoji značajan direktan uticaj SDI na ključne makroekonomske varijable (BDP, stopu nezaposlenosti i izvoz roba i usluga) u Republici Hrvatskoj“ **se pokazala kao tačna ali za vrednosti BDP i izvoz roba i usluga**. Kada posmatramo vrednosti stope nezaposlenosti ova hipoteza se pokazala kao netačna.
- Postavljena hipoteza: „Posredstvom inflacije uticaj SDI na makroekonomske varijable se ne menja značajno u Republici Hrvatskoj“ **se pokazala kao tačna**.

2.3. Uticaj stranih direktnih investicija na ključne makroekonomske varijable BiH (2013-2022.)

Od svih analiziranih zemalja priliv SDI najmanji je u BiH, a razlog su brojni problemi sa kojima se ova država susreće. Kao razlozi zašto strani investitori izbegavaju ulaganje u BiH navode se visok stepen korupcije, neefikasnost pravosudnih organa, veliki odliv mlade radne snage ali i složena zakonska regulativa. Sprovođenje reformi otežava podeljenost države na dva entiteta što dodatno komplikuje složenu zakonsku regulativu. Na nivou države nedostaje transparentnost u komercijalnim procedurama, posebno u javnim tenderima, što dodatno odbija strane investitore.

Vlada čini sve napore kako bi stvorila privlačan ambijent za strane investitore. Pokrenuta je procedura za izmenu Zakona o stranim ulaganjima, koji podrazumeva da domaći i strani investitori imaju jednak tretman, a osnovan je i *Fond za podršku stranim investitorima*. Takođe radi se i na donošenju zakona koji će stranim investitorima garantovati zaštitu od nacionalizacije i eksproprijacije, a procedura koja se odnosi na zapošljavanje stranih državljana u značajnoj meri je pojednostavljena.

Kao prednost BiH navodi se njen geopolitički položaj, između zapadne i istočne Evrope, kao i niz potpisanih sporazuma o slobodnoj trgovini. Takođe, BiH ima dobro razvijen bankarski sistem masu industrijskih zona kao i nizak nivo oporezivanja preduzeća. Reč je o najnižoj stopi poreza na dobit kompanija u ovom delu sveta i ona iznosi svega 10%.¹⁴

SDI najčešće su usmerene u proizvodnju koksa, refinisanih naftnih proizvoda, hemikalija i hemijskih proizvoda, trgovinu na veliko ali i u finansijske uslužne delatnosti. Poslednjih godina primetno je povećanje ulaganja u visokogradnju, proizvodnju odeće i vađenje metalnih ruda.

Analizu kretanja SDI i njihovog uticaja na BDP, stopu nezaposlenosti i izvoz roba i usluga uz kontrolu uticaja inflacije, u BiH, započemo deskriptivnom statističkom analizom.

Tabela 9. Vrednosti deskriptivnih statistika za varijable BiH

	N	Mean	Std. Deviation	Median	Minimum	Maximum
Strane direktne investicije	10	.4820	.12674	.4800	.31	.65
Bruto domaći proizvod	10	19.7960	2.65351	19.3950	16.40	24.53
Stopa nezaposlenosti	10	20.6500	5.71047	19.4500	14.10	27.50
Izvoz roba i usluga	10	7.6990	1.88351	7.1850	5.76	11.52
Inflacija	10	1.2500	4.62991	-.4500	-1.60	14.00

Izvor: Kalkulacija autora na osnovu podataka World Bank

Na osnovu tabele 9 možemo videti numeričke karakteristike SDI, BDP, stope nezaposlenosti, izvoza robe i usluga i stope inflacije u vidu prosečne vrednosti,

¹⁴ Zakon o porezu na dobit Federacije BiH ("Službene novine FBiH", br. 15/2016 i 15/2020), čl. 39.

standardne devijacije, medijane, minimalne i maksimalne vrednosti, izračunate na osnovu podataka u periodu od 2013. do 2022. godine.

U cilju boljeg razumevanja posmatranih kretanja u nastavku rada sprovedemo korelacionu analizu sa Pirsonovim koeficijentom korelacije, koeficijentom parcijalne korelacije i testovima njihove značajnosti a zatim ćemo prikazati rezultate linearne regresione analize uticaja SDI na zavisno promenljive.

Tabela 10. *Pirsonov koeficijent korelacije stranih direktnih investicija u BiH sa zavisnim varijablama i inflacijom*

		Strane direktne investicije u Bosni i Hercegovini
Bruto domaći proizvod	r	.797
	p	.006
Stopa nezaposlenosti	r	-.631
	p	.051
Izvoz roba i usluga	r	.825
	p	.003
Inflacija	r	.604
	p	.064

Izvor: Kalkulacija autora na osnovu podataka World Bank

Tabela 10 nam pokazuje da je u posmatranom periodu registrovana sledeća povezanost promena u iznosu SDI:

- sa BDP imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje BDP) korelaciju koja je statistički značajna ($r=0,797$; $p=0,006<0,05$),
- sa stopom nezaposlenosti imamo jaku negativnu (povećanje SDI uzrokuje smanjenje stope nezaposlenosti) korelaciju koja nije statistički značajna ($r=-0,631$; $p=0,051>0,05$). Ipak, ovde ne smemo odbaciti vezu koja nastaje, jer je realizovana značajnost samo neznatno veća od praga značajnosti, pa bi novo uzorkovanje moglo dati značajnu vezu.
- sa izvozom roba i usluga imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje izvoza roba i usluga) korelaciju koja je statistički značajna ($r=0,825$; $p=0,003<0,05$).

Nije zabeležena statistički značajna povezanost SDI sa stopom inflacije. Naime, registrujemo umerenu pozitivnu korelaciju koja nije statistički značajna ($r=0,604$; $p=0,064>0,05$). Iako i ovde povezanost investicija teorijski nije značajna, realizovana značajnost se samo neznatno razlikuje od praga značajnosti, pa uzimamo u obzir da bi novo uzorkovanje moglo dati statistički značajnu povezanost.

Iz tabele 11 možemo videti da je, kada se u posmatranom periodu kontrolišu promene koje nastaju u stopi inflacije, registrovana sledeća povezanost promena u iznosu SDI:

- sa BDP imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje BDP) korelaciju koja nije statistički značajna ($r=0,653$; $p=0,057>0,05$),
- sa stopom nezaposlenosti imamo umereno negativnu (povećanje SDI uzrokuje smanjenje stope nezaposlenosti) korelaciju koja nije statistički značajna ($r=-0,464$; $p=0,209>0,05$),
- sa izvozom roba i usluga imamo jaku pozitivnu (povećanje SDI uzrokuje povećanje izvoza roba i usluga) korelaciju koja nije statistički značajna ($r=0,740$; $p=0,023<0,05$).

Tabela 11. *Parcijalna korelacija SDI sa zavisno promenljivim uz kontrolu inflacije u BiH*

Inflacija kao kontrolna varijabla		Strane direktne investicije u Bosni i Hercegovini
Bruto domaći proizvod	r	.653
	p	.057
Stopa nezaposlenosti	r	-.464
	p	.209
Izvoz roba i usluga	r	.740
	p	.023

Izvor: Kalkulacija autora na osnovu podataka World Bank

Na osnovu tabele 11 možemo videti da kontrola stope inflacije nije uzrokovala značajnu promenu rezultata kod izvoza roba i usluga. Kada posmatramo stopu nezaposlenosti ona je potvrdila rezultat koji u direktnoj korelacionoj analizi nije bio konkluzivan. Naime, kontrolom stope inflacije dobijamo da povezanost SDI sa stopom nezaposlenosti zaista nije statistički značajna, što ukazuje da rezultat direktne korelacije čija značajnost je neznatno veća od praga značajnosti zaista pouzdano registruje da nema značajne povezanosti. U slučaju BDP imamo značajnu promenu rezultata. Naime, u direktnoj korelaciji dobili smo da je povezanost SDI i BDP jaka, pozitivna i statistički značajna, ali se pri kontroli uticaja stope inflacije ta korelacija smanjuje i uzrokuje da nema značajne povezanosti ($p=0,057>0,05$). Iako je realizovana značajnost neznatno veća od praga značajnosti pri analizi uticaja SDI na BDP BiH pored regresione analize vršićemo i analizu medijacije stope inflacije pri spomenutom uticaju kako bi dobili što pouzdanije rezultate.

Tabela 12. *Rezultati linearne regresione analize uticaja SDI na zavisno promenljive u BiH*

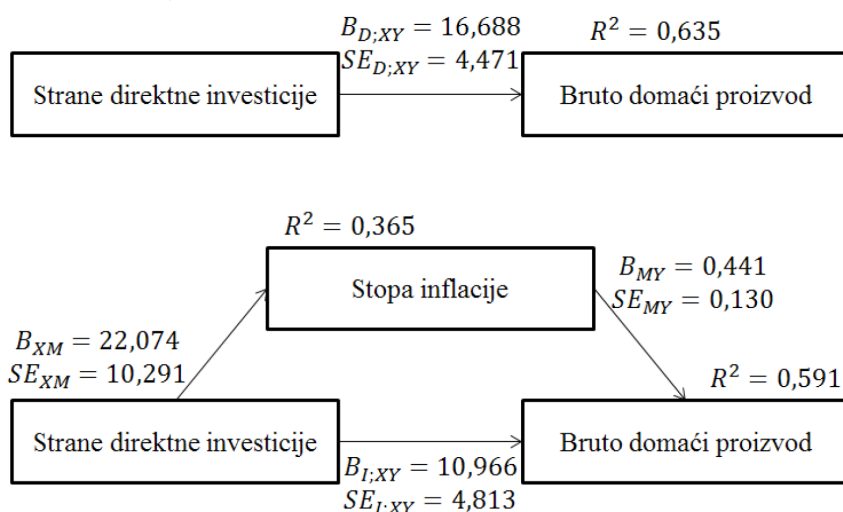
Zavisno promenljiva	B	R ²	p	95.0% Confidence Interval for B	
				Lower Bound	Upper Bound
Bruto domaći proizvod	16.688	.635	.006	6.379	26.997
Stopa nezaposlenosti	-28.417	.398	.051	-56.925	.091
Izvoz roba i usluga	12.267	.681	.003	5.427	19.107

Izvor: Kalkulacija autora na osnovu podataka World Bank

Povećanje SDI u BiH za 1 milijardu dolara uzrokuje povećanje izvoza roba i usluga za 12,267 milijardi dolara. To povećanje je statistički značajno ($p=0,003<0,05$) i kreće se od 5,427 do 19,107 milijardi dolara u 95% slučajeva. Takođe, zaključujemo da je 68,1% varijabiliteta izvoza BiH određeno promenama u iznosu SDI.

Povećanje SDI u BiH za 1 milijardu dolara uzrokuje smanjenje stope nezaposlenosti za 28,417%. To smanjenje nije statistički značajno ($p=0,051>0,05$) a kreće se od -0,091% do 56,925% u 95% slučajeva. Takođe, zaključujemo da je 39,8% varijabiliteta stope nezaposlenosti BiH određeno promenama u iznosu SDI. Iako je realizovana značajnost neznatno veća od praga značajnosti, u tabeli 12 je ovaj rezultat potvrđen kao pouzdan primenom parcijalne korelacione analize kontrolom stope inflacije kao faktora narušavanja uticaja.

Povećanje SDI u BiH za 1 milijardu dolara uzrokuje povećanje BDP za 16,688 milijardi dolara. To povećanje je statistički značajno ($p=0,006<0,05$) i kreće se od 6,379 do 26,997 milijardi dolara u 95% slučajeva. Takođe, zaključujemo da je 63,5% varijabiliteta BDP BiH određeno promenama u iznosu SDI. Sa druge strane, parcijalna korelacija sa kontrolom uticaja stope inflacije pokazala je da se značajnost povezanosti, tj. uticaja SDI u tom slučaju gubi. To ukazuje na moguću značajnu medijaciju stope inflacije pri tom uticaju, tj. da se značajan deo uticaja realizuje posredstvom stope inflacije. Da bismo upotpunili analizu medijacije vršimo i analizu indirektnog uticaja, tj. regresionu analizu modela u kojem su i SDI i stopa inflacije nezavisno promenljive, tj. prediktori BDP u BiH, kao i uticaj SDI na stopu inflacije.



Slika 1. Analiza medijacije stope inflacije pri uticaju SDI na BDP BiH

Izvor: Kalkulacija autora na osnovu podataka World Bank

Na slici 1 vidimo da je indirektan uticaj SDI na BDP manji u odnosu na direktan. Konkretno, povećanjem SDI za 1 milijardu dolara, BDP se povećava za 10,966 milijardi dolara i to povećanje nije statistički značajno ($p=0,057>0,05$) a kreće se od -0,415 do 22,348 u 95% slučajeva. Povećanje stope inflacije za 1% uzrokuje povećanje BDP za 0,441 milijardi dolara i to povećanje je statistički značajno ($p=0,009<0,05$) i kreće se od -0,052 do 0,571 u 95% slučajeva. Pri uticaju SDI na stopu inflacije pokazuje se da povećanje SDI za 1 milijardu dolara uzrokuje povećanje stope inflacije za 22,074% koje nije statistički značajno ($p=0,064>0,05$) a kreće se od -1,658 do 45,806 u 95% slučajeva. Dakle, direktna povezanost između SDI i BDP se gubi, kada se stopa inflacije uključi u model, pa je potvrđena puna medijacija.

Da bismo odredili da li je spomenuta medijacija statistički značajna vršimo Aroian test, jer iako nema značajnog uticaja SDI u modelu sa inflacijom, realizovana značajnost se tek neznatno razlikuje od praga značajnost.

$$|z| = \frac{B_{XM} \cdot B_{MY}}{\sqrt{B_{MY}^2 \cdot SE_{XM}^2 + B_{XM}^2 \cdot SE_{MY}^2 + SE_{XM}^2 \cdot SE_{MY}^2}}$$

$$= \frac{22,074 \cdot 0,441}{\sqrt{0,441^2 \cdot 10,291^2 + 22,074^2 \cdot 0,130^2 + 10,291^2 \cdot 0,130^2}} = 1.76$$

Realizovana vrednost Aroian testa je 1,76, manja je od kritične vrednosti 1,96 za prag značajnosti od 5%, što ukazuje da dobijena medijacija nije statistički značajna. Dakle, iako izvestan uticaj SDI na BDP biva realizovan posredstvom stope inflacije, možemo zaključiti da je taj uticaj značajan i direktno i uz kontrolu uticaja inflacije.

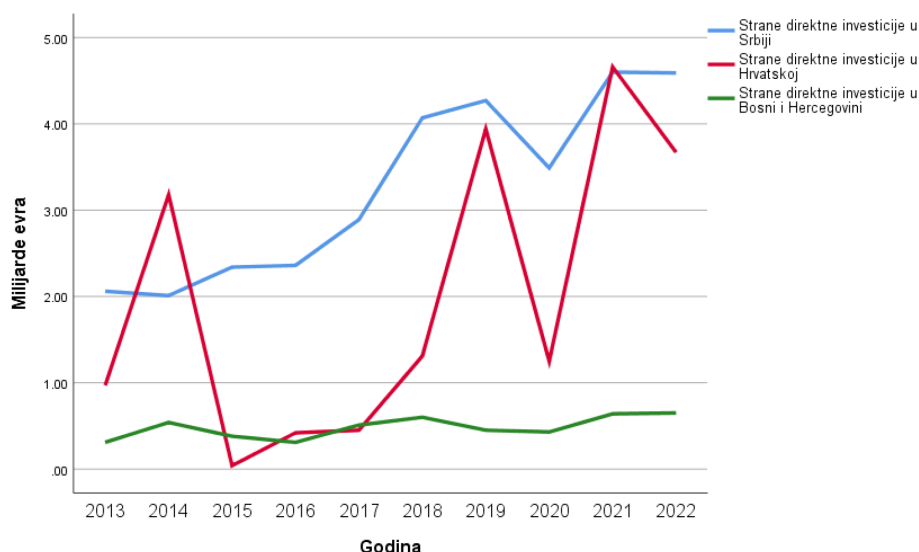
Relativna snaga medijatorskog modela iznosi 0,583, što ukazuje da se 58,3% uticaja SDI na BDP BiH realizuje posredstvom inflacije. Drugim rečima, inflacija umanjuje značaj pozitivnog uticaja SDI na BDP BiH.

Na osnovu analiziranih podataka za period od 2013. do 2022. godine došli smo do sledećih zaključaka:

- Postavljena hipoteza: „Postoji značajan direktan uticaj SDI na ključne makroekonomske varijable (BDP, stopu nezaposlenosti i izvoz roba i usluga) u BiH“ **se pokazala kao tačna ali za vrednosti BDP i izvoz roba i usluga.** Kada posmatramo vrednosti stope nezaposlenosti ova hipoteza se pokazala kao netačna.
- Postavljena hipoteza: „Posredstvom inflacije uticaj SDI na makroekonomske varijable se ne menja značajno u Republici Hrvatskoj“ **se pokazala kao tačna.**

3. GRAFIČKI PRIKAZ KRETANJA MAKROEKONOMSKIH VARIJABLI U ANALIZIRANIM ZEMLJAMA

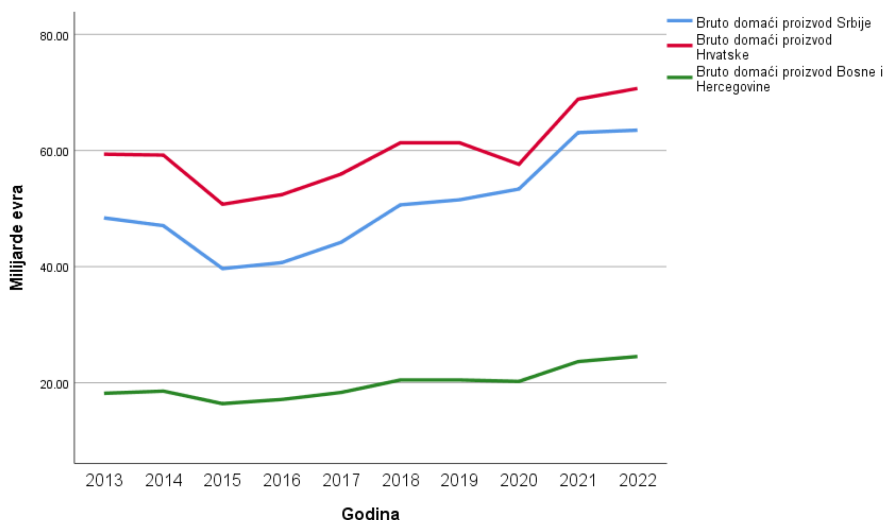
U ovom delu rada biće grafički, uz pomoć linijskih grafikona, prikazano kretanje SDI, BDP, stope nezaposlenosti, izvoza roba i usluga i inflacije u periodu od 2013. do 2022. godine u Republici Srbiji, Republici Hrvatskoj i BiH. Grafikoni su dobijeni na osnovu podataka koji su preuzeti sa zvaničnog sajta Svetske banke. Na jednom grafikonu prikazano je kretanje jedne makroekonomske varijable za sve tri analizirane zemlje, a sve u cilju jasnijeg prikazivanja njihovog kretanja u posmatranom periodu.



Grafikon 1. Kretanje SDI u analiziranim zemljama

Izvor: Kalkulacija autora na osnovu podataka World Bank

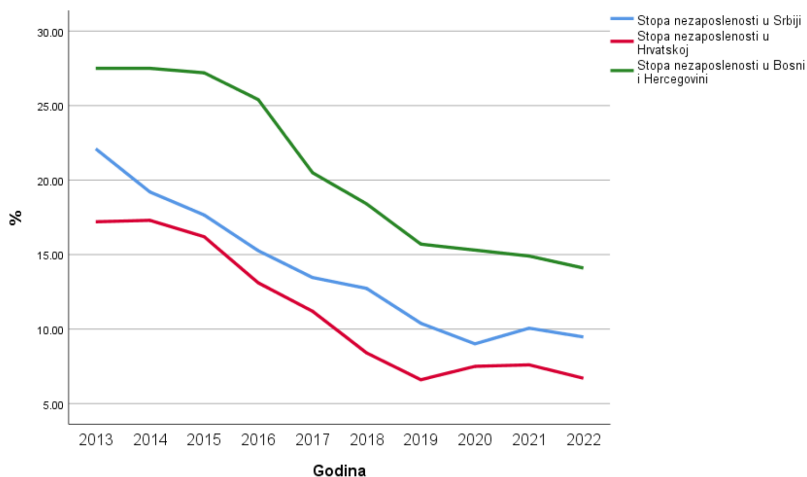
Na grafikonu 1 možemo videti da je u većini slučajeva iznos investicija najveći u Republici Srbiji, osim 2014. i 2021. godine kad je iznos investicija u Republici Hrvatskoj bio neznatno veći. Minimalni iznos investicija beleži BiH, osim 2015. i 2017. godine kada je minimalan iznos investicija zabeležen u Republici Hrvatskoj. Takođe, značajan varijabilitet investicija zabeležen je u Republici Hrvatskoj, gde se iznos investicija značajno menjao. Konstantan blagi rast iznosa investicija u Republici Hrvatskoj zabeležen je u periodu od 2015. do 2018. godine. Sa pojavom pandemije virusa Covid-19, primetan je pad iznosa investicija u Republici Srbiji i Republici Hrvatskoj.



Grafikon 2. Kretanje BDP u analiziranim zemljama

Izvor: Kalkulacija autora na osnovu podataka World Bank

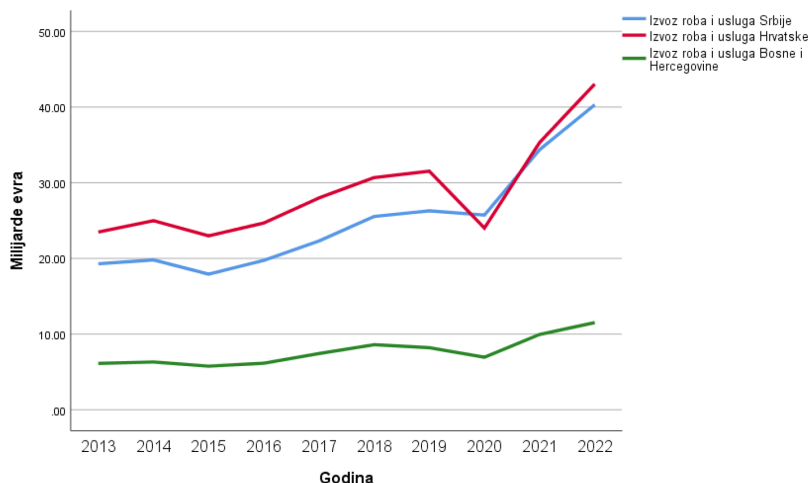
Na grafikonu 2 možemo videti da se po iznosu BDP, od sve ti analizirane zemlje, na prvom mestu nalazi Republika Hrvatska. Na drugom mestu, po iznosu BDP, je Republika Srbija, dok se na trećem mestu nalazi BiH. Ovde primećujemo da BDP u sve tri države ravnomerno raste od 2015. godine sa blagim padom 2020. godine koji je uzrokovan pandemijom virusa Covid-19. Adekvatnim merama, koje su Vlade ovih zemalja primenile u cilju ublažavanja ekonomskih posledica pandemije, BDP beleži blagi rast već 2021. godine.



Grafikon 3. Kretanje stope nezaposlenosti u analiziranim zemljama

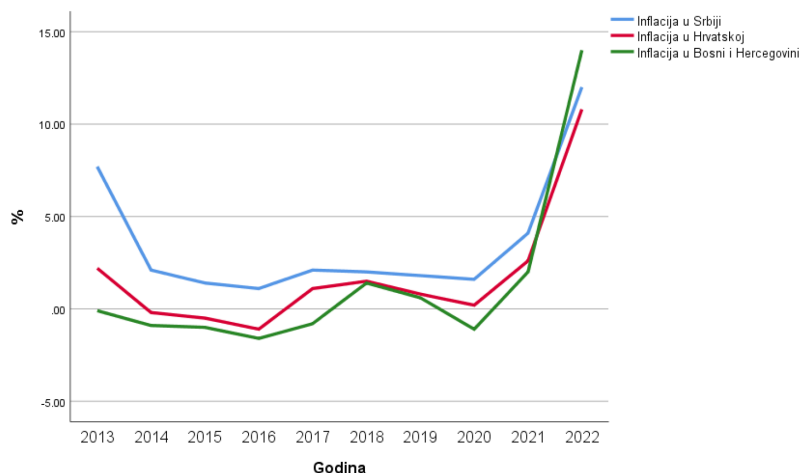
Izvor: Kalkulacija autora na osnovu podataka World Bank

Grafikon 3 nam pokazuje konstantan pad stope nezaposlenosti u sve tri analizirane zemlje. Do blagog rasta stope nezaposlenosti došlo je sa pojavom pandemije virusa Covid-19 ali se on nije dugo zadržao. Takođe, grafikon nam pokazuje i da je stopa nezaposlenosti najniža u Republici Hrvatskoj, što je i opravdano ako uzmemo u obzir da je ona članica EU.



Grafikon 4. Kretanje izvoza roba i usluga u analiziranim zemljama

Izvor: Kalkulacija autora na osnovu podataka World Bank



Grafikon 5. Kretanje inflacije u analiziranim zemljama

Izvor: Kalkulacija autora na osnovu podataka World Bank

Na grafikonu 4 možemo videti blagi rast izvoza roba i usluga u analiziranim zemljama u periodu od 2013. do 2022. godine. Tokom 2020. godine, kada se pojavila pandemija virusa Covid-19 i kada dolazi do zatvaranja granica i zabrane izvoza

deficitarnih proizvoda, izvoz roba i usluga beleži pad, što se na grafikonu jasno može primetiti. Adekvatnim merama, koje su Vlade sve tri zemlje primenile, izvoz roba i usluga beleži oporavak već 2021. godine. Do ponovnog pada izvoza roba i usluga, koji se na grafikonu ne može primetiti, dolazi krajem 2022. godine i on je izazvan ratom u Ukrajini.

Sa grafikona 5 vidimo da se stopa inflacije u proseku ne razlikuje u ove tri analizirane zemlje. Takođe, grafikon nam pokazuje i da se promene u stopi inflacije paralelno dešavaju sa promenama skorova ostalih varijabli, što nam ukazuje da kontrola inflacije neće značajno promeniti rezultate analize uticaja SDI na BDP, stopu nezaposlenosti i izvoz roba i usluga.

Posmatrani grafikoni nam jasno pokazuju da SDI, BDP i izvoz roba i usluga u posmatranom periodu beleže rast u Republici Srbiji, Republici Hrvatskoj i BiH. Takođe, stopa nezaposlenosti beleži pad u analiziranim zemljama u posmatranom periodu. Do pada vrednosti makroekonomskih varijabli dolazi početkom 2020. godine kada se pojavljuje pandemija virusa Covid-19 ali i 2022. godine kada počinje rat u Ukrajini.

4. ZAKLJUČAK

U Republici Srbiji, Republici Hrvatskoj i BiH, SDI predstavljaju najvažniji segment razvoja privrede. Vlade navedenih zemalja pokušavaju reformama svojih pravnih i ekonomskih sistema da stvore adekvatne uslove koji će privući stane investitore. Poseban akcenat u radu stavljen je na investicioni ambijent svake zemlje pojedinačno gde su prikazane njene ključne prednosti ali i nedostaci. Takođe, opisane su i aktivnosti koje su analizirane zemlje preduzele u cilju otklanjanja nedostataka investicionog ambijenta. Istraživanje je pokazalo da je u svim analiziranim zemljama neophodno izvršiti reformu pravosudnog sistema, smanjiti stepen korupcije, povećati transparentnost javnih nabavki ali i rešiti problem nepostojanja validnog katastarskog sistema. Pravni sistem Republike Srbije i BiH treba usaglasiti sa pravnim sistemom EU pošto obe zemlje teže priključivanju EU. Takođe, potrebno je obezbediti stabilno političko uređenje u kome je stabilna monetarna, fiskalna i budžetska politika. Poseban akcenat treba staviti na adekvatan raspored priliva SDI i usmeriti ih u pravcu proizvodnje a ne usluga kao što je do sada bio slučaj u svim analiziranim zemljama.

Pored svih slabosti i nedostataka priliv SDI u analiziranim zemljama beleži rast sve do pojave pandemije virusa Covid-19 početkom 2020. godine. Slična kretanja zabeležile su i analizirane makroekonomske varijable (BDP, stopa nezaposlenosti, izvoz roba i usluga i inflacija). Zahvaljujući adekvatnim merama koje su Vlade ovih zemalja preduzele u cilju ublažavanja ekonomskih posledica pandemije, trend rasta

nastavljen je već 2021. godine. Neke od posmatranih makroekonomskih varijabli beleže ponovo pad tokom 2022. godine što je posledica početka rata u Ukrajini.

U cilju dobijanja što realnije slike uticaja SDI na BDP, stopu nezaposlenosti i izvoz roba i usluga, u periodu od 2013. do 2022. godine, sprovedena je statističa SPSS analiza uz upotrebu odgovarajućih testova. Kao nezavisnu varijablu koristili smo SDI dok su zavisne varijable bile BDP, stopa nezaposlenosti i izvoz roba i usluga. Kao kontrolnu varijablu koristili smo inflaciju. Dobijeni rezultati prikazani su tabelarno i u obliku grafikona.

Na osnovu izvršene analize i dobijenih rezultata možemo **potvrditi** prvu posebnu (H1) hipotezu ali samo u Republici Srbiji. U Republici Hrvatskoj i BiH ova hipoteza se pokazala kao tačna kada posmatramo BDP i izvoz roba i usluga, ali ne i kada posmatramo stopu nezaposlenosti. Sprovedenom analizom **potvrdili** smo drugu posebnu (H2) hipotezu ali u sve tri analizirane zemlje.

Dodatne informacije i zaključci bi se mogli dobiti uzorkovanjem podataka na kvartalnom nivou i njihovom analizom. Takođe, detektovanje drugih latentnih varijabli sa značajnim indirektnim uticajem čije bi izučavanje moglo optimizovati planove investicija i njihova usmerenja.

Literatura

- Blue Europe, (2023): *Foreign Direct Investments (FDI) in Serbia: A review*, <https://www.blue-europe.eu/analysis-en/country-analysis/foreign-direct-investments-fdi-in-serbia-a-review/>.
- Foreign investors council, (2023): *Investiciona i poslovna klima*, Bela knjiga, <https://fic.org.rs/wp-content/uploads/2022/11/06-Investiciona-i-poslovna-klima.pdf>.
- Greene, J. E. (2018): *Using Macroeconomic and Structural Policies To Attain Macroeconomic Objectives*, World Scientific Book Chapters, pp. 183-212.
- Jensen, N. M. (2003): "Democratic governance and multinational corporations: Political regimes and inflows of foreign direct investment", *International Organization*, 57(3), str. 587.
- Lloyds Bank, (2023): *Foreign direct investment (FDI) in Croatia*, <https://www.lloydsbanktrade.com/en/market-potential/croatia/investment>.
- Mügge, D. (2016): "Studying macroeconomic indicators as powerful ideas", *Journal of European Public Policy*, pp. 410-427
- Stojanovic, D., Ilic, B., Mihajlovic, D. (2017): "Strane direktne investicije u ostvarivanju ciljeva održivog razvoja lokalnih zajednica u Srbiji", *Ecologica*, 86(1), str. 265.

- Stojanović, D. (2018): “Strane direktne investicije, izvoz i ekonomski rast u Srbiji”, *Poslovna ekonomija*, 12(1), str. 54.
- Stojanović, D. (2018): Strane direktne investicije, izvoz i ekonomski rast u Srbiji, *Poslovna Ekonomija*, 12(1), str. 62.
- The World Bank, (2023): *BiH Indicators*, <https://data.worldbank.org/country/bih>.
- The World Bank, (2023): *Croatia Indicators*, <https://data.worldbank.org/country/hr>.
- The World Bank, (2023): *Serbia Indicators*, <https://data.worldbank.org/country/RS>.
- U.S. Department of State, (2022): *2022 Investment Climate Statements: Serbia*, Belgrade, str. 3.
- UN, (2021): *The impact of COVID-19 on trade and structural transformation in Serbia*, United Nation: UNECE, str. 33.
- Veličković, M. (2019): *Strane direktne investicije kao faktor privrednog razvoja zemalja Zapadnog Balkana*, Doktorska disertacija, Univerzitet Edukons, Fakultet poslovne ekonomije: Sremski Karlovci, str. 45.
- Zakon o porezu na dobit Federacije BiH („Službene novine FBiH“, br. 15/2016 i 15/2020), čl. 39.

THE IMPACT OF FOREIGN DIRECT INVESTMENTS ON KEY MACROECONOMIC VARIABLES IN THE REPUBLIC OF SERBIA AND THE COUNTRIES OF THE REGION

Abstract: *Macroeconomic variables, as an indicator of the economic situation in a country, are the subject of increasing interest and they can significantly make it easier for us to understand the economic policy that a country is leading. Observing the movement of values macroeconomic variables, we can see how and in what way foreign direct investments (FDI) affect the economy of a country. FDI represents the most important segment of economic development, especially in developing countries such as the analyzed countries (Republic of Serbia, Republic of Croatia and Bosnia and Herzegovina). Today, these countries are making great efforts to make their investment environment attractive for foreign investors. Attracting adequate foreign investments and directing them to key economic branches is the basis for achieving economic development. Special attention in the paper is given to the impact of FDI on key macroeconomic variables (gross domestic product (GDP), unemployment rate and export of goods and services) while controlling the impact of inflation. All the data in the paper were processed with the help of the statistical program SPSS and presented in tables and graphs.*

Keywords: *foreign direct investment, gross domestic product, unemployment rate, export of goods and services, inflation rate, Covid-19 virus pandemic*

FORENZIČKO RAČUNOVODSTVO U DIGITALNOM OKRUŽENJU: TRENDVI I PROMENE

Sažetak: *Ispitivanje prevara privlači sve veću pažnju u novijoj literaturi. Digitalno okruženje značajno je promenilo prirodu prevara, koje postaju sve sofisticiranije i teže za otkrivanje. Ovaj rad analizira ulogu forenzičkog računovodstva u otkrivanju prevara u digitalnom okruženju. Naglašava se značaj primene naprednih tehnologija koje omogućavaju bržu i precizniju identifikaciju anomalija i tragova prevarnog ponašanja. Nalazi ukazuju da kombinacija tradicionalnih forenzičkih metoda i digitalnih analitičkih alata predstavlja ključ za efikasnije suprotstavljanje prevarama u savremenom poslovnom okruženju. Rad doprinosi razumevanju savremenih izazova i tendencija u oblasti forenzičkog računovodstva u eri digitalizacije.*

Ključne reči: *prevara, forenzičko računovodstvo, digitalno okruženje, napredne tehnologije, organizacija*

* Fakultet poslovne ekonomije, Univerzitet Educons, Sremska Kamenica, Srbija.
E-mail: stefan.milojevic@educons.edu.rs

Uvod

Finansijske prevare ostaju sveprisutan izazov u globalnoj ekonomiji, uzrokujući značajne ekonomske gubitke, narušavajući poverenje investitora i potkopavajući integritet finansijskih sistema. Rastuća složenost prevarnih šema, olakšana tehnološkim napretkom i globalizacijom je zahtevala evoluciju forenzičkog računovodstva kao specijalizovane discipline koja kombinuje finansijsku stručnost sa istražnim metodologijama. Forenzičko računovodstvo podrazumeva sistematsko ispitivanje finansijskih evidencija, obrazaca transakcija i struktura korporativnog upravljanja kako bi se otkrile i sprečile prevarne aktivnosti. Može se sagledati kao praksa ili profesija u prevenciji prevara i njihovoj detekciji (Bello, 2020). Široko se primenjuje u korporativnim istragama, podršci u sudskim postupcima, usklađenosti sa propisima i upravljanju rizicima. Forenzičko računovodstvo je, pored ostalog, bitna tema kada se razmatraju poreske prevare (Milojević, 2025). Tehnološke inovacije su dovele do transformacije tradicionalne uloge računovodstvenog informacionog sistema (Knežević et al., 2021a). Budućnost forenzičkog računovodstva se vidi kao obećavajuća, ali i izazovna. Očekuje se da će integracija veštačke inteligencije i prediktivne analitike značajno poboljšati mogućnosti otkrivanja prevara (Daraojimba et al., 2023).

Digitalno forenzičko računovodstvo je brzo rastuća oblast u modernom računovodstvu, koja kombinuje tradicionalne istražne metode sa najsavremenijom digitalnom tehnologijom kako bi se otkrile i sprečile finansijske prevare. Jedna vrsta prevare koja predstavlja veliku zabrinutost u korporativnom i organizacionom svetu je prevara na radu, što se odnosi na prevarna dela koja počinu zaposleni, menadžeri ili povezani insajderi sa namerom da steknu ličnu korist na račun organizacije. Prevaranti su postali sofisticiraniji. Danas oni koriste tehnologije poput VSAT uređaja, širokopojasne tehnologije, I-faksa, satelitskih telefona i mobilnih uređaja za preusmeravanje poziva i interneta kako bi sprovedli svoje prevarne šeme (Tukura, 2007).

Prvi deo rada posmatra poziciju forenzičkog računovodstva u okruženju. Drugi deo rada se bavi uticajem digitalizacije na upravljanje rizikom od prevarnih radnji. Treći deo rada je posvećen razvoju sajber forenzičkog računovodstva. Na kraju slede zaključna razmatranja.

1. Forenzičko računovodstvo i okruženje

Informacioni sistem ima ključnu ulogu u procesu poslovno-finansijskog odlučivanja u savremenom društvu (Mitrović et al., 2025). Jedan od sistema informisanja jeste i računovodstvo, koje u kontinuitetu evoluiru i stiče moderne

karakteristike. Isto važi i za forenzičko računovodstvo koje se razvija u savremenom poslovnom okruženju, koje karakterišu digitalna transformacija, globalizacija i sve veća organizaciona složenost. I u digitalnom okruženju, računovodstveni informacioni sistemi pokazuju mogućnosti za prevarne aktivnosti (Mitrović & Knežević, 2020). Veliki finansijski skandali u poslovanju su doveli do toga da se poveća svest javnosti o zloupotrebama i prevarama, s jedne strane, i pojačanoj potrebi za uslugama forenzičkog računovodstva, s druge strane (Botes & Saadeh, 2018). U kontekstu finansijske bezbednosti se ističe važnost anagažovanja forenzičkih računovođa i forenzičkih revizora, posebno od strane vlasnika ili menadžera u kompanijama. Primer forenzičkog izveštaja se može videti u radu pod nazivom “Strengthening corporate financial resilience: comprehensive fraud examination report”, autora, Milojević, Knežević I Beke Trivunac (2025).

Postoje različite definicije koje su usmerene na razjašnjavanje koncepta forenzičkog računovodstva i potrebnu stručnost u funkciji postizanja uspeha u ovom segmentu. Prema užem pristupu, forenzičko računovodstvo je nauka koja se bavi primenom računovodstvenih činjenica prikupljenih metodama i postupcima revizije radi rešavanja pravnih problema (Siegel & Shim, 2010), i razvilo se kao odgovor na preplitanje pravnih i finansijskih pitanja u poslovnim aktivnostima (Aksoy & Uzay, 2021). Prema širem pristupu, forenzičko računovodstvo sa sagledava kroz usluge koje uključuju primenu specijalizovanog znanja i istraživačkih veština koje poseduju ovlašćene računovođe (CPA) radi prikupljanja, analize i procene dokaznog materijala, kao i za tumačenje i saopštavanje nalaza u sudnici, sali za sastanke ili drugim pravnim ili administrativnim prostorijama (AICPA, 2011). Uprkos stalno rastućem broju znanja o forenzičkom računovodstvu, Huber (2012) je istakao mišljenje da je termin forenzičkog računovodstva loše definisan. Forenzičko računovodstvo je nedovoljno razvijena oblast u obrazovanju i praksi, a to se posebno odnosi na Srbiju (Mitrić et al., 2012). Potrebno je sagledati kakvu ulogu revizorska profesija ima u otkrivanju prevara, posebno ako se ima u vidu sve složenije ekonomsko okruženje i pojava novih vrsta prevara (Knežević et al., 2019). Prevara je i dalje sveprisutna briga mnogih, a među njima se ističu računovođe, revizori i stručnjaci za borbu protiv prevara (Milojević et al., 2024).

Pored toga što sajber kriminal rezultira krađom imovine i gubitkom poslovanja, on i šteti ugledu kompanije, što zauzvrat može uticati na vrednost kompanije na tržištu akcija (Smith et al., 2019). Sa povećanjem broja incidenata finansijskog sajber kriminala, raste i potreba za efikasnim alatima za otkrivanje ovih incidenata (Alshurafat et al., 2024). IT forenzički računovodstveni alati se danas u sve većoj meri prepoznaju kao efikasni alati za otkrivanje finansijskog sajber kriminala.

„Ton na vrhu“ je način na koji upravni odbor kompanije, viši menadžment i generalni direktor doživljavaju svoje odgovornosti u postavljanju tona organizacije,

pri čemu se ističu kao posebno važne njihove lične vrednosti (Soltani, 2014). Postoji bojazan zbog toga što menadžment u želji da ostvari lične ciljeve, može da dođe u situaciju da sprovodi razne vidove manipulacija kako bi obmanjivao korisnike finansijskih informacija (Petrović et al., 2025). Generalni direktori svojim rečima i delima postavljaju etički ton organizacijama. U tom kontekstu, logično je konstatovati da svi oni koji su uključeni u kompaniju traže smernice od vrha (Schwartz et al. 2005), dok Hambrick (2007) navodi da, ako želimo da razumemo zašto organizacije rade stvari koje rade ili zašto rade onako kako rade, moramo uzeti u obzir predrasude i sklonosti njihovih najmoćnijih aktera – njihovih vrhovnih rukovodilaca.

2. Digitalne tehnologije i rizik od prevarnih radnji

Digitalizacija je ostavila snažan uticaj na razvoj računovodstvene profesije. Brzi tehnološki razvoj iz ugla automatizacije i digitalizacije je doveo do toga da mašine zamene ljudski rad (Spasić et al., 2024). Pojava složenih digitalnih finansijskih sistema je rezultirala razvojem novih oblika prevarnih radnji koji su sve softiciraniji, što je zahtevalo promenu tehnika forenzičkog računovodstva. Bihevioralne nauke imaju sve veću ulogu u otkrivanju prevarnih radnji. Spoj bihevioralnih nauka i informacionih tehnologija omogućava dublje razumevanje ljudskog ponašanja u digitalnom okruženju. U tom kontekstu, kako Glogić (2025a) ističe, neuroforenzika ne predstavlja zamenu za tradicionalno računovodstvo, već je to njegova neophodna evolutivna nadogradnja u 21. veku.

Razvoj digitalne tehnologije pruža značajnu dodatnu vrednost u optimizaciji otkrivanja prevara. Sa dubljim razumevanjem ovih tehnika, organizacije mogu poboljšati svoje sisteme interne kontrole i izgraditi jaču kulturu borbe protiv prevara. Jedna od ključnih transformacija u savremenoj praksi forenzičkog računovodstva odnosi se na primenu tehnika analitike velikih podataka. Ovo je posebno važno jer dovodi do poboljšanja sposobnosti identifikovanja anomalija i obrazaca koji mogu ukazivati na prevarne aktivnosti u organizacijama (Kılıç, 2020), a to je posebno korisno kod identifikovanja prevarnog finansijskog izveštavanja. Paralelno s tim, integracija informaciono-komunikacionih tehnologija (IKT) u forenzičko računovodstvo značajno je unapredila efikasnost istražnih procesa, jer su alati zasnovani na ovim tehnologijama doprineli povećanju brzine i preciznosti otkrivanja prevara tokom forenzičkih istraga (Akinbowale, 2018). Njihova primena dovodi i do obezbeđivanja pouzdanih dokaza za potrebe finansijskog izveštavanja i sudskih postupaka.

Blokčejn se može sagledati kao granična digitalna tehnologija koja pruža nove mogućnosti za inovacije (Li & Xu, 2025). Ova tehnologija se takođe pojavila kao

potencijalno rešenje za finansijske prevare, a nekoliko studija je analiziralo njen uticaj na prakse forenzičkog računovodstva. Iako blokčejn poboljšava transparentnost, on takođe predstavlja izazove u vezi sa usklađenošću sa propisima i anonimnošću transakcija koje se odnose na kriptovalute, koje prevaranti mogu iskoristiti za nezakonite finansijske aktivnosti. Kako Aman (2024) ističe, atribut „blokčejn“ pomaže forenzičkim računovođama da prate transakcije iz razloga što su svi akti javni i lako revidirani, odnosno on osigurava integritet podataka smanjujući mogućnost manipulacije, tako da je to od velikog značaja za forenzičke istrage.

Prateći savremenu literaturu, jasno je da je forenzičko računovodstvo prošlo kroz značajnu transformaciju zbog napretka digitalne tehnologije. Savremeno digitalno okruženje karakterišu nove mogućnosti, ali ne samo za jednu, već za obe strane. Naime, ova konstatacija se odnosi kako na počinioc prevarnih radnji, tako i na istražitelje koji iste otkrivaju. U ovom kontekstu se ističe da je digitalizacija u značajnoj meri uticala na promenu načina na koji istražitelji prevara sprovode istragu, što je argumentovano time da se oblici prevara sada pomeraju u digitalnu sferu, čineći tradicionalne metode forenzičkog računovodstva manje relevantnim bez tehnološke podrške. Blokčejn, analiza podataka i sajber forenzika su sada ključni elementi u otkrivanju prevara jer mogu transparentno i efikasno da prate transakcije. Veštačka inteligencija i mašinsko učenje su ključni za otkrivanje prevara u realnom vremenu. Ova tehnologija je sposobna da prepozna sumnjive obrasce transakcija koje je ljudima teško otkriti.

Primena digitalnih tehnologija u forenzičkom računovodstvu zahteva visok nivo stručnosti i tehnološke pismenosti (Glogić, 2025b). Naime, potrebno je da forenzičke računovođe steknu stručnost u digitalnoj forenzici i sajber bezbednosti kako bi efikasno istražili sajber kriminal u finansijama. Tradicionalne metode forenzičkog računovodstva više nisu dovoljne u otkrivanju sajber finansijskih prevara zbog složenosti i brzine digitalnih transakcija. Nedavno su Ofoeda et al. (2022) predložili da forenzičko računovodstvo mora integrisati protokole za sajber bezbednost, otkrivanje anomalija vođeno veštačkom inteligencijom i analitiku blokčejna kako bi se poboljšale istrage sajber prevara.

Brzi napredak tehnologija veštačke inteligencije transformisao je različite sektore, uključujući finansije i računovodstvo. Računovodstvena profesija je značajno pod uticajem veštačke inteligencije. Primenom pravog pristupa veštačka inteligencija može ojačati poziciju računovođa kao strateških partnera, s jedne strane i pokrenuti održivi rast u poslovnom svetu, s druge strane (Aprida et al., 2025). Kao primer dobre prakse, navodi se JP Morgan Chase & Co, jedna od najvećih finansijskih institucija u svetu koja je implementirala algoritme veštačke inteligencije i mašinskog učenja u svrhu unapređenja sistema za otkrivanje prevara (Sabbani, 2023; Dobrovoljska & Rozhkova, 2024). Banka koristi velike jezičke modele (Large

Language Model - LLM) i tehnike mašinskog učenja za analizu *nestrukturisanih podataka* (npr. e-mejllova) i identifikovanje potencijalno prevarnih obrazaca u porukama.

Među bezbrojnim primenama veštačke inteligencije, njena uloga u otkrivanju kreativnih računovodstvenih praksi privukla je značajnu pažnju istraživača i praktičara. Kreativno računovodstvo, koje karakteriše manipulacija finansijskim izveštajima kako bi se predstavila povoljnija slika finansijskog zdravlja kompanije, predstavlja značajne rizike za zainteresovane strane, uključujući investitore, regulatore i širu ekonomiju. Tradicionalne metode otkrivanja često se oslanjaju na ručne revizije i heurističke pristupe, koji mogu oduzimati mnogo vremena i biti skloni ljudskim greškama. Nasuprot tome, veštačka inteligencija nudi potencijal za poboljšanu tačnost i efikasnost kroz analizu zasnovanu na podacima i prepoznavanje obrazaca (Kamau & Kinyua, 2025).

3. Razvoj sajber forenzičkog računovodstva

Istraga sajber kriminala je usmerena na ispitivanje navodnih prevarnih aktivnosti koje su se odvijale na mreži ili su se odnosile na neovlašćeni pristup računarskom sistemu neke organizacije (Akinbowale et al., 2023). Sajber forenzičko računovodstvo, kako ga definiše Hossain (2023), odnosi se na korišćenje principa forenzičkog računovodstva u svrhu istraživanja i sprečavanja sajber kriminala. Sajber forenzičko računovodstvo se u sve većoj meri percipira kao ključno u analizi sajber kriminala i identifikaciji počinitelja, a uključuje korišćenje različitih tehnika kao što su analiza podataka, digitalna forenzika i finansijske istrage u cilju identifikovanja izvora sajber napada i povraćaja ukradene imovine.

Sajber forenzičko računovodstvo se posmatra kroz noviji razvoj koji se fokusira na istraživanje i sprečavanje finansijskih prevara počinjenih putem interneta, uključujući fišing, hakovanje i krađu identiteta (Akinbowale et al., 2020). Drugim rečima, sajber forenzičko računovodstvo ispituje i pokušava da zaustavi sajber kriminal poput krađe identiteta, hakovanja i prevara putem e-pošte koje uključuju novac. Stoga, forenzičko računovodstvo zahteva tehnološko jačanje na kontinuiranoj osnovi i globalnu saradnju (Moid, 2018).

Sajber forenzičko računovodstvo je proučavanje finansijskog kriminala u sajber prostoru (Akinbowale et al., 2020). Stoga, očekuje se usvajanje novih, posebnih veština u digitalnoj forenzici, analizi podataka i istrazi sajber kriminala (Haddad et al., 2024). Knežević et al. (2021) navode da unapređivanje upravljanja rizikom od nastanka prevarnih radnji treba razvijati kroz jačanje kapaciteta forenzičkog računovodstva preko obrazovnog sistema, kao i putem poboljšanja veština

forenzičkih računovođa. Pored toga, potrebna je naglasiti i značaj transformacija u kontekstu strategijskog finansijskog menadžmenta i kontrole, kako bi organizacije mogle da odgovore na kompleksne izazove u okruženju (Milošević et al., 2023). Potrebni su veliki napori kako bi se efikasno upravljalo rizicima od sajber prevara, posebno ako se ima u vidu činjenica da se sajber rizici menjaju u kontinuitetu, a hakeri postaju pametniji. U takvim okolnostima, forenzičkim računovođama je teško da identifikuju i zaustave sajber prevare ukoliko ne promene svoje metode istrage i alate. Ako se tome doda i to da su kriptovalute i blokčejn tehnologija forenzičkom računovodstvu pružile i nove prepreke, situacija postaje još kompleksnija. Postoji zabrinutost kod stručnjaka i naučnika u smislu da bi napredak informacione tehnologije mogao da ometa efikasnu primenu veštačke inteligencije u forenzičkom računovodstvu. To bi za posledicu moglo da ima ometanje pokušaja borbe protiv finansijskih prevara (Zemánková, 2019).

Zaključak

Forenzičke računovođe igraju ključnu ulogu u otkrivanju finansijskih prevara posebno u velikim korporacijama gde su prevarne šeme često složene, ali i veoma dobro prikrivene. U savremenom digitalnom okruženju, od forenzičkih računovođa se očekuje da, pored toga što treba da raspolazu temeljnim znanjem kada su u pitanju računovodstveni i revizorski principi, raspolazu i naprednim kompetencijama iz oblasti računarskih tehnologija, kao i analitike velikih skupova podataka. Prvo, potrebna je interdisciplinarna integracija između informacione tehnologije i računovodstva kako bi se forenzičkim stručnjacima omogućilo da razumeju algoritme veštačke inteligencije, principe blokčejna i tehnike analize velikih podataka. Drugo, finansijske institucije i revizori moraju da investiraju u platforme za forenzičku analitiku koje podržavaju automatizovano otkrivanje i digitalno izveštavanje. Forenzički podaci i analitika velikih podataka mogu poboljšati efikasnost istraga digitalnih finansijskih izveštaja, pod uslovom da je kvalitet analiziranih podataka zagarantovan. Znači, spoj znanja iz informacionih tehnologija i računovodstvene forenzike je preduslov za unapređenje upravljanja rizikom od prevarnih radnji u savremenom okruženju. Bitno je naglasti i to da, sajber forenzičko računovodstvo predstavlja još jedan novi trend koji postaje sve važniji.

Iako blokčejn ima značajan potencijal u sprečavanju prevara, njegova puna integracija u forenzičko računovodstvo zahteva dalja istraživanja i regulatorni razvoj. Korporacije traže robusne mehanizme za otkrivanje prevara, a forenzičko računovodstvo se pojavilo kao ključni alat za obezbeđivanje finansijske transparentnosti i odgovornosti. Tradicionalni pristupi otkrivanju kreativnog

računovodstva pretežno su se oslanjali na modele zasnovane na obračunskom načelu i analizi finansijskih pokazatelja kako bi otkrili menadžerske manipulacije ugrađene u finansijske izveštaje. Ove osnovne tehnike, razvijene mnogo pre integracije veštačke inteligencije i napredne analitike, ostaju ključne za razumevanje kako se upravljanje zaradom istorijski merilo i tumačilo.

Literatura

- AICPA (2011). "The 2011 forensic and valuation services (FVS) trend survey", American Institute of Certified Public Accountants (AICPA), available at: <https://www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/PractAidsGuidance/DownloadableDocuments/2011%20FVS%20Trend%20Survey.pdf> (30.03.2024).
- Akinbowale, O. E. (2018): "Information communication technology and forensic accounting in Nigeria". *International Journal of Business and Finance Management Research*, 6/2018, 1-7.
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020): "An innovative approach in combating economic crime using forensic accounting techniques". *Journal of Financial Crime*, 27/2020, 1253- 1271.
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023): „Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation". *Cogent Economics & Finance*, 11/2023, 2153412.
- Aksoy, T., & Uzay, S. (2021): "Relationship between fraud auditing and forensic accounting". In *Auditing Ecosystem and Strategic Accounting in the Digital Era: Global Approaches and New Opportunities* (pp. 127-146). Cham: Springer International Publishing.
- Alshurafat, H., Shbail, M. O. A., & Almuqiet, M. (2024): "Factors affecting the intention to adopt IT forensic accounting tools to detect financial cybercrimes". *International Journal of Business Excellence*, 33/2024, 169-190.
- Aman, Q. U. I. S. E. R. (2024): "From data to discovery: The impact of technology on forensic accounting. *Ile Journal of Law and Forensic Science*", 2/2024, 1-13.
- Aprida, A., Asmita, D. Y., Lidia, W. O., & Nofryanti, N. (2025): "Digitalization and AI as Drivers of Change in the Accounting Profession: Opportunities for Innovation and Ethical Issues". *TOFEDU: The Future of Education Journal*, 4/2025, 4954-4961.
- Bello, U. (2020): "The effects of forensic accounting technology on fraud detection in Nigeria". *Nile Journal of Business and Economics*, 6/2020, 16-26.

- Botes, V., & Saadeh, A. (2018): "Exploring evidence to develop a nomenclature for forensic accounting". *Pacific Accounting Review*, 30/2018, 135-154.
- Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2023): "Forensic accounting in the digital age: a US perspective: scrutinizing methods and challenges in digital financial fraud prevention". *Finance & Accounting Research Journal*, 5/2023, 342-360.
- Dobrovolska, O., & Rozhkova, M. (2024): "The Impact of Digital Transformation on the Anti-Corruption and Cyber-Fraud System". *Business Ethics and Leadership*, 8/2024, 231-252.
- Glogić, E. (2025a): "Neuroforenzičko računovodstvo kao nova naučna paradigma ili pseudonaučni trend", II međunarodna naučno – istraživačka konferencija, ISRCFA 2025 - "Forenzičko računovodstvo i revizija u doba vještačke inteligencije, kriptoomovine i održivosti - integritet dokaza, regulativa i granice odgovornosti", Tuzla, 28.11. 2025, Zbornik radova ISRCFA, ISSN 3029-4614, pp. 32-51.
- Glogić, E. (2025b): "Digitalizacija i forenzičko računovodstvo: novi alati u detekciji finansijskih prevara", Peti naučni skup „Računovodstvena znanja kao činilac ekonomskog i društvenog napretka, 17. jun 2025. Ekonomski fakultet u Kragujevcu, Zbornik radova, ISBN: 978-86-6091-167-6, str. 593-608.
- Haddad, H. O. S. S. A. M., Alharasis, E. E., Fraij, J., & Al-Ramahi, N. M. (2024): "How do innovative improvements in forensic accounting and its related technologies sweeten fraud investigation and prevention". *WSEAS Transactions on Business and Economics*, 21/2024, 1115-1141.
- Hambrick, D. C. (2007): "Upper echelons theory: An update". *Academy of Management Review*, 32/2007, 334–343.
- Hossain, M. Z. (2023): "Emerging trends in forensic accounting: Data analytics, cyber forensic accounting, cryptocurrencies, and blockchain technology for fraud investigation and prevention". *Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention*. <http://dx.doi.org/10.2139/ssrn.4450488> (16.05.2023)
- Huber, W. D. (2013): "Should the forensic accounting profession be regulated?". *Research in Accounting Regulation*, 25/2013, 123–132, doi:10.1016/j.racreg.2012.11.006
- Kamau, C. G., & Kinyua, N. N. (2025): "Application of Artificial Intelligence in Detecting Creative Accounting Tendencies Among Corporations in Kenya". *African Journal of Commercial Studies*, 6/2025, 103-112.
- Kılıç, B. İ. (2020): "The effects of big data on forensic accounting practices and education". In *Contemporary issues in audit management and forensic accounting* (pp. 11-26). Emerald Publishing Limited. <https://dx.doi.org/10.1108/s1569-375920200000102005>

- Knežević, S., Milojević, S., & Paunović, J. (2021): "Razvoj forenzičkog računovodstva i izazovi u savremenom okruženju", *Revizor - Časopis za upravljanje organizacijama, finansije i reviziju*, 24/2021, 77–90.
- Knežević, S., Mitrović, A., & Cvetković, D. (2019): "The role of auditing profession in detecting frauds in financial statements". *NBP. Nauka, bezbednost, policija*, 24/2019, 97-109.
- Knežević, S., Obradović, T., Mitrović, A., & Milašinović, M. (2021a): "Računovodstveni informacioni sistemi u digitalnom okruženju". *Skup privrednika i naučnika, Industrija 4.0 – mogućnosti, izazovi i rešenja za digitalnu transformaciju privrede*, Zbornik radova: Industrija 4.0 – mogućnosti, izazovi i rešenja za digitalnu transformaciju privrede (str. 390-398). Beograd: Fakultet organizacionih nauka.
- Li, Z., & Xu, Z. (2025): "Digital technology and innovation: The impact of blockchain application on enterprise innovation". *Technovation*, 139/2025, 103136.
- Milojević, S. (2025): "Forenzičko računovodstvo i oporezivanje". *Megatrend revija*, 22/2025, 1-14.
- Milojević, S. V., & Knežević, S. P., Šebek, V. (2024): "Identifikacija i sprečavanje prevarnog finansijskog izveštavanja". *Tokovi osiguranja*, 1/2024, 146-163.
- Milojević, S., Knežević, S., & Beke-Trivunac, J. (2025): "Strengthening corporate financial resilience: Comprehensive fraud examination report". *International Review*, 1-2/2025, 162-171.
- Milošević, M., Stojiljković, M., Raičević, J., & Milojević, S. (2023): "Obrazovanje i obuka u oblasti strateškog finansijskog menadžmenta i kontrole: U kom pravcu Vol. 22, № 1, 2025: 1-1614 Stefan Milojević bi trebalo da idemo?", *Revizor - Časopis za upravljanje organizacijama, finansije i reviziju*, 26/ 2023, 25–36.
- Mitrić, M., Stanković, A., & Lakićević, A. (2012): "Forensic Accounting – the Missing Link in Education and Practice". *Management*, 17/2012, 41-50, 0.7595/management.fon.2012.0032
- Mitrović, A., & Knežević, S. (2020): "Fraud and forensic accounting in the digital environment of accounting information systems: focus on the hotel industry". In *Tourism International Scientific Conference Vrnjačka Banja – TISC, Proceedings*, 5(1), pp. 281-295.
- Mitrović, A., Milašinović, M., & Knežević, S. (2025): "Accounting Information System and Organizational Performance: Evidence from Serbian Small & Medium-Sized Enterprises in the COVID-19 Crisis". In: *Research at the Crossroad of Finance, Marketing and Operations for Sustainable Business*, pp. 34-59.
- Moid, S. (2018): "Fighting Cyber Crimes Using Forensic Accounting: A Tool to Enhance Operational Efficiency". *Wealth: International Journal of Money, Banking & Finance*, 7/2018, 93-99.

- Ofoeda, I. (2022): "Anti-money laundering regulations and financial inclusion: empirical evidence across the globe". *Journal of Financial Regulation and Compliance*, 30/2022, 646-664.
- Petrović, D., Milošević, M., Adamović, M., Miložićić, M. (2025): "Razvoj forenzičkog računovodstva i trendovi u savremenom poslovnom okruženju", II međunarodna naučno – istraživačka konferencija, ISRCFA 2025 - "Forenzičko računovodstvo i revizija u doba vještačke inteligencije, kriptoomovine i održivosti - integritet dokaza, regulativa i granice odgovornosti", Tuzla, 28.11. 2025, Zbornik radova ISRCFA, ISSN 3029-4614, pp. 546-563.
- Sabbani, G. (2023): "AI in Credit Card Fraud Detection: Innovations and Future Directions". *North American Journal of Engineering Research*, 4/2023, 1-4.
- Schwartz, M. S., Dunfee, T. W., & Kline, M. J. (2005): "Tone at the top: An ethics code for directors?" *Journal of Business Ethics*, 58/2005, 79-100.
- Siegel, J. G. & Shim, J. K. (2010): *Accounting Handbook*, 5th ed., Barron's Educational Series, NY: Hauppauge.
- Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019): "Examination of cybercrime and its effects on corporate stock value". *Journal of Information, Communication and Ethics in Society*, 17/2019, 42-60.
- Soltani, B. (2014): "The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals". *Journal of Business Ethics*, 120/2014, 251-274.
- Spasić, K., Novičević Čečević, B., & Antić, L. (2024): "The impact of digitisation of the cost accounting system on organizational efficiency and effectiveness in the healthcare sector of the Republic of Serbia". *BizInfo Blace*, 15/2024, 39-47, <https://doi.org/10.5937/bizinfo2402039S>
- Tukura, D. W. (2007): "Curbing advance fee fraud: A Nigerian success story", Conference of Senior Police Officers, EFCC Training and Research Institute, Karu, FCT, Nigeria (26th and 27th March 2007) *The Effects of Forensic Accounting Technology on Fraud Detection in Nigeria*. Available from: https://www.researchgate.net/publication/344398404_The_Effects_of_Forensic_Accounting_Technology_on_Fraud_Detection_in_Nigeria (14.12.2025)
- Zemánková, A. (2019): "Artificial intelligence and blockchain in audit and accounting: Literature review". *WSEAS Transactions on Business and Economics*, 16/2019, 568-581.

FORENSIC ACCOUNTING IN THE DIGITAL ENVIRONMENT: TRENDS AND CHANGES

Summary: *Fraud investigation has attracted increasing attention in recent literature. The digital environment has significantly changed the nature of fraud, which is becoming increasingly sophisticated and difficult to detect. This paper analyzes the role of forensic accounting in detecting fraud in the digital environment. The importance of applying advanced technologies that enable faster and more accurate identification of anomalies and traces of fraudulent behavior is emphasized. The findings indicate that the combination of traditional forensic methods and digital analytical tools is the key to more effectively countering fraud in the modern business environment. This paper contributes to the understanding of contemporary challenges and tendencies in the field of forensic accounting in the era of digitization.*

Keywords: *fraud, forensic accounting, digital environment, advanced technologies, organization*

Marko Stanojević*

<https://orcid.org/0009-0007-7241-5503>

Danilo Izgarević**

<https://orcid.org/0009-0000-0785-3055>

UDC: 005.934

005.591.6:004.89

DOI: 10.5937/MegRev2502051S

Original scientific paper

Received 15.08.2025.

Approved: 10.11.2025.

INTEGRATION OF ARTIFICIAL INTELLIGENCE IN CORPORATE INFORMATION SECURITY SYSTEMS

Abstract: *As the digital landscape keeps evolving, corporate security systems are facing increasingly complex and ever-changing threats that often outstrip traditional defense strategies. This review explores how artificial intelligence (AI) is transforming corporate security through machine learning, anomaly detection, threat intelligence, and real-time decision-making support. By automating those tedious tasks, sorting through heaps of data, and enabling quick responses to potential threats, AI helps organizations strengthen their digital and physical security systems. This paper dives into the challenges that come with AI integration, like making sure data is reliable, algorithms are transparent, ethical issues are addressed, and governance standards are met. Through various case studies and a look at industry tools such as IBM Watson, Darktrace, and Microsoft Security Copilot, the review highlights how AI is increasingly shaping risk management, compliance, and cost efficiency. Ultimately, it emphasizes the need for strong AI governance frameworks and zero-trust architectures to ensure that implementation is both responsible and secure.*

Keywords: *Artificial Intelligence, Information Security, Corporate Security, Threat Detection, AI Governance*

* E-mail: stanojevic.marko799@gmail.com

* E-mail: daniloizgarevic@gmail.com

1. INTRODUCTION

As we experience this surge in digital growth, corporate security systems are confronted with a range of complex threats that traditional rule-based defenses often find hard to cope with. The advent of artificial intelligence (AI) in these systems has emerged as a vital innovation, promising a more proactive, flexible, and automated approach to safeguarding against the constantly changing risks we encounter.

Recent systematic reviews show that AI techniques like machine learning (ML), deep learning (DL), anomaly detection, and threat intelligence are significantly boosting organizations' capabilities to identify, prevent, detect, and respond to security incidents much faster than traditional methods.¹ For example, AI-driven intrusion detection systems and malware classifiers have proven to outperform static signature-based systems when it comes to spotting new or zero-day threats.²

In addition to boosting technical defenses, AI contributes to corporate security by providing decision support, automating routine tasks, and making resource allocation more efficient. By sifting through large data sets in real time, AI systems can spot hidden patterns and anomalies, allowing for timely alerts and proactive defense measures.³

Using AI in corporate security can definitely provide some great advantages, but it's important to recognize that there are also challenges that come along with it. These challenges encompass the risk of adversarial attacks on AI models, the necessity for high-quality data, and issues related to explainability and transparency. Moreover, organizations must set up appropriate governance mechanisms.⁴ As more autonomous systems are rolled out, ethical and legal concerns like algorithmic bias, privacy implications, and accountability are becoming increasingly important.⁵

AI has the ability to assist security experts in identifying and prioritising threats in the context of safety. It can help them manage incident response, identify malware on a network instantly, and stop invasions before they happen. When AI

¹ Kaur, R., Gabrijelčić, D., & Klobučar, T. (2023): "Artificial intelligence for cybersecurity: Literature review and future research directions", *Information Fusion*, 97, 101804. DOI: 10.1016/j.inffus.2023.101804

² Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024): "Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions", *Frontiers in Big Data*. DOI: 10.3389/fdata.2024.1497535

³ Radadiya, P., Shah, K. & Doshi, N. (2025): "Automating AI in Cybersecurity: A Comprehensive Literature Review", *Journal of Information Systems Engineering and Management*, 10(28s). DOI: 10.52783/jisem.v10i28s.4354

⁴ Kaur, R., Gabrijelčić, D., & Klobučar, T. (2023): "Artificial intelligence for cybersecurity: Literature review and future research directions", *Information Fusion*, 97, 101804. DOI: 10.1016/j.inffus.2023.101804

⁵ Nott, C. (2025): "Organizational adaptation to generative AI in cybersecurity: A systematic review", *arXiv preprint arXiv:2506.12060*, <https://arxiv.org/abs/2506.12060>.

is used in physical security, access control, perimeter security systems, and remote monitoring become more responsive, potent, and efficient. AI significantly helps remote monitoring agents by identifying anomalous events, such as a particular movement at a location where there shouldn't be any movement at that moment. These agents can react more swiftly because they are able to comprehend the situation on the ground more quickly. Additionally, the AI can differentiate between human and generic movements, which lowers the number of false alarms.⁶

2. LITERATURE REVIEW

In terms of technology, artificial intelligence refers to the capacity of a machine to carry out tasks that, until recently, required human intelligence. The capabilities of artificial intelligence software are expected to soon surpass those of humans.⁷ From improving customer and employee experiences to automating repetitive work, artificial intelligence (AI) has had a significant impact on how businesses run. AI is now changing how businesses safeguard their assets, people, and property and directing them towards a more proactive security strategy. AI has been included into the security program of nearly half (46%) of the companies surveyed by Securitas Technology. As the number of applications for AI-powered security grows, this number will only go up. There are many applications for AI in security. AI is a potent instrument that will revolutionise business security and operations, from bolstering safety and security protocols to assisting companies in reviving dormant data concealed within their security architecture.⁸

Businesses are facing challenging issues with the technology's dependability and auditability as they come under increasing pressure to incorporate AI into their processes. AI expenditures are taking up new portions of many businesses' budgets. According to a KPMG survey of business executives, 67% of them said they want to invest in cyber and data security safeguards for their AI models, indicating that they prioritise security monitoring when making budgetary decisions for generative AI. Risk and compliance were mentioned as financial priorities by 52% of respondents.⁹

⁶ Vogel, R. (2025): *How Artificial Intelligence empowers Security Professionals to take their service delivery to a new level*, <https://www.evalink.io/blog/how-artificial-intelligence-empowers-security-professionals-to-take-their-service-delivery-to-a-new-level>.

⁷ Baltezarević, R. (2023): "Uticaj veštačke inteligencije na globalnu ekonomiju", *Megatrend revija*, 20(3), 13–24. DOI: 10.5937/MegRev2303013B

⁸ Securitas(2024): *10 ways AI is transforming business security and operations*, <https://www.securitas.com/en/newsroom/blog/10-ways-ai-is-transforming-business-security-and-operations/>.

⁹ Geller, E. (2025): *AI security issues dominate corporate worries, spending*, <https://www.cyber-securitydive.com/news/artificial-intelligence-security-spending-reports/751685/>.

Two categories of AI security can be identified based on their particular objective: weak AI and so-called strong AI (sometimes known as “superintelligence”). Weak AI security solutions function at a comparatively low level of intelligence, whereas strong AI seeks to emulate human reasoning and behaviour in order to equal or even exceed human intellectual capacity. Their capacity to carry out activities independently and automatically is already creating amazing potential for the security firms that use them, even though they do not gain a thorough understanding of the issues to be solved. Alert management, which increases the accuracy of alert verification and lowers the quantity of false alarms, is a well-known illustration of powerful AI in security.¹⁰

Decision-makers frequently have to choose between two competing goals when it comes to corporate security: keeping up with changing threats and making sure that limited funds are used effectively. AI can assist in resolving these issues by: a) Automating repetitive tasks: By automating processes like risk assessments, vendor reviews, and compliance audits, managers can concentrate on handling problems and making important decisions. b) Turning data overload into insights: A lot of data is produced by security systems. AI breaks through the clutter. Teams can take preemptive measures thanks to its analysis of possible threats, risk identification, bias removal, and prioritisation of actionable insights. c) Improving cost control and resource allocation: AI forecasts risks and makes sure that resources are distributed where they will have the biggest impact by analysing historical and real-time data.¹¹

AI agents created especially for the corporate security sector will allow internal teams to provide services that were previously unthinkable. By speeding up the decision-making process during disruptive occurrences, these agents will not only free up staff members to work on more strategic and sophisticated tasks, but they will also help minimise financial damage. When a security crisis happens in the not-too-distant future, AI agents will explain why it matters, forecast potential outcomes, and give the responding security team practical advice. These agents will revolutionise proactive risk management in the AI era and provide personalised real-time insights for all organisations for the first time.¹²

A number of AI-powered solutions are revolutionising how companies handle security and compliance. These tools are not merely theoretical; they are actively

¹⁰ Vogel, R. (2025): *How Artificial Intelligence empowers Security Professionals to take their service delivery to a new level*, <https://www.evalink.io/blog/how-artificial-intelligence-empowers-security-professionals-to-take-their-service-delivery-to-a-new-level>.

¹¹ Pronect-it (2025): *How AI Can Transform Corporate Security Management: Balancing Risk and Opportunity*, <https://pronect-it.com/how-ai-can-transform-security-management/>.

¹² Crowley, R. (2025): *How AI Agents Will Reimagine Corporate Security Departments*, <https://www.securityinfowatch.com/security-executives/article/55310445/how-ai-agents-will-reimagine-corporate-security-departments>.

influencing how businesses manage risks, safeguard data, and maintain regulatory compliance. A few examples are as follows: a) Darktrace: This tool employs machine learning to automatically detect and address dangers in digital settings. b) Cylance: Proactive endpoint protection using AI-based predictive analytics. c) IBM Watson for cyber security: Determines subtle dangers that conventional systems could overlook by analysing unstructured data. d) Microsoft security copilot: Improves security operations by identifying threats, analysing security data, and suggesting actions using generative AI. For companies in the Microsoft ecosystem, this product is especially helpful because it speeds up incident response and increases security teams' overall effectiveness.¹³

To successfully integrate artificial intelligence into corporate security systems, effective governance mechanisms are vital. They provide a necessary framework for ensuring transparency, accountability, and compliance with ethical and legal standards. Organizations should really focus on weaving AI governance into their corporate, IT, and data governance structures. Corporate governance is all about setting the strategic direction, IT governance deals with the technical implementation, and data governance looks after data quality, privacy, and usage.¹⁴ For instance, within an AI governance framework, identifying risks like algorithmic bias, data breaches, and those mysterious “black box” models is crucial. To safeguard the integrity of autonomous decisions, we need to put in place algorithm audits and oversight mechanisms, including human-in-the-loop controls.¹⁵ By skillfully bringing these governance practices together, we can ensure that AI systems used in security settings operate not just as advanced tools, but as reliable and well-documented components that align with risk management strategies and meet the expectations of stakeholders. The impact of virtual communication on privacy protection and data processing laws is significant, particularly when it involves AI systems that generate and analyze vast amounts of sensor and communication data.¹⁶

To really grasp the practical impact of these advancements, we can look at a few recent case studies that offer clear examples. Take Kempower, a Finnish tech company, for instance. They effectively harnessed generative AI to quicken the process of developing their Information Security Management System (ISMS) in line with ISO 27001 standards. This tactic significantly reduced the time and effort

¹³ Tribe(2025): *AI in Security: Corporate Security and Compliance - Safeguarding Data and Navigating Regulations*, <https://www.tribe.ai/applied-ai/ai-in-corporate-security-and-compliance>.

¹⁴ Mäntymäki, M., Minkkinen, M., Birkstedt, T. & Viljanen, M. (2022): “Defining organizational AI governance”, *AI Ethics*, 2, 603–609. DOI: 10.1007/s43681-022-00143-x

¹⁵ Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2022): “Governance of artificial intelligence: A risk and guideline-based integrative framework” *Government Information Quarterly*, 39(4), 101685. DOI: 10.1016/j.giq.2022.101685

¹⁶ Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku“, *Megatrend Revija*, 17(4), 27-40. DOI: 10.5937/MegRev2004027B

involved in defining, documenting, and implementing key security controls.¹⁷ In a similar vein, various companies in critical fields like finance and infrastructure are turning to large language models (LLMs) for tasks like threat modeling, security automation, and compliance management. However, these implementations still face ongoing challenges, including the necessity for human oversight, the need for model explainability, and the ability to withstand manipulation.¹⁸

In another case, an AI-powered insider risk management system utilizing behavioral analytics and dynamic risk scoring was able to cut incident response times by 47%. This system also decreased false positives and increased detection accuracy, illustrating the operational benefits of AI when it's deployed in a structured and well-governed manner.¹⁹ Taking a wider industry view, IBM's annual security report pointed out that businesses that integrated advanced AI and automation into their security operations were able to cut the average data breach lifecycle by more than 100 days. They also saw a notable decrease in breach costs compared to those that didn't.²⁰

By implementing continuous verification of all access requests throughout AI infrastructure, the zero-trust architecture removes the implicit trust assumptions that give traditional systems their security flaws. This foundation facilitates autonomous threat detection capabilities that identify ransomware and security anomalies in real-time using AI-powered identification, enabling quick responses that reduce the impact on company. Continuous monitoring offers continuous security posture assessment and threat detection that finds possible vulnerabilities before they are exploited, while policy enforcement mechanisms automatically apply data governance rules and access controls, guaranteeing consistent protection without constant manual intervention. Model protection features that protect the intellectual property in trained models and thwart adversarial attacks that might jeopardise the integrity of AI systems are also part of this all-inclusive approach. Governance and visibility tools provide comprehensive oversight of data usage and access patterns, allowing organisations to retain control over their AI initiatives.²¹

¹⁷ Niemeläinen, A., Waseem, M., & Mikkonen, T. (2024): "Enhancing productivity with AI during the development of an ISMS: Case Kempower", *arXiv preprint arXiv:2409.19029*, <https://arxiv.org/abs/2409.19029>.

¹⁸ Nott, C. (2025): "Organizational adaptation to generative AI in cybersecurity: A systematic review", *arXiv preprint arXiv:2506.12060*, <https://arxiv.org/abs/2506.12060>.

¹⁹ Koli, L., Kalra, S., Thakur, R., Saifi, A., & Singh, K. (2025): AI-Driven IRM: Transforming insider risk management with adaptive scoring and LLM-based threat detection, *arXiv preprint arXiv:2505.03796*, <https://arxiv.org/abs/2505.03796>.

²⁰ Columbus, L. (2023): "Study reveals how AI, automation protect enterprises against data breaches", *VentureBeat*, <https://venturebeat.com/security/ibm-study-reveals-how-ai-automation-protect-enterprises-against-data-breaches/>.

²¹ Giddings, M. (2025): *Enterprise-Grade Security and Governance the Trust Foundation of AI Factories*, <https://www.netapp.com/blog/enterprise-ai-security-zero-trust-ai-factory/>.

3. CONCLUSION

Integrating artificial intelligence into corporate security systems is a game-changer for how organizations protect their assets, data, and staff. With the rise of increasingly complex and widespread threats, AI stands out as a proactive, adaptable, and scalable solution that significantly improves both digital and physical security. From improving threat detection and incident response to optimizing resource management and reducing human mistakes, AI tools are revolutionizing our security landscape.

While welcoming AI into the world of security opens up some thrilling possibilities, it also presents a number of challenges we need to tackle. We can't overlook important issues such as data quality, transparency in models, algorithmic bias, and governance. It's essential for organizations to build governance frameworks that are not only efficient but also adhere to legal standards and ethical practices, all while supporting their operational goals. For AI systems to function both safely and effectively, it's vital to integrate essential elements like zero-trust architectures, constant monitoring, and the involvement of humans in the process.

In the future, research needs to hone in on establishing standardized frameworks for AI governance within the security sector. We need to work on making complex models more understandable and investigate how AI interacts with emerging technologies like quantum computing and blockchain. As the corporate threat landscape evolves, collaboration among technologists, policymakers, and security professionals will be key to ensuring that AI is a source of resilience rather than risk. By taking on the opportunities and responsibilities of AI, organizations can build security systems that are intelligent, ethical, and equipped to face the challenges that lie ahead.

Literature

- Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024): "Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions", *Frontiers in Big Data*. DOI: 10.3389/fdata.2024.1497535
- Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku“, *Megatrend Revija*, 17(4), 27-40. DOI: 10.5937/MegRev2004027B
- Baltezarević, R. (2023): "Uticaj veštačke inteligencije na globalnu ekonomiju", *Megatrend revija*, 20(3), 13–24. DOI: 10.5937/MegRev2303013B
- Columbus, L. (2023): "Study reveals how AI, automation protect enterprises against data breaches", *VentureBeat*, <https://venturebeat.com/security/>

- ibm-study-reveals-how-ai-automation-protect-enterprises-against-data-breaches/.
- Crowley, R. (2025): *How AI Agents Will Reimagine Corporate Security Departments*, <https://www.securityinfowatch.com/security-executives/article/55310445/how-ai-agents-will-reimagine-corporate-security-departments>.
 - Geller, E. (2025): *AI security issues dominate corporate worries, spending*, <https://www.cybersecuritydive.com/news/artificial-intelligence-security-spending-reports/751685/>.
 - Giddings, M. (2025): *Enterprise-Grade Security and Governance The Trust Foundation of AI Factories*, <https://www.netapp.com/blog/enterprise-ai-security-zero-trust-ai-factory/>.
 - Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023): "Artificial intelligence for cybersecurity: Literature review and future research directions", *Information Fusion*, 97, 101804. DOI: 10.1016/j.inffus.2023.101804
 - Koli, L., Kalra, S., Thakur, R., Saifi, A., & Singh, K. (2025): "AI-Driven IRM: Transforming insider risk management with adaptive scoring and LLM-based threat detection", *arXiv preprint arXiv:2505.03796*, <https://arxiv.org/abs/2505.03796>.
 - Mäntymäki, M., Minkkinen, M., Birkstedt, T. & Viljanen, M. (2022): "Defining organizational AI governance", *AI Ethics*, 2, 603–609. DOI: 10.1007/s43681-022-00143-x
 - Niemeläinen, A., Waseem, M., & Mikkonen, T. (2024): "Enhancing productivity with AI during the development of an ISMS: Case Kempower", *arXiv preprint arXiv:2409.19029*, <https://arxiv.org/abs/2409.19029>.
 - Nott, C. (2025): "Organizational adaptation to generative AI in cybersecurity: A systematic review", *arXiv preprint arXiv:2506.12060*, <https://arxiv.org/abs/2506.12060>.
 - Pronect-it (2025): *How AI Can Transform Corporate Security Management: Balancing Risk and Opportunity*, <https://pronect-it.com/how-ai-can-transform-security-management/>.
 - Radadiya, P., Shah, K. & Doshi, N. (2025): "Automating AI in Cybersecurity: A Comprehensive Literature Review", *Journal of Information Systems Engineering and Management*, 10(28s). DOI: 10.52783/jisem.v10i28s.4354
 - Securitas (2024): *10 ways AI is transforming business security and operations*, <https://www.securitas.com/en/newsroom/blog/10-ways-ai-is-transforming-business-security-and-operations/>.
 - Tribe (2025): *AI in Security: Corporate Security and Compliance - Safeguarding Data and Navigating Regulations*, <https://www.tribe.ai/applied-ai/ai-in-corporate-security-and-compliance>.

- Vogel, R. (2025): *How Artificial Intelligence empowers Security Professionals to take their service delivery to a new level*, <https://www.evalink.io/blog/how-artificial-intelligence-empowers-security-professionals-to-take-their-service-delivery-to-a-new-level>.
- Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2022): “Governance of artificial intelligence: A risk and guideline-based integrative framework”, *Government Information Quarterly*, 39(4), 101685. DOI: 10.1016/j.giq.2022.101685

INTEGRACIJA VEŠTAČKE INTELIGENCIJE U SISTEME KORPORATIVNE BEZBEDNOSTI

Sažetak: *Kako se digitalni pejzaž stalno razvija, korporativni bezbednosni sistemi se suočavaju sa sve složenijim i stalno promenljivim pretnjama koje često nadmašuju tradicionalne odbrambene strategije. Ovaj pregledni rad istražuje kako veštačka inteligencija (AI) transformiše korporativnu bezbednost kroz mašinsko učenje, otkrivanje anomalija, obaveštajne podatke o pretnjama i podršku u donošenju odluka u realnom vremenu. Automatizacijom tih zamornih zadataka, sortiranjem gomila podataka i omogućavanjem brzih odgovora na potencijalne pretnje, AI pomaže organizacijama da ojačaju svoje digitalne i fizičke bezbednosne sisteme. Ovaj rad se bavi izazovima koji dolaze sa integracijom AI, kao što je osiguravanje da su podaci pouzdani, algoritmi transparentni, da se rešavaju etička pitanja i da se ispunjavaju standardi upravljanja. Kroz različite studije slučaja i pogled na industrijske alate kao što su IBM Watson, Darktrace i Microsoft Security Copilot, rad ističe kako AI sve više oblikuje upravljanje rizicima, usklađenost i efikasnost troškova. Na kraju krajeva, naglašava potrebu za jakim okvirima za upravljanje AI i arhitekturama nultog poverenja kako bi se osiguralo da je implementacija i odgovorna i bezbedna.*

Ključne reči: *Veštačka inteligencija, Korporativna bezbednost, Otkrivanje pretnji, Upravljanje veštačkom inteligencijom*

TRANSFORMACIJA UPRAVLJANJA LJUDSKIM RESURSIMA KROZ VEŠTAČKU INTELIGENCIJU

Sažetak: *Razvoj veštačke inteligencije (VI) predstavlja jedan od ključnih pokretača digitalne transformacije savremenog poslovanja, a njen uticaj naročito dolazi do izražaja u oblasti upravljanja ljudskim resursima (HRM). Integracija VI u HR procese omogućava organizacijama da unaprede efikasnost, objektivnost i preciznost donošenja odluka u domenu regrutacije, selekcije, evaluacije i razvoja zaposlenih. Automatizacijom administrativnih zadataka, primenom prediktivne analitike i algoritama mašinskog učenja, HR menadžment prelazi iz operativne u stratešku funkciju zasnovanu na podacima. Ovaj rad analizira ključne aspekte transformacije HRM-a kroz primenu VI, uz poseban osvrt na njenu ulogu u optimizaciji procesa selekcije i zapošljavanja. Empirijski nalazi ukazuju da primena VI doprinosi smanjenju vremena zapošljavanja, povećanju objektivnosti i poboljšanju iskustva kandidata, dok istovremeno otvara i niz etičkih i regulatornih pitanja u vezi sa transparentnošću algoritama i zaštitom privatnosti podataka. Zaključuje se da veštačka inteligencija, uz odgovornu i etičku primenu, postaje nezaobilazan strateški alat u savremenom upravljanju ljudskim resursima, koji omogućava razvoj agilnijih, inkluzivnijih i efikasnijih organizacija.*

Ključne reči: *veštačka inteligencija, upravljanje ljudskim resursima, selekcija kandidata, digitalna transformacija, automatizacija, etika u HRM-u, prediktivna analitika*

* Megatrend Univerzitet, Beograd, Srbija
E-mail: marijanazimonjic1978@gmail.com

** Union-Nikola Tesla Univerzitet, Beograd, Srbija
E-mail: milinko.velickovic@gmail.com

UVOD

Savremeno poslovno okruženje karakterišu ubrzane tehnološke promene, globalizacija i digitalna transformacija koje su dovele do redefinisanja načina na koji organizacije funkcionišu i upravljaju svojim resursima. Jedan od najznačajnijih fenomena koji oblikuje savremeno poslovanje jeste veštačka inteligencija (VI), koja se definiše kao sposobnost mašina da uče iz podataka, donose odluke i rešavaju probleme koji su do sada zahtevali ljudsku kogniciju.¹

Primena veštačke inteligencije postaje sve rasprostranjenija u različitim poslovnim funkcijama, ali posebno dubok uticaj ima u oblasti upravljanja ljudskim resursima (HRM). HR menadžment je tradicionalno zasnovan na interakciji između ljudi, proceni potencijala, motivaciji i razvoju zaposlenih. Međutim, s pojavom naprednih digitalnih tehnologija, HRM prolazi kroz temeljnu transformaciju – prelazak sa administrativne i operativne uloge na stratešku funkciju zasnovanu na analizi podataka i automatizaciji procesa.²

Veštačka inteligencija u HRM-u omogućava automatizaciju rutinskih zadataka kao što su analiza biografija, zakazivanje intervju a i evaluacija kompetencija kandidata, čime se značajno smanjuje vreme potrebno za zapošljavanje i povećava objektivnost odluka.³ Prema istraživanju koje su sprovedi Cappelli i Tambe (2020), organizacije koje koriste AI u selekciji kandidata beleže i do 70% kraće procese zapošljavanja i 40% smanjenje pristrasnosti u odabiru.⁴ Ovi podaci potvrđuju da VI ne predstavlja samo tehnološku inovaciju, već i strateški alat koji menja paradigmu HR upravljanja.

Pored efikasnosti, značajna prednost VI leži u njenoj sposobnosti da omogućiti odluke zasnovane na podacima (data-driven decision making), što povećava tačnost predviđanja uspeha kandidata i smanjuje rizik od pogrešnih zapošljavanja. Ipak, paralelno s ovim prednostima, primena VI otvara i brojna etička i pravna pitanja, naročito u pogledu transparentnosti algoritama, zaštite privatnosti kandidata i mogućnosti reprodukcije društvenih predrasuda kroz podatke.⁵

Cilj ovog rada jeste da istraži načine na koje veštačka inteligencija transformiše procese upravljanja ljudskim resursima, sa posebnim naglaskom na selekciju i

¹ Russell, S., & Norvig, P. (2021): *Artificial Intelligence: A Modern Approach* (4th ed.), Pearson.

² Stone, D. L., & Deadrick, D. L. (2015): "Challenges and opportunities affecting the future of human resource management", *Human Resource Management Review*, 25(2), 139–145.

³ Cappelli, P., & Tambe, P. (2020): "HR Goes Digital: The Promise and Peril of Technology in HR", *MIT Sloan Management Review*, 61(2), 23–31.

⁴ Tambe, P., Cappelli, P., & Yakubovich, V. (2019): "Artificial intelligence in human resources management: Challenges and a path forward", *California Management Review*, 61(4), 15–42.

⁵ Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020): "Mitigating bias in algorithmic hiring: Evaluating fairness interventions in practice" in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 469–481.

zapošljavanje. Posebno će biti analizirani primeri primene VI u praksi globalnih kompanija, kao i empirijski dokazi o njenom doprinosu efikasnosti, objektivnosti i kvalitetu HR procesa. Rad takođe nastoji da identifikuje izazove i etičke implikacije koje prate ovu transformaciju, kako bi se obezbedio održiv i odgovoran pristup primeni veštačke inteligencije u poslovnom okruženju.

POJAM I ZNAČAJ VEŠTAČKE INTELIGENCIJE

Veštačka inteligencija (VI) predstavlja oblast računarskih nauka koja se bavi razvojem sistema sposobnih da obavljaju zadatke koji zahtevaju ljudsku inteligenciju, kao što su učenje, zaključivanje, prepoznavanje obrazaca i donošenje odluka.⁶ Suština VI ogleda se u njenoj sposobnosti da simulira procese ljudskog razmišljanja i ponašanja, omogućavajući računarima da analiziraju ogromne količine podataka, prepoznaju obrasce i prilagođavaju se novim informacijama.⁷

Najvažniji podsklopovi VI uključuju mašinsko učenje (machine learning), obradu prirodnog jezika (Natural Language Processing – NLP) i prediktivnu analitiku. Mašinsko učenje podrazumeva razvoj algoritama koji omogućavaju sistemima da uče iz podataka i poboljšavaju svoje performanse bez eksplicitnog programiranja.⁸ NLP omogućava računarima da razumeju, interpretiraju i generišu ljudski jezik, čime se otvara prostor za primene poput chatbotova, automatizovane podrške korisnicima i analize sentimenta.⁹ Prediktivna analitika koristi statističke modele i algoritme mašinskog učenja za predviđanje budućih događaja, ponašanja korisnika ili poslovnih trendova, što ima posebnu primenu u donošenju strateških odluka u poslovnom okruženju.¹⁰

Razvoj veštačke inteligencije ima dugu istoriju, koja počinje sredinom XX veka. Termin „artificial intelligence“ prvi put je upotrebio John McCarthy 1956. godine na konferenciji na Univerzitetu Dartmouth, čime je označen početak nove naučne discipline.¹¹ Tokom narednih decenija, razvoj VI prolazio je kroz nekoliko faza — od tzv. „AI zima“, kada je interesovanje za ovu oblast opadalo zbog ograničenih mogućnosti računara, do savremenog „buđenja“ u XXI veku, koje je

⁶ Russell, S., & Norvig, P. (2021): *Artificial Intelligence: A Modern Approach* (4th ed.), Pearson.

⁷ Baltezarević, R. (2023): „Uticaj veštačke inteligencije na globalnu ekonomiju“, *Megatrend revija*, 20(3), 13–24. DOI: 10.5937/MegRev2303013B

⁸ Goodfellow, I., Bengio, Y., & Courville, A. (2016): *Deep Learning*, MIT Press.

⁹ Davenport, T., & Ronanki, R. (2018): „Artificial intelligence for the real world“, *Harvard Business Review*, 96(1), 108–116.

¹⁰ McCarthy, J., Minsky, M., Rochester, N., & Shannon, C. (1955): *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Dartmouth College.

¹¹ Brynjolfsson, E., & McAfee, A. (2017): *Machine, Platform, Crowd: Harnessing Our Digital Future*, W. W. Norton & Company.

omogućeno eksponencijalnim razvojem procesorske snage, velikih podataka (big data) i naprednih algoritama mašinskog učenja.¹²

Danas, VI predstavlja jedan od ključnih stubova četvrte industrijske revolucije (Industrija 4.0), uz robotiku, internet stvari (IoT) i automatizaciju. Prema istraživanju *World Economic Forum*a (2023), više od 80% globalnih kompanija već koristi ili planira da implementira AI rešenja u poslovnim procesima u naredne dve godine, dok se očekuje da će tržište VI dostići vrednost od preko 500 milijardi dolara do 2027. godine.¹³

Značaj VI u savremenom poslovanju ogleda se u njenoj sposobnosti da poveća efikasnost, preciznost i brzinu odlučivanja. VI sistemi omogućavaju automatizaciju rutinskih zadataka, optimizaciju poslovnih procesa, analizu velikih skupova podataka i personalizaciju korisničkog iskustva⁸. U kontekstu upravljanja ljudskim resursima, VI omogućava organizacijama da bolje razumeju ponašanje zaposlenih, predvide fluktuaciju kadrova i unaprede procese selekcije i razvoja zaposlenih, čime postaje ključni pokretač digitalne transformacije HRM-a.¹⁴

U tom smislu, veštačka inteligencija više nije samo tehnološki trend, već strateški alat koji menja način na koji organizacije funkcionišu, donose odluke i stvaraju konkurentsku prednost. Kombinovanjem analitičkih mogućnosti VI i ljudske kreativnosti, savremene organizacije stiču mogućnost da kreiraju inovativne, agilne i održive poslovne modele prilagođene zahtevima digitalne ekonomije.¹⁵

UPRAVLJANJE LJUDSKIM RESURSIMA – KONCEPT I FUNKCIJE

Upravljanje ljudskim resursima (HRM) predstavlja jedan od ključnih pod-sistema savremenih organizacija, čija je osnovna uloga da obezbedi optimalno korišćenje ljudskog potencijala radi postizanja strateških ciljeva preduzeća.¹⁶ U kontekstu digitalne transformacije i globalne konkurencije, HRM više nije ograničen na administrativne i operativne zadatke, već postaje strateški partner

¹² World Economic Forum. (2023): *The Future of Jobs Report 2023*, Geneva: WEF.

¹³ Brougham, D., & Haar, J. (2018): "Smart technology, artificial intelligence, robotics, and algorithms (STARA): Employees' perceptions of our future workplace", *Journal of Management & Organization*, 24(2), 239–257.

¹⁴ Tambe, P., Cappelli, P., & Yakubovich, V. (2019): "Artificial intelligence in human resources management: Challenges and a path forward", *California Management Review*, 61(4), 15–42.

¹⁵ Jarrahi, M. H. (2018): "Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making", *Business Horizons*, 61(4), 577–586.

¹⁶ Dessler, G. (2019): *Human Resource Management* (16th ed.), Pearson Education.

menadžmenta, odgovoran za razvoj kompetencija, organizacione kulture i inovativnih praksi koje podstiču dugoročni uspeh organizacije.¹⁷

Savremeni koncept upravljanja ljudskim resursima zasniva se na integraciji tri ključna pristupa: menadžerskog, psihološkog i strateškog. Menadžerski pristup naglašava ulogu HR funkcije u planiranju, organizovanju, vođenju i kontroli ljudskog kapitala, dok psihološki pristup polazi od razumevanja motivacije, zadovoljstva i ponašanja zaposlenih. Strateški pristup, s druge strane, usmerava HRM ka kreiranju dugoročne dodate vrednosti kroz usklađivanje politike upravljanja ljudima sa poslovnim strategijama organizacije.¹⁸

Prema Armstrongu (2020), osnovne funkcije upravljanja ljudskim resursima mogu se podeliti na sledeće oblasti:

1. **Planiranje kadrova** – predviđanje potreba za zaposlenima na osnovu budućih ciljeva i planova rasta organizacije;
2. **Regrutacija i selekcija** – privlačenje i odabir kandidata sa odgovarajućim kompetencijama i vrednostima;
3. **Razvoj i obuka zaposlenih** – kontinuirano unapređenje znanja i veština kroz programe edukacije i karijernog razvoja;
4. **Procena performansi** – sistematsko merenje učinka zaposlenih radi unapređenja efikasnosti;
5. **Nagrađivanje i motivacija** – dizajniranje sistema nagrađivanja koji podstiču angažovanost i lojalnost;
6. **Odnosi sa zaposlenima i organizaciona kultura** – izgradnja pozitivne radne klime, međuljudskih odnosa i vrednosnih standarda;
7. **Zadržavanje talenata** – sprovođenje mera koje smanjuju fluktuaciju i podstiču dugoročnu posvećenost.¹⁹

Efikasan HRM sistem obezbeđuje da organizacija raspolaže pravim ljudima, na pravom mestu i u pravo vreme, što direktno utiče na produktivnost, inovativnost i konkurentnost preduzeća.²⁰ U tom smislu, HRM ne treba posmatrati samo kao operativnu funkciju, već kao strateški instrument organizacionog razvoja.

Uloga HRM-a značajno se menja sa razvojem novih tehnologija, naročito veštačke inteligencije, analitike podataka i automatizacije. Tradicionalne metode

¹⁷ Ulrich, D., & Dulebohn, J. H. (2015): "Are we there yet? What's next for HR?", *Human Resource Management*, 54(2), 147–171

¹⁸ Zimonjić, M. (2025): "The impact of the human factor on the development and importance of aviation communication in maintaining flight safety", *Megatrend revija*, 22(1), 173–184. DOI: 10.5937/MegRev2501173Z

¹⁹ Armstrong, M. (2020): *A Handbook of Human Resource Management Practice* (15th ed.), Kogan Page.

²⁰ Becker, B. E., & Huselid, M. A. (2006): "Strategic human resources management: Where do we go from here?", *Journal of Management*, 32(6), 898–925.

regrutacije i selekcije zamenjuju se digitalnim platformama i algoritamskim analizama, dok HR menadžeri sve više koriste alate za prediktivno planiranje kadrova, analizu performansi i personalizovani razvoj zaposlenih. Ovaj prelazak ka digitalno podržanom HRM-u označava pojavu koncepta „HR 4.0“, u kojem ljudski resursi postaju ključni deo šire digitalne strategije organizacije.²¹

U tom kontekstu, ljudski kapital se sve više posmatra kao strateški resurs koji organizacijama omogućava stvaranje konkurentne prednosti. Kompetencije, kreativnost i inovativnost zaposlenih postaju glavni faktori uspeha, dok HR menadžeri preuzimaju ulogu strateških arhitekata koji oblikuju organizacionu kulturu, podstiču učenje i podržavaju digitalnu transformaciju.²²

Upravljanje ljudskim resursima, dakle, prevazilazi tradicionalne administrativne granice i postaje centralni element organizacionog upravljanja. Uloga HR menadžera u novom digitalnom okruženju ogleda se u sposobnosti da poveže tehnologiju, ljude i strategiju — stvarajući održive sisteme koji istovremeno unapređuju performanse i čuvaju ljudsku dimenziju poslovanja.²³

INTEGRACIJA VEŠTAČKE INTELIGENCIJE U UPRAVLJANJE LJUDSKIM RESURSIMA (HRM)

Integracija veštačke inteligencije (VI) u upravljanje ljudskim resursima predstavlja jedan od najznačajnijih koraka u digitalnoj transformaciji savremenih organizacija. Zahvaljujući razvoju algoritama mašinskog učenja, analitike podataka i automatizacije procesa, HRM se iz tradicionalne administrativne funkcije transformiše u strateški, prediktivni i analitički sistem koji podržava donošenje odluka zasnovanih na podacima (data-driven decision making).²⁴

Primena veštačke inteligencije u HRM-u obuhvata gotovo sve faze ciklusa upravljanja ljudskim kapitalom — od planiranja kadrova i regrutacije do razvoja, evaluacije i zadržavanja zaposlenih. Najveći uticaj, međutim, uočava se u procesima selekcije i zapošljavanja, gde VI omogućava automatizaciju, objektivizaciju i ubrzanje odluka. AI alati koriste algoritme za prepoznavanje obrazaca u

²¹ Marler, J. H., & Boudreau, J. W. (2017). An evidence-based review of HR Analytics. *The International Journal of Human Resource Management*, 28(1), 3–26.

²² Bissola, R., & Imperatori, B. (2019): “HR 4.0: The digital transformation of human resources”, *Management and Organizational Studies*, 7(2), 15–28.

²³ Zimonjić, M. (2025): “The importance of applying the asset valuation model to medium-sized enterprises”, *Ekonomija - Teorija I Praksa*, 18(2), 15–26, <https://casopis.fimek.edu.rs/index.php/etp/article/view/331>. DOI: 10.5937/etp2502015Z

²⁴ Stone, D. L., Deadrick, D. L., Lukaszewski, K. M., & Johnson, R. (2015): “The influence of technology on the future of human resource management”, *Human Resource Management Review*, 25(2), 216–231.

biografijama kandidata, procenu kompetencija na osnovu digitalnih tragova i predviđanje verovatnoće uspeha na određenom radnom mestu.²⁵

Prema istraživanju Tambea, Cappellija i Yakuboviča (2019), organizacije koje koriste AI sisteme u selekciji kandidata beleže značajna poboljšanja u efikasnosti — vreme potrebno za zapošljavanje skraćuje se i do 70%, dok se preciznost procene kandidata povećava za 30–40%. Slične rezultate pokazuje i izveštaj IBM Watson Talenta (2019), prema kojem prediktivni modeli na osnovu istorijskih podataka mogu identifikovati najuspešnije kandidate, smanjujući fluktuaciju zaposlenih i troškove regrutacije.²⁶

U oblasti obuke i razvoja zaposlenih, veštačka inteligencija omogućava personalizovano učenje kroz inteligentne platforme za upravljanje znanjem (AI-driven learning management systems). Ovi sistemi analiziraju potrebe zaposlenih i predlažu sadržaje i programe obuke u skladu sa individualnim razvojnim ciljevima. Takođe, veštačka inteligencija može da prati napredak zaposlenih, identifikuje nedostatke u kompetencijama i automatski preporuči dodatne obuke — čime se proces učenja čini dinamičnim, prilagodljivim i efikasnijim.²⁷

U segmentu evaluacije performansi, veštačka inteligencija doprinosi objektivnosti i transparentnosti. Umesto tradicionalnih metoda procene koje se oslanjaju na subjektivne ocene nadređenih, AI alati analiziraju kvantitativne pokazatelje kao što su produktivnost, angažovanost i komunikacija zaposlenih, pružajući sveobuhvatan uvid u njihov doprinos organizaciji. Na taj način se eliminišu predrasude i neusklađenosti u proceni, što doprinosi pravednijem sistemu nagrađivanja i motivacije.²⁸

Još jedan važan vid integracije VI u HRM jesu chatbot sistemi i virtuelni asistenti, koji automatizuju komunikaciju između HR odeljenja i zaposlenih. Chatbotovi mogu davati informacije o politikama kompanije, slobodnim danima, benefitima ili statusu prijave, čime se povećava dostupnost HR usluga i zadovoljstvo zaposlenih⁸. Ovi alati takođe prikupljaju povratne informacije koje se kasnije koriste za analizu zadovoljstva i optimizaciju organizacione kulture.

Ipak, iako integracija VI donosi značajne koristi, ona otvara i niz etičkih i pravnih pitanja. Prema Raghavanu i saradnicima (2020), algoritmi korišćeni u procesima zapošljavanja mogu nehotice reprodukovati pristrasnosti prisutne u istorijskim podacima, što može dovesti do diskriminatornih odluka.²⁹ Zbog toga

²⁵ Black, S. E., & van Esch, P. (2020): "AI-enabled recruitment: Exploring the impact on HRM", *The International Journal of Human Resource Management*, 31(22), 2824–2846.

²⁶ IBM Watson Talent Report. (2019): *How AI transforms recruitment and employee retention*, IBM Research.

²⁷ Jarrahi, M. H. (2018): "Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making", *Business Horizons*, 61(4), 577–586.

²⁸ Marler, J. H., & Boudreau, J. W. (2017): "An evidence-based review of HR analytics", *The International Journal of Human Resource Management*, 28(1), 3–26

²⁹ Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020): "Mitigating bias in algorithmic hiring: Evaluating fairness interventions in practice" in *Proceedings of the 2020 Conference*

je od suštinskog značaja uvođenje mehanizama nadzora, transparentnosti i etičkog okvira koji obezbeđuju pravičnost i odgovornost u primeni VI u HRM-u.

U budućnosti se očekuje da će integracija veštačke inteligencije u HR funkcije biti još dublja, kroz upotrebu generativnih modela, napredne analitike talenata i automatizovane procese karijernog planiranja. HR menadžeri će, prema prognozama, sve više koristiti kombinovane sisteme (Human-AI collaboration), u kojima tehnologija preuzima analitičke i operativne zadatke, dok čovek zadržava kontrolu nad etičkim i strateškim aspektima odlučivanja.³⁰

Kao rezultat toga, veštačka inteligencija postaje ključni pokretač evolucije HRM-a — prelaska sa reaktivne i operativne funkcije na proaktivnu, stratešku i prediktivnu funkciju, koja povezuje ljudski i tehnološki kapital u jedinstveni sistem organizacionog učenja i inovacija.

EMPIRIJSKI DEO: UTICAJ VEŠTAČKE INTELIGENCIJE NA PROCESE SELEKCIJE I ZAPOSŁJAVANJA

Digitalna transformacija poslovanja dovela je do sve veće integracije veštačke inteligencije (VI) u upravljanje ljudskim resursima (HRM). U poslednje dve godine, broj kompanija koje koriste algoritme za selekciju i zapošljavanje porastao je za više od 50% (Glassdoor, 2024). Cilj ovog istraživanja je da se analizira kako primena VI utiče na efikasnost, kvalitet i pravičnost procesa zapošljavanja, kroz komparativnu studiju tri međunarodne kompanije koje posluju u različitim industrijama – Swire Coca-Cola, Mitsubishi UFJ Trust & Banking i Sodexo – u periodu 2024–2025.

Metodologija istraživanja

Istraživanje je sprovedeno kao **komparativna studija slučaja sa pre-post analizom** u svakoj kompaniji. Korišćeni su sekundarni podaci iz izveštaja kompanija, javnih publikacija i nezavisnih analiza o primeni AI rešenja u HRM-u (HireVue, Paradox.ai, LinkedIn Reports, SHRM, 2024–2025). Glavni indikatori performansi su:

- vreme zapošljavanja (time-to-hire),
- trošak po zapošljavanju (cost-per-hire),
- kvalitet zapošljavanja (quality of hire),
- zadovoljstvo kandidata (candidate NPS),
- raznolikost kandidata (diversity ratio).

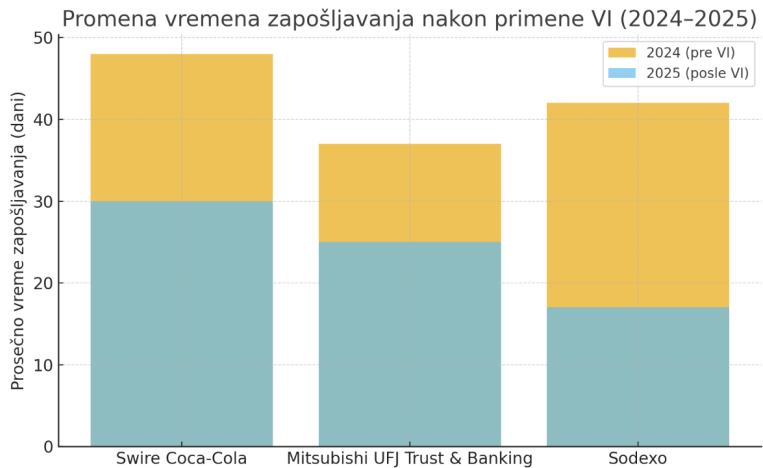
on Fairness, Accountability, and Transparency, 469–481.

³⁰ Brynjolfsson, E., & McAfee, A. (2017): *Machine, Platform, Crowd: Harnessing Our Digital Future*, W. W. Norton & Company.

Rezultati komparativne analize

Kompanija	Swire Coca-Cola	Mitsubishi UFJ Trust & Banking
AI alat / sistem	HireVue platforma (video analiza, prediktivni modeli)	Interni AI video sistem za selekciju diplomaca
Period primene	2024–2025	2024–2025
Time-to-hire	↓ sa 48 na 30 dana (-37%)	↓ za 32%
Cost-per-hire	↓ za 25%	↓ za 20%
Candidate NPS	+79	+58,4
Diversity ratio	+16% raznolikosti	+19% raznolikosti
Ključni efekti	Brža selekcija i veća preciznost u proceni kandidata	Poboljšano iskustvo kandidata i veća pravičnost procesa

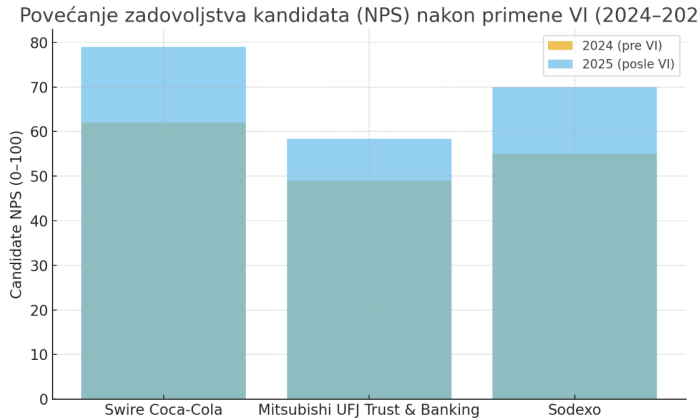
Izvor: Podaci preuzeti i sintetizovani iz javno dostupnih studija slučaja i internih HR izveštaja kompanija (2024–2025).



Grafikon 1: Promena vremena zapošljavanja nakon primene veštačke inteligencije

Izvor: Podaci autora na osnovu izveštaja HireVue, Paradox.ai, LinkedIn Reports (2024–2025).

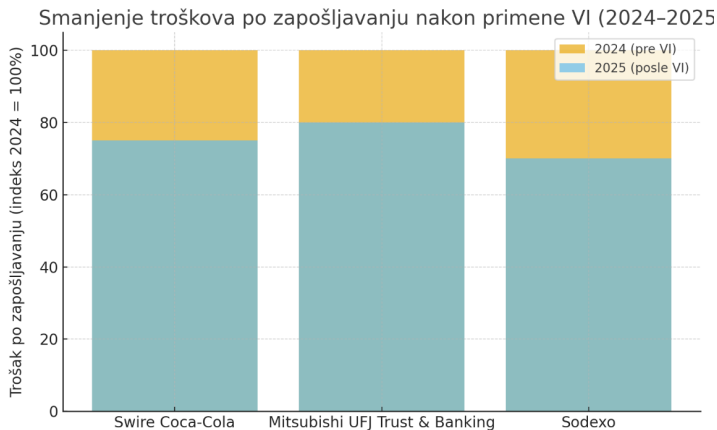
Grafikon 1 prikazuje smanjenje prosečnog vremena zapošljavanja (*time-to-hire*) u posmatranim kompanijama tokom perioda 2024–2025. Uočava se da je najizraženiji efekat zabeležen kod Sodexa, gde je vreme zapošljavanja skraćeno za 60%, zahvaljujući automatizaciji procesa putem *Paradox Conversational ATS* sistema. Swire Coca-Cola beleži smanjenje od 37%, dok je kod Mitsubishi UFJ Trust & Banking zabeležen pad od 32%. Ovi rezultati potvrđuju da primena VI omogućava značajno povećanje operativne efikasnosti i ubrzava donošenje odluka u selekciji kandidata.



Grafikon 2: *Povećanje zadovoljstva kandidata*

Izvor: Podaci autora na osnovu izveštaja HireVue, Paradox.ai, LinkedIn Reports (2024–2025).

Grafikon 2 prikazuje porast zadovoljstva kandidata procesom selekcije, izražen kroz Candidate Net Promoter Score (NPS). Nakon implementacije VI alata, sve tri kompanije beleže rast zadovoljstva kandidata, što ukazuje na pozitivnu percepciju automatizovanih procesa. Najveći porast zabeležen je kod Swire Coca-Cole (+79 NPS), gde kandidati navode da su video-intervjui bili brži i transparentniji. Sodexo beleži NPS od +70, dok je Mitsubishi UFJ Trust & Banking ostvario +58,4, što je posebno značajno s obzirom na visoku konkurenciju u finansijskom sektoru. Ovi podaci ukazuju da VI ne samo da ubrzava proces zapošljavanja, već i poboljšava iskustvo kandidata (candidate experience) kroz efikasnu komunikaciju i transparentnost.



Grafikon 3: *Smanjenje troškova po zapošljavanju nakon primene veštačke inteligencije*

Izvor: Podaci autora na osnovu izveštaja HireVue, Paradox.ai, LinkedIn Reports (2024–2025).

Grafikon 3 prikazuje efekat primene VI na troškove zapošljavanja. Sva tri sistema pokazala su značajno smanjenje troškova po zaposlenom, što se najviše vidi kod Sodexa (–30%) zbog visokog nivoa automatizacije u masovnim zapošljavanjima. Swire Coca-Cola beleži smanjenje troškova za 25%, dok je kod Mitsubishi UFJ Trust & Banking ušteda iznosila 20%. Smanjenje troškova rezultat je automatizacije ponavljajućih zadataka, smanjenja angažovanja eksternih agencija i preciznijeg targetiranja kandidata putem prediktivnih algoritama. Ovi rezultati potvrđuju da VI značajno doprinosi racionalizaciji troškova i povećanju profitabilnosti HR funkcije.

Rezultati pokazuju da primena VI dovodi do značajnog poboljšanja efikasnosti i kvaliteta procesa zapošljavanja. Sva tri sistema — HireVue, Paradox i AI video-analitika — smanjuju administrativno opterećenje HR timova i povećavaju objektivnost selekcije. Međutim, primećeni su i izazovi: kod Swire Coca-Cole, kandidati su izražavali zabrinutost u vezi sa privatnošću snimaka intervjua; dok je u finansijskom sektoru (Mitsubishi UFJ Trust & Banking) istaknuta potreba za većom transparentnošću algoritama i zaštitom od implicitne pristrasnosti. Sodexo je, s druge strane, pokazao da u visoko-volumenskim zapošljavanjima VI značajno smanjuje vreme zapošljavanja i troškove, ali uz rizik da se smanji individualizovani pristup kandidatu.

U periodu 2024–2025, implementacija VI alata u HRM-u dovela je do prosečnog skraćenja vremena zapošljavanja za 42%, smanjenja troškova za 25%, i povećanja zadovoljstva kandidata za 20–30%.

Ove promene potvrđuju da VI nije samo alat za automatizaciju, već i strateški instrument za donošenje odluka zasnovanih na podacima.

ZAKLJUČAK

Transformacija upravljanja ljudskim resursima kroz primenu veštačke inteligencije (VI) predstavlja jedan od najznačajnijih pomaka u savremenom poslovanju. Analiza sprovedena u ovom radu pokazala je da implementacija AI alata u HRM, posebno u procesima selekcije i zapošljavanja, donosi višestruke koristi — od skraćenja vremena zapošljavanja i smanjenja troškova, do povećanja objektivnosti, pravičnosti i zadovoljstva kandidata. Rezultati komparativne studije tri međunarodne kompanije (Swire Coca-Cola, Mitsubishi UFJ Trust & Banking i Sodexo) potvrđuju da primena VI omogućava efikasnije procese odlučivanja i doprinosi stvaranju konkurentne prednosti.

Pored pozitivnih efekata, istraživanje ukazuje i na niz izazova koji prate ovu transformaciju. Najznačajniji među njima odnose se na pitanja etike,

transparentnosti algoritama i zaštite privatnosti podataka kandidata. Iako VI može doprineti smanjenju subjektivnih pristrasnosti, postoji rizik da algoritmi reprodukuju postojeće obrasce diskriminacije ako nisu adekvatno nadgledani i validirani. Stoga je od ključnog značaja uspostavljanje etičkog i regulatornog okvira koji će obezbediti odgovornu upotrebu veštačke inteligencije u HRM praksi.

U budućnosti se očekuje dalja integracija VI u sve segmente HR ciklusa — od prediktivnog planiranja kadrova do razvoja i zadržavanja talenata. HR menadžeri će sve više koristiti kombinovane modele saradnje čoveka i mašine, gde tehnologija preuzima analitičke zadatke, a čovek zadržava ulogu strateškog i etičkog nadzora.

Zaključno, veštačka inteligencija nije samo tehnološki alat, već strateški partner u modernom upravljanju ljudskim resursima. Njena uspešna implementacija zahteva ravnotežu između efikasnosti i humanosti, između podataka i etike. Samo organizacije koje prepoznaju ovu ravnotežu moći će da u potpunosti iskoriste potencijal VI i stvore održive, inkluzivne i inovativne radne okvire za budućnost.

Literatura

- Armstrong, M. (2020): *A Handbook of Human Resource Management Practice* (15th ed.), Kogan Page.
- Becker, B. E., & Huselid, M. A. (2006): "Strategic human resources management: Where do we go from here?", *Journal of Management*, 32(6), 898–925.
- Bissola, R., & Imperatori, B. (2019): "HR 4.0: The digital transformation of human resources", *Management and Organizational Studies*, 7(2), 15–28.
- Black, S. E., & van Esch, P. (2020): "AI-enabled recruitment: Exploring the impact on HRM", *The International Journal of Human Resource Management*, 31(22), 2824–2846.
- Baltezarević, R. (2023): "Uticaj veštačke inteligencije na globalnu ekonomiju", *Megatrend revija*, 20(3), 13–24. DOI: 10.5937/MegRev2303013B
- Brougham, D., & Haar, J. (2018): "Smart technology, artificial intelligence, robotics, and algorithms (STARA): Employees' perceptions of our future workplace", *Journal of Management & Organization*, 24(2), 239–257.
- Brynjolfsson, E., & McAfee, A. (2017): *Machine, Platform, Crowd: Harnessing Our Digital Future*, W. W. Norton & Company.
- Cappelli, P., & Tambe, P. (2020): "HR goes digital: The promise and peril of technology in HR", *MIT Sloan Management Review*, 61(2), 23–31.
- Davenport, T., & Ronanki, R. (2018): "Artificial intelligence for the real world", *Harvard Business Review*, 96(1), 108–116.
- Dessler, G. (2019): *Human Resource Management* (16th ed.), Pearson Education.

- Goodfellow, I., Bengio, Y., & Courville, A. (2016): *Deep Learning*, MIT Press.
- IBM Watson Talent Report. (2019): *How AI transforms recruitment and employee retention*, IBM Research.
- Jarrahi, M. H. (2018): "Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making", *Business Horizons*, 61(4), 577–586.
- Marler, J. H., & Boudreau, J. W. (2017): "An evidence-based review of HR analytics", *The International Journal of Human Resource Management*, 28(1), 3–26.
- McCarthy, J., Minsky, M., Rochester, N., & Shannon, C. (1955): *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Dartmouth College.
- Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020): "Mitigating bias in algorithmic hiring: Evaluating fairness interventions in practice" in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 469–481.
- Russell, S., & Norvig, P. (2021): *Artificial Intelligence: A Modern Approach* (4th ed.), Pearson.
- Stone, D. L., & Deadrick, D. L. (2015): "Challenges and opportunities affecting the future of human resource management", *Human Resource Management Review*, 25(2), 139–145.
- Stone, D. L., Deadrick, D. L., Lukaszewski, K. M., & Johnson, R. (2015): "The influence of technology on the future of human resource management", *Human Resource Management Review*, 25(2), 216–231.
- Tambe, P., Cappelli, P., & Yakubovich, V. (2019): "Artificial intelligence in human resources management: Challenges and a path forward", *California Management Review*, 61(4), 15–42.
- Ulrich, D., & Dulebohn, J. H. (2015): "Are we there yet? What's next for HR?", *Human Resource Management*, 54(2), 147–171.
- World Economic Forum. (2023): *The Future of Jobs Report 2023*, Geneva: World Economic Forum.
- Zimonjić, M. (2025): "The impact of the human factor on the development and importance of aviation communication in maintaining flight safety", *Mega-trend revija*, 22(1), 173–184. DOI: 10.5937/MegRev2501173Z
- Zimonjić, M. (2025): "The importance of applying the asset valuation model to medium-sized enterprises", *Ekonomija – Teorija i Praksa*, 18(2), 15–26. DOI: 10.5937/etp2502015Z

THE TRANSFORMATION OF HUMAN RESOURCE MANAGEMENT THROUGH ARTIFICIAL INTELLIGENCE

Summary: *The development of artificial intelligence (AI) represents one of the key drivers of digital transformation in modern business, with a particularly profound impact on human resource management (HRM). The integration of AI into HR processes enables organizations to enhance efficiency, objectivity, and accuracy in decision-making related to recruitment, selection, evaluation, and employee development. By automating administrative tasks and applying predictive analytics and machine learning algorithms, HR management evolves from an operational to a strategic, data-driven function. This paper analyzes the key aspects of HR transformation through the use of AI, with a special focus on its role in optimizing recruitment and selection processes. Empirical findings indicate that AI contributes to reducing hiring time, increasing fairness and transparency, and improving the candidate experience, while simultaneously raising ethical and regulatory concerns regarding algorithmic transparency and data privacy. The paper concludes that, when applied responsibly and ethically, artificial intelligence has become an indispensable strategic tool in modern human resource management, enabling the creation of more agile, inclusive, and efficient organizations.*

Keywords: *artificial intelligence, human resource management, recruitment, selection, digital transformation, automation, HR ethics, predictive analytics*

ETIČKI ASPEKT U CIVILNOM VAZDUHOPLOVSTVU I TRANSPORTU (CARGO) USLUGE

Apstrakt: Sektor vazdušnog tereta pokazao je otpornost u poslednjim godinama, održavajući stabilnost uprkos značajnim globalnim izazovima. Vazdušni teretni prevoznici imaju ključnu ulogu u ekonomskom rastu, omogućavajući izvoznicima pristup međunarodnim tržištima i obezbeđujući snabdevanje proizvođača i potrošača širom sveta.

Postojeći izazovi uključuju bezbednosne propise, bilateralne sporazume i standarde sigurnosti. Međutim, napredni operateri i aerodromi uspešno sarađuju sa regulatornim telima kako bi ostvarili ciljeve bezbednosti, istovremeno podstičući liberalizaciju tržišta i razvoj sektora.

Sektor se razvio iz fragmentirane podrške u integrisane logističke operacije sa jasnim fokusom na korisnički servis. Aerodromi moraju predvideti promene na tržištu, strateški rasporediti resurse i uskladiti razvoj infrastrukture sa jasnom marketinškom strategijom kako bi zadovoljili potrebe klijenata.

Koordinisane strategije marketinga i razvoja infrastrukture ključne su za optimizaciju rasta vazdušnog tereta i podršku nacionalnoj ekonomiji, pošiljaocima, potrošačima i industriji u celini. Ove strategije će se kontinuirano prilagođavati dinamičnim tržišnim promenama i novim izazovima u narednim godinama.

Ključne reči: vazdušni teret, logistika, aerodromi, razvoj infrastrukture, marketinška strategija, regulatorna usklađenost, ekonomski rast, međunarodna trgovina.

* Megatrend Univerzitet, Beograd – Pravni fakultet, Beograd, Srbija
E-mail: andjelka.racic@gmail.com

UVOD

Civilno vazduhoplovstvo jedno od dve grane vazdušnog saobraćaja pored, između ostalih, prevoza putnika, danas u savremenim svetlu domira u pružanju transportu, prevozu roba i dobara. Ova podvrsta civilnog vazduhoplovstva poznata je i kao air cargo. Konkretno obuhvata sav teret koji se prevozi avionima, osim pošte i prtljaga putnika. Transport se može realizovati kroz posvećene teretne avione ili putem prostora u trupovima putničkih aviona („belly capacity“). Iako količinski predstavlja samo mali deo globalnog transporta – oko 1% ukupne težine robe – vazdušni transport čini značajan deo vrednosti prevezene robe, približno 35%. Ova statistika sugerise da se avionima pretežno prevoze visokovredne pošiljke, dok su jeftiniji, teži i manjoj vrednosti proizvodi uglavnom prepušteni drumskom, železničkom ili pomorskom transportu.

Međutim, vrednost po kilogramu nije jedini faktor koji određuje upotrebljivost vazdušnog transporta. Akademska istraživanja i industrijska praksa ukazuju na niz drugih kriterijuma koji značajno utiču na odluku o korišćenju aviona kao modaliteta transporta. Ovi faktori, često označavani kao „air-eligibility“ kriterijumi, uključuju kako tehničke karakteristike proizvoda, tako i vremenske, logističke i tržišne uslove. Iako istorijski postoji korelacija između vrednosti robe i procenta prevezene težine vazduhom, u savremenim uslovima drugi faktori postaju sve važniji u odabiru optimalnog transportnog moda.

1. ETIČKI ASPEKT U CIVILNOM VAZDUHOPLOVSTVU I TRANSPORTU TERETA

Pored tehničkih, logističkih i ekonomskih faktora, u razmatranju civilnog vazdušnog transporta tereta od izuzetnog značaja je i etički aspekt koji se odnosi na održivost, bezbednost i društvenu odgovornost. Vazdušni transport, iako efikasan i brz, nosi sa sobom izazove u pogledu uticaja na životnu sredinu, prvenstveno kroz emisiju štetnih gasova i buku, što ima dugoročne posledice po klimatske promene i zdravlje ljudi. Etički je pitanje kako industrija može da balansira između ekonomskog razvoja i zaštite prirodnih resursa, uz poštovanje prava zaposlenih, kao i bezbednosti putnika i tereta. Takođe, upravljanje vazdušnim teretom mora biti u skladu sa međunarodnim propisima koji sprečavaju prevoz opasnih materija i trgovinu zabranjenim proizvodima, čime se doprinosi globalnoj sigurnosti i poštenoj konkurenciji. U tom smislu, etika postaje ključni faktor koji oblikuje budućnost civilnog vazduhoplovstva i doprinosi njegovoj održivosti i društvenoj prihvatljivosti.

2. ISTORIJSKI RAZVOJ VAZDUŠNOG TERETA

Civilno vazduhoplovstvo u cargo transportu ima dug istorijat, počev od korišćenja balona, dirigibla i golubova pismoša. Prvi registrovani transport komercijalnog tereta avionom desio se 1910. godine u SAD, kada su transportovane role svile između Dejtona i Kolumbusa. Sledili su eksperimenti sa transportom pošte 1911. godine, dok je 1914. uvedena redovna vazдушna poštanska služba. U Nemačkoj je prvi zvanični poštanski let obavljen 1912. godine, dok je sveobuhvatna poštanska mreža u SAD postavljena tek 1925. godine, kada su uvedene prve ugovorne rute (Contract Airmail, CAM). Nastupanjem Drugog svetskog rata značajno doprinosi transportu vazдушnim putem, omogućavajući masovni prevoz vojne i civilne robe. Istaknuti primeri uključuju transport tereta preko „The Hump“ rute između Indije i južne Kine tokom 1942–1945. godine, kao i vazdušni most za opsednuti Berlin 1948–1949. godine. Zatim, početak 1970-ih godina nastupa period dominacije avio kurirskih službi sa ekspresnom dostavom od vrata do vrata, uključujući DHL (1969) i FedEx (1971), koje su redefinisale koncept logistike i distribucije robe na globalnom nivou. Ulazak širokotrupnih aviona, prvenstveno Boeinga 747, omogućio je transport većih količina tereta po nižoj ceni po jedinici, dok je prvi teretni 747 model Lufthansa operativno koristila 1972. godine. Danas je cargo vazduhoplovstvo jedno od dominantnih oblika ekspresne dostave robe, te je tako do 2018. godine u svetu bilo u funkciji 1.870 teretnih aviona, dod čega su 30% činili veliki širokotrupni avioni (>80 tona), 33% srednji širokotrupni (40–80 tona), a 37% standardni avioni sa kapacitetom do 45 tona. Očekuje se da će globalna flota teretnih aviona porasti na oko 3.260 jedinica do 2037. godine, kroz kombinaciju novih aviona i konverzije putničkih u teretne.¹

3. GLOBALNA LIBERALIZACIJA VAZDUŠNOG TRANSPORTA

2.1. Utvrđivanje cene avio (cargo) transporta

Globalizacija svetskog tržišta je uticala i na avio-industriju. Tokom 1970-ih godina cargo civilno vazduhoplovstvo posaje fleksibilnije u domenu planiranja ruta, vrši se bolja iskorišćenost kapaciteta, te i razvoj novih logističkih modela, uključujući isporuku robe „just-in-time“. Slično, globalna liberalizacija avio-tržišta u Aziji, Latinskoj Americi i Evropskoj uniji otvorila je mogućnosti međunarodnog povezivanja i smanjenja regulatornih prepreka. Razvijaju se novi modeli civilnog cargo vazduhoplovstva. Neke od najznačajniji su: *Model hub-and-spoke*,² primenjen kod

¹ AIR CARGO GUIDE ACI-NA Air Cargo Committee Air-Cargo-Guide.pdf str 15

² je sistemski ili organizaciona struktura u kojoj centralni „hub“ (čvorište) funkcioniše kao glavni punkt za kontrolu, koordinaciju ili distribuciju, dok više „spoke“ (krakova) povezuje

legacy avio-kompanija, i *direktne rute (point-to-point)*³, karakteristične za Low Cost Carriers (LCC), optimizuju troškove i iskorišćenost resursa, dok „Open Skies“⁴ sporazumi omogućavaju veću konkurenciju i internacionalizaciju vazdušnog transporta. Ove promene su značajno doprinele globalnoj integraciji logističkih mreža i postavile vazdušni transport kao ključni element savremenih poslovnih modela.

Nadalje, transpartnost usluga, kao i konkurencija, doprinele su utvrđivanju cene avio (cargo) transporta.

Kako cena usluge ne zavisi od jednog faktora, već on niza povezanih varijabli faktora, opšte je utvrđeno da visokovredne robe često koriste avio-transport, uprkos višim troškovima. Konkretno visokovredne robe obično se transportuju u manjim količinama, što ih čini pogodnim za vazdušni transport. Na primer, zlato se nikada ne kupuje u količinama dovoljnim da ispuni kontejner od dvadeset stopa. Slična logika važi i za elektroniku, precizne instrumente, sofisticiranu industrijsku opremu i druge vredne proizvode koji su manjih dimenzija i težine. Zatim, pojedina roba izoskuje izuzetno brzo i pouzdano dostavljanje. To uključuje kvarljive proizvode, medicinsku robu i sezonske artikle sa striktno definisanim rokovima isporuke. Sa porastom vrednosti robe koja se prevozi, povećava se i rizik nasupanja štete koje se ogleda u krađi ili oštećenju. Vazdušni transport ne samo da omogućava najbrže, već i najbezbednije kretanje robe između destinacija. Vredna roba vezuje velike kapitalne resurse generišući visoke kamate za svoje vlasnike. Uštedom vremena u transportu smanje se i kamata, te ušteda vremena kroz vazdušni transport stoga ima značajniju vrednost kada je u pitanju visokovredna roba. Na kraju, brzi i pouzdani avio-transport omogućava smanjenje nivoa zaliha. Proizvođači mogu koristiti strategiju „just-in-time“ dostave, smanjujući potrebe za velikim skladištima, oslobađajući kapital i smanjujući troškove zastare i držanja zaliha.

Dakle, vazdušni transport omogućava povećanu brzinu, pouzdanost, sigurnost i smanjenje troškova inventara.

2.1. Izbor cargo transporta.

Sa druge strane i u okviru civilnog cargo vazduhoplovstva postavlja se pitanje izbora cargo transporta. U akademskoj literaturi postoji široka rasprava o faktoru izbora modaliteta transporta. Većina istraživanja koristi koncept ukupnih distributivnih troškova (Total Distribution Cost – TDC) kako bi kvantifikovala

periferni čvor sa hub-om. Ovaj model se široko koristi u logistici, transportu, telekomunikacijama i poslovnim mrežama.

³ su model transporta ili distribucije u kojem svaka destinacija ima direktnu vezu sa svakom drugom destinacijom, bez prolaska kroz centralni čvor (hub).

⁴ je međunarodni sporazum između dve ili više zemalja koji omogućava slobodno i neograničeno vazdušno saobraćanje između tih zemalja, sa minimalnim regulatornim ograničenjima. Cilj je da se podstakne konkurencija, povećava izbor letova i unapredi globalni avio-saobraćaj.

uticaj transportnih odluka na ukupne troškove proizvodnje i distribucije. Ispravna procena TDC omogućava kompanijama da optimizuju profitabilnost, a ne da se fokusiraju samo na vidljive troškove transporta. Kao i kod utvrđivanja cene, tako i na izbor transporta (cargo) kao najvažniji faktori su: Vrednost proizvoda, Fizičke karakteristike, Kvarljivost, Predvidljivost potražnje, Geografski faktori.

Konkrtno proizvodi koji imaju višu vrednost, manji obim, višu gustinu, te perishabilni proizvodi, bilo u smislu fizičke propadljivosti (npr. jagode, sveže meso, morske plodove) ili ekonomske propadljivosti (npr. čestitke za Božić), često zahtevaju brzu isporuku. Takođe, nepredvidljiva potražnja zahtevaju brzu isporuku kako bi se izbegli gubici prodaje, što često opravdava upotrebu vazdušnog transporta. Na primer, potražnja za pelena za dojenčad je relativno predvidiva, dok sezonska igračka može zahtevati brzu proizvodnju i distribuciju. Posebno treba naglasiti faktore specifičnih karakteristika tržišta, poput loše razvijene drumskog infrastrukture, sigurnosnih rizika, dugotrajnih carinskih procedura, nepristupačnog terena ili udaljenosti od transportnih čvorišta, koji značajno utiču na izbor vrste transporta. Na primer, unutrašnji gradovi bivšeg Sovjetskog Saveza često su dostupni samo vazduhom. Kao i oklonost da neujednačena distribucija tereta može dovesti do značajnih razlika u cenama povratnih letova, čime se unapređuje ekonomska isplativost vazdušnog transporta za određene proizvode.

Treba napomenuti da se neke robe smatraju „zatvorenim“ za određeni modalitet. Na primer, jagode iz Kalifornije koje se izvoze u Japan mogu koristiti samo vazdušni transport, dok roba poput žitarica, nafte ili drveta koristi isključivo pomorski transport. Većina tereta nije striktno vezana za jedan modalitet, već se izbor vrši na osnovu analize troškova, brzine, pouzdanosti i sigurnosti. Naftu sigurno nećete transportovati avio prevozom, kao ni matične ćelije brodom.

3. Poslovni modeli u vazdušnom transportu tereta

U okviru terente avio industrije koristi se par poslovnih modela, kao dominantno među njima su isključivo teretni prevoznici, integratori (operateri koji isporučuju teret od tačke do tačke, a ne samo od aerodroma do aerodroma), prevoznici sa teretom u putničkom delu aviona (belly cargo) i kombinovani prevoznici koji upravljaju flotom i putničkih i teretnih aviona. To je poslovanje koje vredi razvijati. Prema podacima Međunarodne asocijacije za vazdušni saobraćaj (IATA), ukupni BDP Severne Amerike koji je podržan vazdušnim saobraćajem iznosio je 844 milijarde dolara 2017. godine, a deo toga činilo je 19,2 miliona metričkih tona vazdušnog tereta. U nastavku su opisani ovi poslovni modeli.⁵

⁵ Ibidem str. 12

3.1. Isključivo teretni prevoznici -all-cargo carriers

Upravljaaju namenski teretnim avionima (Cargolux i Atlas Air). Poslovanje im se zasniva većim delom u radu sa špediterima, nego na direktnoj dostavi rodi. Špediteri iznajmjuju proctor avi komanije, komslodiju pakate(robu) u palete I vreše distribuciju korisnicima. Avio komanije I špediteri zaključuju dugoročne ugovore, što omogućava stabilnost poslovanja, ekonomiju obima, smanjenje nabavnih cena i zaštitu od cenovnih oscilacija.

3.2. Prevoznici sa teretom u putničkom delu (Belly cargo)

Putničke avio-kompanije koje obavljaju prevoz tereta u prtljažnim delovima svojih aviona predstavljaju značajan segment tržišta vazdušnog kargo saobraćaja. Ovaj model poslovanja omogućava ostvarivanje dodatnog prihoda korišćenjem postojećih kapaciteta namenjenih putničkom prevozu. Procene ukazuju da se između 40 i 50% ukupnog svetskog vazdušnog tereta transportuje upravo kao belly cargo.

Budući da potražnja za prevozom putnika i tereta potiče iz različitih tržišnih segmenata, usklađivanje kapaciteta i potražnje za teretnim prostorom može predstavljati izazov. Ipak, s obzirom na to da su kapaciteti u prtljažnim delovima već raspoloživi, marginalni troškovi prevoza tereta ostaju niski. Na taj način, prevoz tereta u putničkim avionima može doprineti povećanju ukupne profitabilnosti i efikasnijem iskorišćavanju resursa, naročito na letovima sa manjim brojem putnika.

3.3. Integratori (od vrata do vrata)

Integratori, poznati i kao ekspresni prevoznici, predstavljaju segment avio-teretne industrije koji pruža kompletnu logističku uslugu od pošiljaoca do primaoca, odnosno sistem transporta „od vrata do vrata“. Najpoznatiji predstavnici ovog modela su UPS, FedEx i DHL, koji su globalno prepoznati po visokom stepenu organizovanosti i pouzdanosti. Razvoj elektronske trgovine u poslednjoj deceniji, podstaknut platformama kao što su Alibaba i Amazon, značajno je povećao obim poslova ekspresnih prevoznika. Kao odgovor na rastuću potražnju, kompanije poput SF Express i Amazon Air uspostavile su flote od približno pedeset teretnih aviona svaka, što predstavlja izuzetno brz napredak u relativno kratkom periodu. Karakteristično za ovaj poslovni model jeste vertikalna integracija – integratori obično poseduju i upravljaju celokupnom transportnom infrastrukturom, uključujući avione, vozila za dostavu i centralne logističke centre (hubove). Iako su troškovi ekspresnog prevoza viši u poređenju sa drugim oblicima transporta, ta cena odražava nivo kontrole, brzine i pouzdanosti koje ovaj sistem pruža, kao i sposobnost integratora da samostalno organizuje i koordinira svaki segment procesa isporuke do krajnjeg korisnika.

3.4. Kombinovani prevoznici

Kombinovani prevoznici koriste i putničke i teretne avione. Kao i isključivo teretni prevoznici, oni uglavnom sarađuju sa špediterima koji obavljaju preuzimanje i dostavu robe krajnjim kupcima. Kompanije poput Lufthansa, KLM/Air France, Cathay Pacific Airways i Korean Air imaju flote koje uključuju i putničke i teretne avione, pa se zato svrstavaju u kombinovane prevoznike. Na pojedinim linijama, ovi prevoznici mogu ostvarivati i do polovine ukupnih prihoda upravo od prevoza tereta.

4. Ključni trendovi u vazdušnom kargo saobraćaju

Danas, kada celokupno tržište iziskuje efikasnost, ekonomičnost i transparentu najpovoljniju cenu usluga, novi način distribucije tereta (cargo) se drastično modifikuje u odnosu na prethodna pravila distribucije. Prema ranijoj poslovnoj tradiciji špediteri su koristili informacije o cenama i rasporedu letova kako bi napravili pretpostavke o pošiljkama, danas dostavljaju sve relevantne informacije o proizvodu prevoznici ili distributivnim platformama, a prevoznici bi zatim daju ponudu dostupne opcije na osnovu karakteristika i zahteva konkretne pošiljke. Nakon toga, špediteri vreše odaberu najprikladnije ponude i izvrše rezervaciju.

Međusobna povezanost učesnika u procesu može se značajno unaprediti ako svi koriste iste standardizovane tehnologije i procese.

- Iz perspektive klijenta, karakteristike pošiljke i zahtevi za transport mogu se lako podeliti sa različitim učesnicima u lancu koristeći istu strukturu podataka i tehnologiju.
- Iz perspektive prevoznika, povezanost sa različitim kupcima postaje jednostavnija, što omogućava da se istovremeno primi i obradi mnogo veći broj zahteva za ponudom.
- Platforme trećih strana mogu imati vodeću ulogu u povezivanju učesnika različitih veličina i kapaciteta.

Digitalizacija omogućava pristup podacima u realnom vremenu i bržu reakciju, čime se olakšava proces prodaje i rezervacije za obe strane. Klijenti mogu preciznije definisati svoje potrebe i jednostavno ih ažurirati, dok prevoznici imaju bolju vidljivost svojih rezervacija i mogu pravovremeno informisati zemaljsko osoblje.⁶

Pored već navedenih (prevoznici sa teretom u putničkom delu (Belly cargo)) izmena u poslovanju isporuke robe avio ulugama, naročito nakon COVID -19, dominante promene se ogledaju i u sledećem:

⁶ Air Cargo Distribution Current trends and prospects, [air_cargo_distribution_current_trends_and_prospects.pdf](#) str.1

4.1. Rast e-trgovine

Ekspanzija e-trgovine tokom poslednje decenije značajno je uvećala potražnju za vazdušnim transportom robe. Projekcije pokazuju da će potražnja u ovom segmentu rasti i do 20% u narednih pet godina. Ovaj dinamičan razvoj omogućio je integrisanim ekspresnim prevoznicima stopu rasta koja nadmašuje prosečan rast vazdušnog teretnog saobraćaja. Tako su 2017. godine integratori beležili rast od 11,5%, dok je globalni promet tereta porastao za 10%. Pojava novih konkurenata dodatno je podstakla tržišnu utakmicu. Najznačajniji izazivač duopola FedEx-a i UPS-a postala je kompanija Amazon, koja je razvila sopstvenu mrežu avio-transporta kroz Amazon Air. Sa snažnim finansijskim resursima i inovativnim pristupom, Amazon je uspeo da uspostavi nacionalnu mrežu frejter aviona u funkciji dostave svojih paketa. Iako se nalazi u ranim fazama razvoja, rast e-trgovine već je značajno proširio tržište i stvorio nove prilike za industriju.

4.2. Nekonvencionalni kargo aerodromi

Tradicionalno, najveći teretni promet bio je koncentrisan na velikim međunarodnim čvorištima poput JFK (Njujork), LAX (Los Anđeles), ORD (Čikago), MIA (Majami) i YYZ (Toronto), Minhen, Frankfurt, London, Amsterdam, Tokio, Moskva, kao i niz drugih svetski poznatih aerodroma. Međutim, poslednjih godina beleži se rast aktivnosti na manjim, do tada manje poznatim kargo aerodromima. Ovaj fenomen je prvenstveno posledica rasta e-trgovine i širenja Amazon Air mreže, kao i u poslednje vreme Alibaba express i Temu. Manji aerodromi postali su važna operativna središta zahvaljujući pogodnoj lokaciji u blizini potrošača i manjem stepenu zagušenja, kao i usled specifične strategije koje čine, između ostalih, finansijski podsticaji, niski operativni troškovi i garantovana potražnja lokalnih kompanija.

4.3. Temperaturno osetljiva roba – prehrambeni i farmaceutski proizvodi

Kako je već istaknuto, vazdušni transport posebno je pogodan za kvarljivu robu i proizvode koji zahtevaju striktan temperaturni režim. Potražnja za svežom hranom raste u razvijenim zemljama usled rasta prihoda, porasta stanovništva i sve većeg naglaska na zdravu ishranu. Zahvaljujući naprednim logističkim lancima i inovativnim tehnologijama, razvijeni su specijalizovani kontejneri, sistemi za praćenje temperature u realnom vremenu i namenski kargo terminali. Pored hrane, farmaceutski sektor postao je sve značajniji korisnik vazdušnog transporta, naročito sa rastućim zahtevima globalnog tržišta i starenjem populacije. Kako bi se poboljšala reputacija vazdušnog transporta u pogledu farmaceutskih proizvoda, uvedene su međunarodne sertifikacije (npr. IATA CEIV Pharma⁷), koje

⁷ CEIV Pharma (Center of Excellence for Independent Validators in Pharmaceutical Logistics) je sertifikacioni program IATA-e (Međunarodne asocijacije za vazdušni saobraćaj),

su podigle standarde i unapredile kvalitet usluge. Proces sertifikacije je složen i skup, ali omogućava aerodromima i avioprevoznicima jačanje konkurentnosti i privlačenje korisnika sa specifičnim potrebama.

4.5. Globalna trgovina

Liberalizacija trgovinskih i transportnih politika značajno je ubrzala globalne tokove robe. Koncepti poput „otvorenog neba“, avio-alijansi i fleksibilnijih pravila vlasništva nad kompanijama doprineli su širenju tržišta i postizanju ekonomije obima u industriji. Međutim, poslednjih godina beleže se i tendencije ka protekcionizmu, kroz revizije sporazuma (npr. prelazak sa NAFTA⁸ na USMCA⁹), uvođenje carina i trgovinskih sankcija. Takve politike poslovanja imaju direktan odraz na vazdušni sektor, jer povećavaju neizvesnost i mogu ograničiti slobodne tokove robe. Primer procesa izlaska Ujedinjenog Kraljevstva iz EU (Brexit) pokazuje koliko razgradnja dugotrajnih sporazuma može biti složena i štetna za kontinuitet trgovine.

4.6. Inovativne tehnologije: Blockchain

Blockchain predstavlja decentralizovanu mrežu zasnovanu na transparentnom deljenju podataka između svih učesnika. Za razliku od tradicionalnih centralizovanih sistema, blockchain obezbeđuje verifikaciju transakcija i nepromenljiv trag svih unosa. Time se povećava sigurnost, eliminiše redundantnost podataka i omogućava bolja transparentnost. U avio-industriji blockchain se već testira u oblasti digitalnih dokumenata (npr. tovarni listovi, akreditivi), a potencijalno i u održavanju – kroz digitalne dnevnik servisa, praćenje porekla delova i povećanje njihove sledljivosti. Iako postoje visoka očekivanja, primena blockchain tehnologije u praksi još je u razvoju i otvorena je za dalje istraživanje i standardizaciju.

koji je napravljen da poveća standarde u rukovanju farmaceutskim proizvodima u avio-kargu. Program osigurava da objekti, infrastruktura, procedure, osoblje, sistemi kvaliteta i uslovi skladištenja/transporta ispunjavaju globalno usklađene kriterijume za farmaceutsku logistiku u lancu snabdevanja vazdušnim putem. Cilj je da se obezbede usaglašenost, bezbednost, efikasnost i integritet proizvoda, naročito za lekove visoke vrednosti i osetljive na temperaturu.

⁸ Severnoamerički sporazum o slobodnoj trgovini (NAFTA) bio je prelomni trgovinski sporazum između Sjedinjenih Američkih Država, Kanade i Meksika, čiji je cilj bio uklanjanje trgovinskih barijera i promovisanje ekonomske saradnje između ove tri zemlje.

⁹ USMCA (United States–Mexico–Canada Agreement) je trgovinski sporazum koji je zamenio NAFTA-u. Cilj USMCA je da modernizuje i unapredi trgovinske odnose između Sjedinjenih Američkih Država, Meksika i Kanade, uvodeći nove odredbe o digitalnoj trgovini, intelektualnoj svojini, radnim pravima i zaštiti životne sredine, dok i dalje održava slobodnu trgovinu između tri zemlje.

5.7. Inovativne tehnologije: Dronovi

Razvoj bespilotnih letelica otvara nove mogućnosti za vazdušni teret. Za razliku od putničkog saobraćaja, transport robe putem dronova nosi manji rizik, dok istovremeno nudi brza rešenja u okviru e-trgovine. Kompanije poput Amazona, Google-a (Alphabet), JD.com i brojne druge kompanije razvijaju i testiraju dronske sisteme za dostavu. Upotreba dronova posebno je atraktivna u udaljenim ili infrastrukturno ograničenim oblastima, ali i u urbanim sredinama gde je brzina isporuke ključna. Regulativa u Severnoj Americi još uvek zaostaje, ali primer kompanije Wing Aviation (Alphabet) koja je 2019. godine dobila odobrenje za komercijalnu upotrebu dronova u Virdžiniji pokazuje da se očekuje širenje ovih praksi. Dugoročno posmatrano, dronovi imaju potencijal da postanu integralni deo lanca isporuke u logistici i e-trgovini.

5. BILATERALNI SPORAZUMI O AVIO-SERVISIMA

Međunarodna avijacija uređena je nizom bilateralnih i nekim multilateralnim sporazumima između i među vladama, koji su se razvijali u okviru Čikaške konvencije iz 1944. godine.

Čikaška konvencija, formalno poznata kao *Međunarodna konvencija o civilnom vazduhoplovstvu*, potpisana je 7. decembra 1944. godine u Čikagu, SAD. Ova konvencija predstavlja temelj modernog međunarodnog civilnog vazduhoplovstva i postavila je okvir za bezbedan, efikasan i uređen razvoj međunarodnog avio-saobraćaja. Prvobitno je potpisana od strane 52 države, dok danas gotovo sve zemlje sveta poštuju njene odredbe.

Jedan od ključnih principa konvencije je suverenitet nad vazdušnim prostorom, prema kojem svaka država ima potpuno i isključivo pravo nad svojim teritorijalnim nebom. Istovremeno, konvencija promoviše međunarodnu saradnju, podstičući države da razvijaju vazdušni saobraćaj na način koji je siguran, ekonomski opravdan i u skladu sa međunarodnim standardima.

Konvencija je takođe ustanovila Međunarodnu organizaciju civilnog vazduhoplovstva (ICAO), čija je uloga da postavlja tehničke i operativne standarde i preporuke (SARPs – *Standards and Recommended Practices*) koje države primenjuju u svom vazduhoplovstvu. Kroz ovaj okvir regulisano je licenciranje pilota, sertifikacija letelica i navigacionih sistema, kao i prava putnika i tereta, čime je omogućena veća sigurnost i odgovornost avio-kompanija.

Jedan od najvažnijih doprinosa Čikaške konvencije jeste uvođenje sloboda vazdušnog saobraćaja, koje definišu prava država i avio-kompanija da koriste međunarodne letove. Pet osnovnih sloboda vazdušnog saobraćaja može se prikazati u:

Sloboda	Značenje
1. Sloboda preleta	Avio-kompanija iz jedne države može preleteti preko teritorije druge države bez sletanja.
2. Sloboda tehničkog sletanja	Avio-kompanija može sleteti u drugu državu samo radi tehničkih potreba (gorivo, servis), bez ukrcavanja ili iskrcavanja putnika/tereta.
3. Sloboda prevoza putnika/tereta do druge države	Avio-kompanija može prevoziti putnike ili teret iz svoje države u drugu državu.
4. Sloboda prevoza putnika/tereta iz strane države	Avio-kompanija može prevoziti putnike ili teret iz strane države u svoju državu.
5. Sloboda tranzita	Avio-kompanija može prevoziti putnike ili teret između dve strane države, preko svoje države.

Čikaška konvencija iz 1944. godine ne samo da je postavila pravni i institucionalni okvir za međunarodno vazduhoplovstvo, već je i omogućila kontinuiran rast globalnog avio-saobraćaja, promovišući sigurnost, saradnju i ekonomski razvoj. Danas, više od sedam decenija kasnije, principi ove konvencije ostaju ključni za funkcionisanje međunarodnog civilnog vazduhoplovstva.

Na temelju ovih principa, u drugoj polovini 20. i početkom 21. veka razvijene su politike „Otvorenog neba“ (Open Skies), koje predstavljaju bilateralne ili multilateralne sporazume sa ciljem liberalizacije međunarodnog avio-saobraćaja. Za razliku od tradicionalnih bilateralnih ugovora koji su ograničavali broj letova, kapacitet i cene, sporazumi Open Skies omogućavaju avio-kompanijama potpisničkih država da slobodno uspostavljaju linije, biraju aerodrome i prilagođavaju raspored letova tržišnim zahtevima. Takve politike povećavaju konkurenciju, smanjuju troškove za putnike i korisnike teretnog transporta, a istovremeno podstiču rast avio-saobraćaja i ekonomski razvoj.

Primeri uključuju Sporazum Sjedinjenih Američkih Država i Evropske Unije Open Skies (2007), koji kompanijama omogućava slobodno letenje bez ograničenja kapaciteta ili frekvencije, i sporazume Sporazum Sjedinjenih Američkih Država sa Kanadom, koji je dodatno proširio tržište transatlantskog i severnoameričkog vazdušnog saobraćaja. Kroz ove inicijative jasno se pokazuje kontinuitet između principa Čikaške konvencije i savremenih liberalizacijskih politika – oba pravna okvira teže sigurnom, efikasnom i globalno integrisanom civilnom vazduhoplovstvu.

Nadalje, od 2005 godine, posmatrano kroz prizmu sporazuma Sjedinjenih Američkih Država, kao dominantnog prevoznika u civilnom avio saobraćaju, kao multilateralni sporazumi se navode između:

- Sjedinjene Američke Države / Evropska unija
Sjedinjene Američke Države i Evropska unija postale su prvi Open Skies sporazum 2007. godine (Faza 1), dok su pregovori o njegovoj reviziji završeni 2010. godine (Faza 2). Sporazum reguliše vazduhoplovne odnose između SAD i

svih 27 članica EU, a pristup su mu omogućile i države koje nisu članice EU, poput Islanda i Norveške. Njegova primena proširila je liberalizovane principe Open Skies na države članice EU koje ranije nisu imale bilateralne ugovore sa SAD, kao što je Velika Britanija, dok su pravne restrikcije u pogledu broja avio-kompanija i pristupa ključnom londonskom aerodromu Hitrou ukinute. Sporazum takođe uključuje određena sedma prava slobode za kargo-servise. Evropske aviokompanije sada imaju otvorena sedma prava za transport tereta između SAD i trećih zemalja, dok su američke kompanije ograničene na prava koja su prethodno dogovorena bilateralno sa pojedinim članicama EU, poput Francuske i Nemačke. Zbog ovih dodatnih liberalnih elemenata, sporazum se često naziva „Open Skies plus“.

Jedna od ključnih inovacija je koncept EU avioprevoznika, prema kojem SAD priznaju bilo koju aviokompaniju u vlasništvu ili pod kontrolom državljana bilo koje članice EU da posluje na linijama između EU i SAD. Sporazum je takođe omogućio evropskim aviokompanijama da učestvuju u transportu putnika i tereta u okviru programa Fly America i na međunarodnim tržištima SAD-a gde ne postoji bilateralni ugovor. S druge strane, američkim kompanijama omogućeno je angažovanje stranih avioprevoznika za pružanje međunarodnih usluga, što ranije nije bilo dozvoljeno.

Pored ovih aspekata, sporazum podstiče blisku saradnju SAD i EU u različitim pitanjima, uključujući i primenu ICAO principa balansirano upravljanja bukom na aerodromima. Američki kargo-prevoznici izražavaju zabrinutost da bi potencijalna ograničenja buke na evropskim aerodromima mogla negativno uticati na ekonomsku održivost njihovog poslovanja. Dodatna prava i fleksibilnosti su moguća, ali zahtevaju promene u zakonodavstvu: u SAD-u u pogledu vlasničke strukture aviokompanija, a u EU-u u vezi sa ograničenjima buke. Na primer, ukoliko SAD dozvole većinsko vlasništvo EU državljana nad američkim aviokompanijama, američke kompanije bi zauzvrat mogle dobiti otvorena sedma prava slobode za kargo-servise između EU i drugih država.

- Sjedinjene Američke Države / Brazil
SAD i Brazil su krajem 2010. godine parafirali fazni Open Skies sporazum, koji je konačno stupio na snagu u maju 2019. Sporazum uključuje neograničen broj aviokompanija, otvorene međunarodne rute, deljenje kodova, cene i čartere. Međutim, ne uključuje sedma prava slobode za kargo-servise, iako su SAD predlagale njihovo uvođenje.
- Sjedinjene Američke Države / Kolumbija
SAD i Kolumbija su takođe krajem 2010. postigle fazni Open Skies sporazum. Većina odredbi se odmah primenila na kargo-servise. Nakon završetka fazne primene krajem 2012. godine, pun Open Skies za kombinovane i kargo-servise

je na snazi. Sporazum ipak ne uključuje sedma prava slobode za kargo-servise, mada su SAD predložile njihovo dodavanje.

- Sjedinjene Američke Dražave / Kina

Tokom godina, SAD i Kina su postepeno liberalizovale svoje avijacione odnose. Najznačajniji pomak bio je u maju 2007. godine, kada su se dve strane dogovorile o proširenju prava. Od marta 2011. godine sporazum predviđa neograničene frekvencije, designate i otvorene međunarodne rute, uključujući peta i šesta prava slobode za kargo-servise. Takođe, sporazum nudi posebna sedma prava slobode za kompanije koje uspostave kargo-hub u drugoj zemlji pod određenim uslovima. Ipak, kargo čarteri, kao i kombinovani čarteri, ostaju podložni kvotama na određenim relacijama. Kod kombinovanih servisa i dalje postoje ograničenja u broju designate i frekvencija, uz postepeno povećanje do 2011. Nakon toga dodatna liberalizacija nije sprovedena. Pojavile su se i teškoće u sprovođenju, poput pitanja međusobnog odobravanja „koterminalizacije“ kargo tačaka.

- Sjedinjene Američke Dražave / Japan

SAD i Japan su krajem 2009. godine zaključili Open Skies sporazum, koji je stupio na snagu u oktobru 2010, kada je otvorena četvrta pista na aerodromu Haneda u Tokiju. Sporazum je ukinuo prethodna ograničenja na rute, deljenje kodova, designate, frekvencije i čartere. Omogućio je jednak tretman svih američkih kargo-prevoznika. Međutim, ne uključuje sedma prava slobode za kargo-servise. Godine 2019. Sjedinjene Američke Dražave i Japan su pregovarali o proširenju pristupa Haneda aerodromu, što je američkim kombinovanim prevoznici donelo dodatne letove. Međutim, proširenje prava za kargo-prevoznike nije omogućeno, iako su potvrđena peta prava slobode i mogućnosti „change-of-gauge“.

6. BEZBEDNOSNA OGRANIČENJA U SEKTORU VAZDUŠNOG TERETA

Bezbednost vazdušnog saobraćaja predstavlja jedan od ključnih elemenata za razvoj civilnog vazduhoplovstva i međunarodnu saradnju. Nadzor nad ovom oblašću obuhvata kako međunarodne standarde i regulative, tako i nacionalne mere kontrole. Efikasna koordinacija među međunarodnim i domaćim organizacijama omogućava smanjenje rizika od nesreća, terorizma i drugih kriminalnih aktivnosti u vazduhoplovstvu. Analizirom uloga ključnih organizacija i nadležnih službi u obezbeđivanju bezbednosti vazdušnog saobraćaja, možemo konstatovati da međunarodne i domaće organizacije, zajedno sa aerodromskim službama, čine integrisan sistem bezbednosti vazdušnog saobraćaja. Kroz regulative, standarde,

obuku i nadzor, ove institucije omogućavaju efikasno smanjenje rizika, zaštitu putnika, posade i infrastrukture, te unapređenje globalnog vazduhoplovnog sistema. Kontinuirana međunarodna saradnja i unapređenje standarda ostaju ključni za budući razvoj civilnog vazduhoplovstva.

Najdominatnija za procenu bezbednosti civilnog vazduhoplovstva u Sjedinjeni Američkim Državama (u daljem tekstu SAD) je Federalna uprava za avijaciju (FAA) koja utvrđuje da li avio-kompanije partnera ispunjavaju obaveze propisane Čikaškom konvencijom u vezi sa regulacijom sopstvenih avioprevoznika. Države koje zadovoljavaju minimalne međunarodne standarde dobijaju Kategoriju 1, što omogućava njihovim kompanijama da nastave i prošire operacije u SAD u skladu sa bilateralnim sporazumima. Države koje ne ispunjavaju standarde svrstavaju se u Kategoriju 2, a njihove kompanije mogu nastaviti postojeće operacije pod pojačanim nadzorom FAA, dok nove operacije mogu obavljati samo korišćenjem aviona iznajmljenih od američkih prevoznika ili stranih prevoznika iz Kategorije 1. Zaključno sa novembrom 2012. godine, zemlje klasifikovane kao Kategorija 2 uključuju: Bangladeš, Barbados, Belize, Obalu Slonovače, Kurasao, Demokratsku Republiku Kongo, Gambiju, Ganu, Gvajanu, Haitiju, Honduras, Indoneziju, Kiribati, Crnu Goru, Nauru, Nikaragvu, Paragvaj, Filipine, Srbiju, Sent Marten, Svazilend, Ukrajinu, Urugvaj i Zimbabve. Kompanije iz ovih zemalja ne mogu započeti nove niti proširiti postojeće operacije u SAD, bez obzira na bilateralne sporazume, dok su zemlje koje su unapredile svoj status na Kategoriju 1, kao što su Kuvajt i Tajland, oslobođene ovih ograničenja.

Na domaćem planu, radi osiguravanja bezbednog vazduhoplovnog okruženja u skladu sa međunarodnim standardima i preporučenom praksom, kao i preuzetim međunarodnim obavezama, odgovorni i kvalifikovani inspektorski timovi Direktorata civilnog vazduhoplovstva Republike Srbije kontinuirano nadziru rad svih aktera u vazduhoplovstvu. Ovaj nadzor obuhvata pružaoce usluga u vazdušnom saobraćaju, avio-prevoznike, vlasnike i korisnike vazduhoplova, operatere aerodroma, letilišta i aerodromskih platformi, investitore, vazduhoplovno-tehničke organizacije, vazduhoplovno osoblje, centre za obuku, kao i druga pravna i fizička lica koja obavljaju delatnosti ili pružaju usluge u sektoru vazduhoplovstva. Kada je u pitanju nadzor stranih avio-prevoznika, isključivo se sprovodi u skladu sa obavezama iz Čikaške konvencije, Zakona o vazdušnom saobraćaju i relevantnih podzakonskih akata, koji implementiraju Evropsku uredbu o bezbjednosnom pregledu stranih vazduhoplova na aerodromskim platformama. U skladu sa radnim aranžmanima između Direktorata civilnog vazduhoplovstva Republike Srbije i Evropske agencije za bezbjednost vazduhoplovstva (EASA), Direktorat vrši SAFA inspekcije (Safety Assessment of Foreign Aircraft) i prosleđuje prikupljene podatke u centralnu bazu EASA.

Tokom boravka na teritoriji Republike Srbije, strani vazduhoplovi mogu biti predmet unutrašnjeg i spoljašnjeg pregleda na aerodromskoj platformi od strane ovlašćenih inspektora Direktorata. Pregled obuhvata kontrolu isprava i knjiga vazduhoplova, dokumenata posade, stanja samog vazduhoplova, njegove opreme, kao i odeljaka namenjenih za prevoz putnika, prtljaga, pošte i tereta. Svi predgledi se sporvode u skladu sa procedurama i standardima koje propisuje nadležni organ Evropske unije. Ukoliko, se pojavimi opravdana sumnja da dokumentacija, posada ili tehničko stanje vazduhoplova nisu u skladu sa odgovarajućim međunarodnim standardima bezbednosti, ovlašćeno lice Direktorata preduzima propisane mere utvrđene evropskim regulativama poput upućivanja zahtevata da se vazduhoplov ne koristi dok se problemi ne reše, u skladu sa instrukcijama za kategorizaciju nalaza inspekcija (INST. RI.01/002), kao i kontaktiranja nadležne vazduhoplovne vlasti države operatera ili države registracije u cilju preduzimanja odgovarajućih korektivnih mera, ne samo za konkretni vazduhoplov, već i za druge vazduhoplove koji mogu biti pogođeni ukoliko je nepravilnost od opšteg karaktera. Sve navedene mere su deo šireg okvira saradnje između Direktorata civilnog vazduhoplovstva Republike Srbije i Evropske agencije za bezbednost vazduhoplovstva (EASA), kako bi se obezbedio visok nivo bezbednosti civilnog vazduhoplovstva u skladu sa međunarodnim standardima.

Treba istaći da su standardi bezbednosti kargo-letova manje rigorozni u poređenju sa putničkim operacijama, uključujući: pravila o maksimalnom radnom i letnom vremenu, izveštavanje o vremenskim uslovima, korišćenje alternativnih aerodroma, angažovanje dispečera, opremu za gašenje požara i hitne izlaze za evakuaciju.

Pravilnost i bezbednost civilnog transport (cargo) vazduhoplovstva vrše agencije osnovane na međunarodnom nivou, poput:

- ICAO (Međunarodna vazduhoplovna agencija) propisuje standarde i preporučene prakse za bezbednost vazdušnog saobraćaja i koordinira međunarodne regulative.
- IATA (Međunarodna asocijacija avio-prevoznika) razvija operativne standarde i sertifikate za bezbednost, kao što je IOSA.
- IFALPA (Međunarodna federacija pilota) pruža smernice za postupanje u kriznim situacijama, uključujući otmice.
- IFATCA (Međunarodna federacija kontrolora leta) razvija standarde i obuku za kontrolore leta, čime doprinosi bezbednosti vazdušnog saobraćaja.
- ACI (Međunarodna organizacija aerodroma) postavlja standarde za rad aerodroma i sigurnosne procedure.
- Interpol koordinira međunarodnu borbu protiv kriminala, uključujući terorizam i krijumčarenje u vazduhoplovstvu.
- Međunarodni sud pravde ima nadležnost za rešavanje sporova proisteklih iz Čikaške konvencije (član 84), čime doprinosi pravnom okviru vazduhoplovne bezbednosti.

ZAKLJUČAK

Uprkos izuzetno izazovnim okolnostima sa kojima se sektor vazdušnog tereta suočavao poslednjih godina, industrija je ostala relativno stabilna i sada je u poziciji da nastavi dugoročni trend stabilnog rasta. Vazdušni teretni prevoznici imaju ključnu ulogu u podsticanju ekonomskog rasta, omogućavajući izvoznicima pristup stranim tržištima, kao i snabdevanje proizvođača i potrošača proizvodima iz celog sveta.

Kao i ranije, industrija se suočava sa brojnim izazovima, od kojih su najvažniji pitanja bezbednosti, bilateralni sporazumi i standardi sigurnosti. Ipak, sofisticirani kargo-prevoznici i aerodromi uspešno pronalaze načine za saradnju sa regulatornim telima kako bi se postigli važni ciljevi u oblasti bezbednosti i zaštite, dok istovremeno rade na povećanju liberalizacije međunarodnih tržišta, čime se omogućava dalji rast i razvoj sektora.

Svi učesnici u industriji – prevoznici, aerodromi, špeditorske kompanije i drugi – moraju aktivno učestvovati u primeni strategija regulatornog rasterećenja, kako bi se ostvario puni ekonomski potencijal vazdušnog tereta u korist nacionalne ekonomije, pošiljalaca, potrošača i same industrije.

Tokom poslednjih godina, sektor vazdušnog tereta evoluirao je iz disperzovane avio-podrške u integrisanu i sofisticiranu logističku operaciju sa jasnim fokusom na korisnički servis. Kako globalna tržišta nastavljaju da se dinamično razvijaju, aerodromi moraju razumeti promene koje su se već dogodile i koje će se dešavati u budućnosti, te usmeriti svoje resurse kako bi iskoristili predstojeći rast.

Važno je napomenuti da izolovane marketinške kampanje retko donose značajne rezultate. Razvoj kargo-faciliteta bez jasnog marketinškog fokusa može dovesti do promašenih investicija ili do izgradnje objekata koji ne zadovoljavaju potrebe korisnika. Marketing i razvoj infrastrukture moraju biti usklađeni i imati jedinstvenu strategiju kako bi se postigli najbolji rezultati. Aerodromi koji teže rastu sektora vazdušnog tereta moraju aktivno pratiti potrebe svojih klijenata, ponuditi im jasnu viziju dostupnih mogućnosti i razviti objekte koji zadovoljavaju te potrebe.

Na kraju, strategije marketinga i razvoja infrastrukture predstavljaju trenutni prikaz industrije koja je u stalnom kretanju. Ove strategije će se kontinuirano razvijati kako bi odgovorile na dinamične promene i nove izazove koji će oblikovati sektor vazdušnog tereta u narednim godinama.

Litertarura

- Kreća Avramov: *Međunarodno javno pravo* (Beograd, skripta).
- Agencija pomorske sigurnosti, *ISPS Code (Međunarodni kodeks za bezbjednost brodova i lučkih postrojenja)*, Bar, 2004.
- Babić Obrad, Nestjasov Feđa (2011): *Kontrola leta*.
- Bukovac Puvača Maja, Debeljak-Rukavina Sandra (2007): „Odgovornost za štete prouzrokovane zloupotrebom zrakoplova“, *Zbornik Pravnog fakulteta u Zagrebu*, 58, 1-2.
- Ejodus (2010): *Međunarodna bezbednost: teorije, sektori i nivoi*, *Službeni Glasnik*.
- Filip (2006): *Englesko-srpski rečnik tehničkih termina u evropskim direktivama Novog pristupa i Globalnog pristupa*.
- Gaćinović, Radoslav (2011): *Terorizam u političkoj i pravnoj teoriji*, Medija centar „Odbrana“, 2. dopunjeno izdanje.
- Ivošević Borislav (2011): *Pomorsko pravo*.
- Janić Čedomir, Berković Mladen, Kuletin Ante, Gajić Dejan, Gabrijel Zdravko, Basarić Srđa (1963): *Vazduhoplovno jedriličarstvo*, Savezna uprava za civilnu vazдушnu plovību, Štampa Grafičko preduzeće „Slobodan Jović“.
- Marković Tomislav: *Terorizam kao nekonvencionalna prijetnja savremenoj bezbjednosti*, n.p., n.d.
- Pejanović Ljubo, Bejatović Milorad (2009): *Avioterorizam*.
- Polonščak Filip (2015): *Analiza sustava prihvata i otpreme zrakoplova na zračnoj luci*, Sveučilište u Zagrebu.
- Pomorska enciklopedija, 2. izdanje, Tom 1 (A–Cez), Zagreb: Jugoslovenski Leksikografski Zavod, 1976.
- Pravilnik o posebnim mjerama carinskog nadzora i carinskom postupku za robe koje se koriste za snabdijevanje prevoznih sredstava u međunarodnom saobraćaju, *Sl. list RCG*, br. 78/06.
- Prosenica Petra: *Piratstvo i pranje novca*, Pomorski fakultet u Rijeci.
- Rečnik srpskohrvatskog književnog jezika, 2. fototipsko izdanje, Knjiga I, Novi Sad – Zagreb: Matica srpska – Matica Hrvatska, 1967.
- Rečnik srpskohrvatskog književnog jezika, 2. fototipsko izdanje, Knjiga V, Novi Sad: Matica srpska, 1973.
- Stevan: *Bezbednost vazdušnog saobraćaja*, Univerzitet u Nišu, n.d.
- Stanković (1970): *Vojna enciklopedija*, Tom 1, 2. izdanje, Vojnoizdavački zavod Beograd, Štampa „Mladinska knjiga“ Ljubljana.
- Vučinić Miloš: *Prijetnje od pomorskog terorizma*, Tivat: Fakultet za mediteranske poslovne studije, materijal sa predavanja, n.d.

- Vučković Branko, Vučković Vesna (2012): *Sigurnost i bezbjednost marina i jahti*, Tivat.
- Vujaklija Milan (1980): *Leksikon stranih reči i izraza*, Beograd: Prosveta.
- Zakon o vazdušnom saobraćaju, *Sl. list RCG*, br. 30/12.
- *Sl. list CG*, br. 51/08; br. 46/07; br. 62/2013; br. 20/11; br. 13/07; br. 17/07; br. 6/08.
- *Sigurnost na moru*, Rijeka: Pomorski fakultet u Rijeci, 2001.
- Zec Damir: *Vazdušni saobraćaj*, <http://document.s.tips/documents/vazdusni-saobracaj.html>.
- *Civil Aviation Authority of Montenegro*, http://www.caa.me/index.php?strana=fiksna&id=2&meni_top=2.
- Polonščak Filip: *Međunarodna pravila za izbjegavanje sudara na moru*, <http://www.pfst.unist.hr/uploads/Meunarodna%20pravila%20za%20izbjegavanje%20sudara%20na%20moru.pdf>.
- *International Civil Aviation Organization*, ICAO – *International Civil Aviation Organization*, <https://www.icao.int>.
- *International Air Transport Association*, IATA – *International Air Transport Association*, <https://www.iata.org>.
- *International Federation of Air Line Pilots' Associations*, IFALPA – *The Global Voice of Pilots*, <https://www.ifalpa.org>.
- *International Federation of Air Traffic Controllers' Associations*, IFATCA – *International Federation of Air Traffic Controllers' Associations*, <https://ifatca.org>.
- *Airports Council International*, ACI – *Airports Council International*, <https://aci.aero>.
- *International Criminal Police Organization*, Interpol – *International Criminal Police Organization*, <https://www.interpol.int>

ETHICAL ASPECT IN CIVIL AVIATION AND TRANSPORT (CARGO) SERVICES

Abstract: *The air cargo sector has demonstrated resilience in recent years, maintaining stability despite significant global challenges. Air cargo carriers are vital to economic growth, enabling exporters to access international markets and ensuring the supply of goods to producers and consumers worldwide.*

Key challenges persist, including safety regulations, bilateral agreements, and security standards. However, advanced cargo operators and airports collaborate effectively with regulatory authorities to meet safety objectives while promoting market liberalization and sector development.

The sector has evolved from fragmented air support into integrated logistics operations with a strong focus on customer service. Airports must anticipate market changes, allocate resources strategically, and align infrastructure development with clear marketing strategies to meet client needs. Isolated initiatives risk misallocated investments or facilities that fail to serve users effectively.

Coordinated marketing and infrastructure strategies are essential for optimizing air cargo growth, supporting national economies, shippers, consumers, and the industry. As the sector continues to evolve, these strategies will adapt to dynamic market conditions and emerging challenges in the coming years.

Keywords: *air cargo, logistics, airports, infrastructure development, marketing strategy, regulatory compliance, economic growth, international trade.*

Albina Kecman*

<https://orcid.org/0009-0001-3018-5400>

Vladimir Stanković**

<https://orcid.org/0000-0002-0570-4926>

Paun Lučanović***

<https://orcid.org/0009-0002-1938-1651>

UDK: 330.341.1:005.952

005.961:005.336.1

DOI: 10.5937/MegRev2502095K

Originalni naučni rad

Primljen 09.07.2025.

Odobren 03.11.2025.

ULOGA LJUDSKIH RESURSA U KONKURENTNOSTI I EKONOMSKOM RASTU

Sažetak: *Ljudski resursi – odnosno skup znanja, veština, sposobnosti, iskustva i kreativnosti zaposlenih – predstavlja jedan od najznačajnijih resursa savremene privrede. Znanje, sposobnost i inovativnost radnika utiču na rast produktivnosti, što direktno doprinosi povećanju konkurentnosti preduzeća i ekonomskom rastu zemlje.*

U savremenim ekonomijama, materijalni resursi (poput zemlje, kapitala ili tehnologije) više nisu presudni — ljudski faktor je taj koji omogućava da se ti resursi optimalno koriste. Na mikro nivou, ljudski resursi su ključni za konkurentsku prednost preduzeća, dok je na makro nivou osnova nacionalne konkurentnosti i održivog razvoja.

Ključne reči: *ljudski resursi, konkurentnost, ekonomski rast, obrazovanje*

* E-mail: albinakecman@gmail.com

** E-mail: dedabor@gmail.com

*** E-mail: paunlucanovic3@gmail.com

1. UVOD

Savremeno tržište rada zahteva nove kompetencije, kao što su: digitalna pismenost, analitičko i kritičko mišljenje, sposobnost adaptacije, timski rad i kreativno rešavanje problema.

Kontinuirano obrazovanje (formalno, neformalno i informalno) postaje uslov za održavanje zaposlenosti i konkurentnosti pojedinca i društva.

Indikatori ljudskih resursa u globalnoj ekonomiji su obuhvaćeni u Globalnom indeksu konkurentnosti (Global Competitiveness Index)¹ koji meri: kvalitet obrazovanja, stepen stručnosti radne snage, ulaganja u istraživanje i razvoj, inovativni kapacitet ekonomije. Ovi pokazatelji pokazuju da zemlje koje više ulažu u obrazovanje, obuku i razvoj ljudskih potencijala — imaju viši nivo konkurentnosti i brži ekonomski rast.

Potreba za doživotnim učenjem je posledica: dinamičnog razvoja savremenog društva, brzog tehnološkog napretka, naročito u oblasti informaciono-komunikacionih tehnologija, promene u strukturi zanimanja i radnih zahteva.

Obrazovanje, svakako, ne povećava samo proizvodne rezultate, već čoveku pruža priliku za lični razvoj i veće društveno zadovoljstvo. Jasno je, takođe, da ljudske veštine mogu dati rezultate samo ukoliko ih oni koriste voljno i sa motivacijom.

2. LJUDSKI RESURSI ILI LJUDSKI KAPITAL U NAUCI I PRIVREDNOJ PRAKSI

U nauci i privrednoj praksi pojam ljudskog kapitala još se uvek teško u potpunosti prihvata. Razlog za to leži u izvesnoj odojbnosti prema upotrebi termina „kapital“, koji očigledno podrazumeva i određene vlasničke odnose — čak i kada je reč o čoveku kao mislećoj individui. Ipak, treba imati na umu razliku između ljudskog i vlasničkog kapitala, koji obuhvata proizvodna sredstva i može se tržišnim transakcijama otuđiti. U svakodnevnom ekonomskom rečniku termin „ljudski kapital“ se ne navodi tako često.²

Umesto njega, dugo vremena je bio u upotrebi pojam „čovekova vrednost“ u proceni kompenzacija za smanjenje radne sposobnosti ili smrti pojedinaca, ili određivanja nekih poreskih sistema. Ovaj pojam je danas prihvaćen i uobičajeno se koristi, premda češće u ekonomskoj nauci nego u praksi privrede.

Obrazovanje je osnovni način formiranja ljudskog kapitala, jer razvija znanja, veštine i kompetencije koje povećavaju produktivnost pojedinca.

¹ World Economic Forum (2012): *The Global Competitiveness Report 2014-2015*, Preuzeto 22. Decembra, 2015.

² Alfred Maršal (1956), *Principles of Economics*, Macmillan - London

Istovremeno, ono je predmet interesovanja više nauka – pedagogije, koja proučava procese učenja i vaspitanja, psihologije, koja se bavi motivacijom, kognitivnim procesima i razvojem ličnosti, sociologije, koja istražuje društveni kontekst obrazovanja i njegov uticaj na socijalnu mobilnost i nejednakosti.

Sa stanovišta ekonomije, obrazovanje se posmatra kao ulaganje u ljudski kapital: to ulaganje ima svoje troškove (vreme, novac, resurse), ali i prinose (veće zarade, veća zaposlenost, veća produktivnost). Ekonomski aspekt obrazovanja, dakle, povezuje pojam investicije u ljude sa proizvodnim efektima tih investicija, koji se najčešće mere novčanim pokazateljima — kao što su zarade, prinos na obrazovanje ili ukupni rast nacionalne ekonomije.

Formiranje ljudskog kapitala (obrazovanje, obuka, usavršavanje) zahteva unutrašnju motivaciju pojedinca — želju za učenjem, napredovanjem, ličnim razvojem. Bez motivacije, investicije u obrazovanje ne daju puni efekat.

Korišćenje ljudskog kapitala u praksi (rad, inovacije, produktivnost) zavisi od radne motivacije, odnosno od toga da li pojedinci imaju podsticaje da primenjuju svoja znanja i veštine. U ekonomskom kontekstu, motivacija se povezuje sa sistemima nagrađivanja, mogućnostima napredovanja, priznanjem i organizacionom kulturom koja podstiče kreativnost i inicijativu.

Učenje, odnosno kontinuirano obrazovanje, zahteva izvesne napore koji će biti uloženi samo ukoliko postoje jasni i konkretni motivacioni razlozi. To se odnosi i na primenu već formiranog ljudskog kapitala, kako u privrednim, tako i u brojnim neprivrednim delatnostima, koje u značajnoj meri utiču na poslovanje privrede, njen rast i razvoj.

Privredni razvoj nije samo povećanje obima proizvodnje ili rasta BDP-a. On podrazumeva i kvalitativne promene u ekonomskoj strukturi, kao što su: tehnološke inovacije, modernizacija proizvodnje, povećanje efikasnosti, razvoj novih sektora i usluga, unapređenje institucija i organizacija.

Sve te promene ne mogu nastati bez ljudskog kapitala — jer upravo ljudi osmišljavaju, organizuju i realizuju te procese.

Drugim rečima, ljudski kapital nije samo faktor proizvodnje, već nosilac promena u celokupnom ekonomskom sistemu. Ovi elementi imaju značajan uticaj na neto zarade, nivo zaposlenosti, kao i na odnos između štednje i potrošnje, što direktno određuje i obim ulaganja u ljudski kapital. Intenzitet delovanja institucionalnih faktora razlikuje se od zemlje do zemlje, pa je shodno tome i njihov uticaj na ponašanje učesnika na tržištu znatno različit.

3. KONKURENTNOST KAO IZAZOV SAVREMENOG DRUŠTVA

U uslovima globalizacije, konkurentnost država predstavlja sposobnost jedne privrede da: proizvodi robe i usluge koje mogu uspešno da se prodaju na međunarodnom tržištu, održava visoku zaposlenost, obezbedi stabilan ekonomski rast i rast životnog standarda stanovništva. Poboljšanje konkurentnosti nije kratkoročan proces — ono zahteva duboke strukturne i institucionalne promene, uz snažno oslanjanje na ljudski kapital, inovacije i efikasne politike države.

U takvim okolnostima, konkurentnost postaje ne samo cilj, već i sredstvo („oružje“) za izlazak iz krize. To znači da države: nastoje da poboljšaju svoje ekonomske performanse (produktivnost, izvoz, inovacije), podstiču investicije u obrazovanje i istraživanje, jačaju institucije tržišta, razvijaju preduzetničku klimu i digitalnu transformaciju.

Razvoj kao višeslojan proces Prema Todaru i Smitu (2006), razvoj nije samo ekonomski rast, već višeslojan proces društvenih promena koji obuhvata: transformaciju društvenih struktura (institucije, tržišta, obrazovanje, zdravstvo), promenu stavova i vrednosti ljudi (radna etika, inovativnost, odgovornost, solidarnost), evoluciju institucija države koje treba da obezbede jednake šanse i pravičnost u društvu.³

Cilj takvog razvoja je izgradnja modernog, inkluzivnog i održivog društva, u kome se podjednako vrednuju: ekonomska efikasnost, socijalna pravednost i kvalitet života građana. Preduslovi za savremeni model razvoja jesu: pravedna socijalna politika, smanjenje siromaštva, univerzalno obrazovanje (dostupno svima, kao osnova za jednake šanse), povećanje kvaliteta života, jačanje demokratskih institucija i razvoj društvenih vrednosti kao što su solidarnost, tolerancija i odgovornost.

U tom smislu, ljudski kapital postaje ključni element svakog uspešnog modela razvoja — jer samo obrazovani, zdravi i motivisani pojedinci mogu podsticati i održavati pozitivne promene u društvu.

Životni standard neke zemlje zavisi od njene sposobnosti da proizvodi robe i usluge, što je direktna funkcija produktivnosti.⁴ Produktivnost zavisi od četiri ključna faktora: fizički kapital (mašine, zgrade, infrastruktura), ljudski kapital (znanje, obrazovanje, veštine i zdravlje radne snage), prirodni resursi (zemljište, rude, energenti), tehnološko znanje (sposobnosti primene nauke u proizvodnji i inovacijama).⁵ Odnos između ova četiri faktora određuje dugoročni ekonomski rast i razlike u životnom standardu među zemljama.

³ Todaro, P.M. & Smith, S.C. (2006): *Ekonomski razvoj*, Šahinpašić - Sarajevo.

⁴ Mankiw, N.G., & Taylor, M.P. (2008): *Ekonomija*, Data Status - Beograd.

⁵ Mankiw, N.G., & Taylor, M.P. (2008): *Ekonomija*, Data Status - Beograd.

4. UTICAJ GLOBALNE EKONOMSKE KRIZE

Globalna ekonomska kriza, koja je započela u SAD 2008. godine, imala je širok i dugotrajan efekat na ceo svet: pad investicija, rast nezaposlenosti, usporavanje proizvodnje i izvoza, povećanje javnog duga.

Posebno su pogođene tranzicione ekonomije — zemlje koje su u procesu prelaska sa planske na tržišnu ekonomiju (poput Srbije). Te zemlje imaju nedovoljno razvijene institucije, nestabilan finansijski sistem i ograničene resurse za podsticanje razvoja.⁶

Prosečan prihod u najbogatijim zemljama sveta je deset puta veći od onog u najsiromašnijim. To rezultira ogromnim razlikama u: kvalitetu života, pristupu zdravstvu i obrazovanju, životnom veku, tehnološkom napretku, mogućnostima za zapošljavanje i lični razvoj.

Iako su razlike u prihodima očigledne, uzroci tih razlika su složeni i manje vidljivi. Postavljaju se ključna pitanja razvojne ekonomije: Zašto neke zemlje uspevaju da postanu ekonomski prosperitetne, dok druge zaostaju? Koji je odnos između institucija, obrazovanja, tehnologije i kulture u procesu razvoja? Kako bogate zemlje mogu očuvati svoj standard bez produbljivanja globalnih nejednakosti? I, najvažnije: šta nerazvijene zemlje mogu da učine da se pridruže klubu razvijenih? Odgovori na ova pitanja vode ka saznanju da su investicije u ljudske resurse – kroz obrazovanje, zdravlje, istraživanje i inovacije – najpouzdaniji put ka dugoročnom i inkluzivnom razvoju.

Mnogi istraživači tvrde da globalizacija dovodi do smanjenja siromaštva. U uzorku od 80 zemalja rast prihoda najsiromašnijih bio jednak prosečnom rastu BDP-a po glavi stanovnika.⁷ Kako je utvrđeno da globalizacija ima pozitivnu korelaciju sa ekonomskim rastom, iz toga proizilazi zaključak da ona utiče na smanjenje siromaštva. Pojedini autori ističu da je smanjenje siromaštva bilo relativno ograničeno u odnosu na postignute stope rasta.⁸ Povećanje nejednakosti onemogućilo je značajnije ublažavanje siromaštva.⁹

Posmatranje siromaštva na globalnom nivou ima brojne nedostatke, jer, pre svega, zanemaruje regionalne specifičnosti i različite trendove u pojedinim delovima sveta. Pretpostavimo da postoje samo dva faktora proizvodnje - rad i kapital. Polazi se od pretpostavke da će se zemlje u međunarodnoj trgovini specijalizovati u skladu sa obiljem ovih faktora. Prema ovoj teoremi, u procesu međunarodne

⁶ Drucker, P.F. (2008): *Management*, Collins - New York.

⁷ Dollar, D. and Kraay, A. (2001): *Trade, Growth and Poverty*, The World Bank, Development Research Group - Washington.

⁸ Vandermoortele, J. (2002): *Are we really reducing global poverty*, UNDP - New York.

⁹ Chen, S. and Ravallion, M. (2000): *How Did the Poorest Fare in the 1990s?*, World Bank, Development Research Group - Washington.

trgovine dobitnici će biti vlasnici faktora proizvodnje kojim zemlja obiluje, dok će gubitnici biti vlasnici faktora kojeg je u manjku. Shodno tome, ukoliko zemlja raspolaže relativno većim količinama kapitala, očekuje se povećanje nejednakosti. Nasuprot tome, ako zemlja ima relativno više radne snage, razlika u prihodima će se smanjivati. U državama sa ograničenim ljudskim kapitalom, globalizacija može takođe doprineti smanjenju jaza, zahvaljujući lakšem pristupu znanju (na primer, putem interneta), što umanjuje premiju na ulaganja u ljudski kapital.¹⁰

Globalizacija deluje i preko obrazovanja. Otvorenost ekonomije doprinosi poboljšanju kvaliteta obrazovanja.¹¹ Prema istraživanjima, porast prosečnog broja završenih razreda u obrazovanju dovodi do smanjenja nejednakosti.¹² Iako globalizacija u određenoj meri nepovoljno utiče na raspodelu dohotka unutar pojedinih zemalja, to ne znači da se rast i pravednost međusobno isključuju. Ključ leži u promišljenoj kombinaciji ekonomskih politika koje istovremeno podstiču rast i ublažavaju socijalne razlike. Problem je u tome što, osim obrazovanja, gotovo da nema faktora koji istovremeno imaju pozitivan uticaj i na rast i na smanjenje nejednakosti.¹³ Zbog toga je neophodno sprovesti korektivne mere usmerene na ublažavanje negativnih efekata globalizacije na raspodelu dohotka i socijalnu pravdu.

5. STRATEGIJA RAZVOJA LJUDSKIH RESURSA U SRBIJI

U stručnim krugovima često nailazimo na kontradiktorne stavove o obrazovanju i znanju u Srbiji. Razlozi za visoku nezaposlenost u ovoj zemlji uključuju nedovoljno direktnih stranih investicija, mali broj dostupnih poslova, veliki broj nisko kvalifikovanih radnika, kao i neadekvatan obrazovni sistem, koji proizvodi diplomce koji nakon završetka škole ostaju bez posla. Postoji jasna nesrazmera između obrazovnog sistema i tržišta rada, naročito u vezi s praktičnim znanjem i veštinama.

Problem se povećava kada diplomci i dalje nemaju potrebne veštine, sposobnost da samostalno rešavaju probleme, analitičko razmišljanje, ili veštine timskog rada. S obzirom na to da ekonomski razvoj postavlja sve veće zahteve za kvalifikacijama potrebnim za ulazak u radnu snagu, može se očekivati da će osnovni uslov

¹⁰ Taylor, A. (2002): "Globalization, Trade and Development: Somme Lessons from History", *NBER Working Paper Series*.

¹¹ Rodrik, D. (1998): "Why do more open economies have bigger governments?", *Journal of Political Economy*, 106(5), 997-1032, Forthcoming.

¹² Lundberg, M. and Squire, L. (2000): "The Simultaneous Evolution of Growth and Inequality", *World Bank Working Paper*.

¹³ Lundberg, M. and Squire, L. (2000): "The Simultaneous Evolution of Growth and Inequality", *World Bank Working Paper*.

za zapošljavanje uskoro biti završena srednja škola. U tom kontekstu, ključna promena u srednjem stručnom obrazovanju treba da bude uspostavljanje fleksibilnog sistema koji će odgovarati novim zahtevima tržišta rada i obezbediti sticanje znanja i vrednosti za brži i kvalitetniji profesionalni razvoj.

Kvalitetno visoko obrazovanje treba da proizvodi stručnjake sposobne da se suoče sa oštrom međunarodnom konkurencijom. Univerzitet bi trebao biti viđen kao centar za sticanje znanja, obavljanje profesionalnih zadataka, i prostor za kulturni i društveni razvoj. Od suštinske je važnosti razvijanje saradnje između univerziteta, privrede i međunarodnih institucija.¹⁴

Konkurentska pozicija Srbije nisu povoljna. Prema rezultatima Globalnog indeksa konkurentnosti, Srbija zaostaje u oblasti inovativnosti, institucionalne efikasnosti i tržišta rada; nedovoljno ulaganje u ljudski kapital i obrazovanje ograničava sposobnost privrede da se prilagodi savremenim izazovima; dominiraju stare proizvodne strukture, a nedostaje dovoljno tehnoloških inovacija i znanja.

Iz ovih razloga je neophodno da država usmeri pažnju na: reformu obrazovnog sistema, razvoj veština u skladu sa tržišnim potrebama, podsticanje istraživanja, inovacija i preduzetništva, jačanje institucionalnih kapaciteta i transparentnosti.¹⁵

Poseban naglasak stavljen je na potrebu da Srbija: razvija državnu politiku u oblasti ljudskog kapitala, jača obrazovni sistem kao strateški resurs, unapređuje kvalitet nastave i usaglašenost sa tržištem rada, podstiče inovativnost, preduzetništvo i digitalne veštine. Cilj takve politike je da se poveća konkurentnost nacionalne ekonomije i obezbedi održiv ekonomski rast.

6. ZAKLJUČAK

U eri globalizacije i mnogobrojnih reformi, kada kapital dolazi do izražaja, može se sa sigurnošću reći da je ključni faktor u razvoju privrede produktivnost rada. Ona se temelji na znanju, inovacijama i domišljatosti, odnosno na jačanju ljudskog kapitala. S obzirom na to da želimo da izgradimo konkurentnu prednost nacionalnih razvojnih subjekata, upravljanje treba da se fokusira na politiku, praksu i strukturu koje će zajednički uticati na ponašanje organizacija te na njihove poglede i radnu efikasnost.

Povećanje produktivnosti kod ljudi može se postići obrazovanjem i rastom prihoda, što predstavlja ulaganje u ljudski kapital. Savremeni razvojni trendovi u zemljama s tržišnom privredom pokazali su da su obrazovanje i formiranje

¹⁴ Mitrović, V., Mitrović, I. (2015): "Uloga ljudskog kapitala u povećanju konkurentnosti privrede Srbije", *International Scientific Conference of IT and Business-Related Research*, Ekonomski fakultet u Kos.Mitrovici, Srbija.

¹⁵ World Economic Forum (2012): *The Global Competitiveness Report 2020-2021*.

ljudskog kapitala, posebno u kontekstu razvoja i implementacije novih tehnoloških dostignuća, na vrhu prioriteta globalnih nacionalnih strategija i politika koje se bave socijalnim, ekonomskim i tehnološkim napretkom.

Povećanje konkurentnosti nije moguće bez sistematskog ulaganja u ljude — u njihovo obrazovanje, zdravlje, motivaciju i društveno okruženje koje podstiče rad i stvaralaštvo. Ljudskiresursi su osnovni stub izlaska iz krize i izgradnje održive ekonomije.

Literatura

- Chen, S., Ravallion, M. (2000): *How Did the Poorest Fare in the 1990s?*, World Bank, Development Research Group – Washington.
- Dollar, D., Kraay, A. (2001): *Trade, Growth and Poverty*, The World Bank, Development Research Group – Washington.
- Lundberg, M., Squire, L. (2000): “The Simultaneous Evolution of Growth and Inequality”, *World Bank Working Paper*.
- Maršal, A. (1956): *Principles of Economics*, Macmillan - London
- Mankiw, N.G., Taylor, M.P. (2008): *Ekonomija*, Data Status - Beograd.
- Petrović, P. (2010): „Uticaj ljudskih resursa na privredni rast i razvoj Srbije“, *Ekonomski horizonti*, 12(1), str. 103-119
- Rodrik, D. (1998): “Why do more open economies have bigger governments?”, *Journal of Political Economy*, 106(5), 997-1032, Forthcoming.
- World Economic Forum (2018): *The Global Competitiveness Report*.
- World Economic Forum (2019): *The Global Competitiveness Report*.
- Taylor, A. (2002): Globalization, “Trade and Development: Somme Lessons from History”, *NBER Working Paper Series*.
- Todaro, P.M., Smith, S.C. (2006): *Ekonomski razvoj*, Šahinpašić - Sarajevo.
- Vandermoortele, J. (2002): *Are we really reducing global poverty*, UNDP - New York.
- Mitrović, V., Mitrović, I. (2020): “Uticaj ljudskog kapitala u povećanju konkurentnosti privrede Srbije“, *International Scientific Conference of IT and Business-Related Research*, Ekonomski fakultet u Kos.Mitrovici, Srbija.
- Zjalić, Lj.M. (2011): *Razvoj ljudskih resursa u funkciji Struktural nih promena i novih uslova rada: inovativnost - Nezaobilazan činilac razvoja*, Fakultet za menadžment malih i srednjih preduzeća, Beograd.

THE ROLE OF HUMAN RESOURCES IN COMPETITIVENESS AND ECONOMIC GROWTH

Abstract: *Human resources - that is, the set of knowledge, skills, abilities, experience and creativity of employees - is one of the most important resources of the modern economy. The knowledge, ability and innovation of workers influence the growth of productivity, which directly contributes to increasing the competitiveness of companies and the economic growth of the country.*

In modern economies, material resources (such as land, capital or technology) are no longer crucial — it is the human factor that enables these resources to be used optimally. At the micro level, human resources are key to a company's competitive advantage, while at the macro level, it is the basis of national competitiveness and sustainable development.

Keywords: *human resources, competitiveness, economic growth, education*

Marko Stanojević*
<https://orcid.org/0009-0007-7241-5503>
Danilo Izgarević**
<https://orcid.org/0009-0000-0785-3055>

UDC: 005.961:005.336.1
005.73:005.934

DOI: 10.5937/MegRev2502105S

Original scientific paper

Received 15.06.2025.

Approved: 17.09.2025.

THE ROLE OF HUMAN RESOURCE MANAGEMENT IN ENHANCING CORPORATE INFORMATION SECURITY CULTURE

Abstract: *Organizations are increasingly wrestling with the task of safeguarding their digital and physical assets, especially as security threats, both from within and outside, grow more complex. While technological solutions are crucial, human behavior remains one of the most significant and vulnerable aspects of corporate security systems. This paper examines the key role of Human Resource Management (HRM) in fostering and bolstering a solid corporate security culture. It examines how various HRM functions, including recruitment, onboarding, employee training, policy enforcement, and performance evaluations, can be effectively leveraged to shape employee behavior, decrease human error, and strengthen the overall resilience of the organization. This paper introduces a novel viewpoint on Human Risk Management, which seeks to identify, assess, and mitigate the vulnerabilities associated with human actions. This includes issues like falling for phishing scams, insider threats, and mishandling data. It specifically addresses the challenges that come with hybrid and remote work environments, where security risks can increase due to the spread of technology and communication hurdles. The paper highlights how essential it is to align security awareness programs with the overall culture and values of the organization. It suggests moving away from the usual compliance-focused training and instead adopting more engaging, behavior-driven approaches.*

Keywords: Human Resource Management, Information Security, Corporate Security, Human Risk, Cybersecurity Awareness

* E-mail: stanojevic.marko799@gmail.com

** E-mail: daniloizgarevic@gmail.com

1. INTRODUCTION

Organizations are tasked with the challenging job of keeping operations running smoothly while also protecting both their physical and intangible assets from various security threats. Human Resource Management (HRM) plays a key role in influencing how employees understand, respond to, and follow security guidelines, which ultimately shapes the overall security culture of the company. This culture consists of the shared values, beliefs, practices, and behaviours that dictate how seriously security is regarded at all levels. Creating a strong security culture is essential for reducing insider threats, ensuring compliance with security policies, and strengthening the organization's overall resilience.

Numerous studies have highlighted that the culture within an organization greatly influences how employees deal with information security. In settings where there's a strong emphasis on internal focus, control, or hierarchy, employees are generally more likely to follow security policies.¹ Additionally, human resource management (HRM) practices, like thorough background checks, continuous security training, performance reviews tied to security outcomes, and monitoring are vital for boosting information systems security.² Studies in similar environments have found a strong link between HR processes and the success of information security measures, underscoring HR's essential role in connecting organizational policies with employee security behaviour.³

Cultural alignment looks to be an essential factor in how effective HRM interventions can be. Studies focusing on organizational culture and information security culture indicate that the broader corporate culture can impact whether specific security subcultures flourish or falter.⁴ When employees connect with common values, it can really enhance information security practices, often bolstered by aspects like psychological capital.⁵ It's interesting to note that while we often talk

¹ Karlsson, M., Karlsson, F., Åström, J. & Denk, T. (2022): "The effect of perceived organizational culture on employees' information security compliance", *Information and Computer Security*, 30(3), 382-401.

² Kumah, P. (2022): "The Role of Human Resource Management in Enhancing Organizational Information Systems Security" in: *Research Anthology on Business Aspects of Cybersecurity* (pp.300-325).

³ Al-Thunaibat, M.Y., Al-shawabkeh, A.A. & Al-baqor, K. K. (2020): "The Role of Human Resource Management Processes in Achieving Information Security: An Applied Study on Saudi Government Universities", *Management & Economics Research Journal*, 2(3), 1-23. DOI: 10.48100/merj.v2i3.107

⁴ Solomon, G., & Brown, I. (2021): "The influence of organisational culture and information security culture on employee compliance behaviour", *Journal of Enterprise Information Management*, 34(4), 1203-1228.

⁵ Riemenschneider, C. K., Burney, L. L & Bina, S. (2023): "The influence of organizational values on employee attitude and information security behavior: The mediating role of

about safety culture in terms of physical health, it actually has a lot in common with security culture. When we look at HRM practices that promote a safety culture, like training, engaging employees, and changing mindsets, we see that these elements are also crucial for building a robust security culture.⁶

Employee interactions with policies, sharing of sensitive information, and interpretation of organisational regulations are all impacted by communication in virtual settings, particularly within legal-informatics systems. A security-oriented culture can be strengthened by reducing uncertainty and the danger of non-compliance through efficient virtual communication channels supported by transparent legal-informatica protocols.⁷ HR must make use of this communication infrastructure in companies where remote or hybrid work is prevalent in order to establish security standards, direct employee conduct, and guarantee responsibility in dispersed environments. According to a 2024 study of IT and security experts, almost 87% of participants were employed by companies that provide quarterly or more training to staff members on how to recognise cyberattacks. Furthermore, 33% of respondents stated that they are afraid about human error and faults in how staff members respond.⁸

While interest in this area is on the rise, we still face significant gaps in understanding how HRM can best design, implement, and uphold a security culture that works across different industries and national settings. The differences in organizational cultures, employee values, and outside regulatory pressures indicate that a “one-size-fits-all” approach to HRM security strategies might not work. Additionally, there’s still a lack of empirical research that clearly outlines how HRM practices lead to tangible improvements in security culture and the resulting security outcomes.

This paper sets out to explore the ways in which certain HRM strategies can improve the security culture within companies. It aims to identify the most effective HRM practices, understand their interaction with organizational culture, and uncover the factors that can either promote or impede their successful implementation.

psychological capital”, *Information and Computer Security*, 31(2), 172-198.

⁶ Al-Mekhlafi, A.-B. A. (2025): “Importance of Effective Human Resources Management in Creating a More Secure Work Environment by Improving Safety Culture”, *International Journal of Intellectual Human Resource Management (IJIHRM)*, 5(01), 14-23.

⁷ Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku”, *Megatrend Revija*. 17(4), 27-40. DOI: 10.5937/MegRev2004027B

⁸ Petrosyan, A. (2025): *Human risk management in global organizations 2024*, https://www.statista.com/statistics/1622615/human-risk-management-global/?srsltid=AfmBOooug_aRonZEFQYjDazd0Q1vLnuU5Kv6BllQZoyl73Ksc3u46y.

2. LITERATURE REVIEW

Employees at a certain organisation with a range of backgrounds and expertise make up its human resources. In the social sciences, this word refers to the workforce as one of the three means of production; in the economic unit management context, it refers to specific employees and business departments that deal with personnel policy.⁹ On the other hand, human resource management encompasses all aspects of personnel management, including hiring, onboarding, performance reviews, and training. It involves developing a productive workforce that advances organisational objectives. The goal of human risk management is to recognise and reduce the hazards associated with human conduct. These two HRMs have a complimentary relationship. While human risk management makes sure those personnel perform securely, human resource management lays the groundwork by recruiting, educating, and involving staff members.¹⁰ Human Risk Management could identify employees who are more susceptible to phishing attempts and offer more focused training, while Human Resource Management might offer broad security awareness training. Human Risk Management guarantees compliance through frequent audits and feedback loops, whereas Human Resource Management may develop regulations pertaining to data handling.¹¹

The creation of a powerful personal brand and a consistent marketing communication plan show how people's actions, how they portray themselves, and how they internalise their principles can affect how others perceive their professionalism, accountability, and trustworthiness inside a company.¹² Similar dynamics can be used by HRM to reinforce a security culture by motivating staff members to internalise organisational security values and act in ways that consistently reflect those values. Putting a strong emphasis on communication that is honest, aligned with values, and consistent helps minimise the gaps between what individuals do and what organisations demand.

Human risk is the possibility that an individual's activities, whether deliberate or not, and whether coming from within or without, will disrupt or harm an organisation. Human risk, also referred to as human error, is a topic that has

⁹ Pujer, K. (2017): "Zarządzanie rozwojem pracowników. Założenia teoretyczne i praktyczne egzemplifikacje", in: Buzowska, B., Paliga, R., Pujer, K.: *Zarządzanie personelem w organizacji. Wybrane problemy teorii i praktyki*. Wydawnictwo Exante, Wrocław.

¹⁰ Baltezarević, B., Baltezarević, R., & Baltezarević, V. (2018). Aktivnosti starijih osoba na onlajn društvenim mrežama. *Megatrend revija*, 15(3), 167.

¹¹ Robinson, K. (2024): *HRM: The Difference Between Human Risk and Resource Management in Cyber Security*, <https://www.metacompliance.com/blog/cyber-security-awareness/hrm-human-risk-and-resource-management>.

¹² Milovanović, S., Lukinović, M. & Baltezarević, R. (2018): "Lični brend i integrisano market-ing komuniciranje", *Megatrend revija*, 15(1), 177-186. DOI: 10.5937/MegRev1801177M

recently gained attention from the cyber security sector, which is always trying to stay one step ahead of its enemies. Because AI-based security solutions have made it easier and more common to thwart broad attempts, cybercriminals have turned their attention to focused tactics that capitalise on human error. In order to prevent this increasing human risk, organisations must change.¹³ One of the most important issues for businesses is still the protection of HR data. Due to the digital storage of sensitive employee data, such as addresses, banking information, and social security numbers, businesses are finding it more and more difficult to safeguard this information from ever-increasing dangers. HR teams must give strong data security measures top priority in order to reduce risks due to the growth of remote and hybrid work, a changing regulatory environment, and an increase in cyberattacks.¹⁴

It is the duty of all employees and other stakeholders in an organisation to ensure the security of HR data. However, there is a unique and significant responsibility for the human resources department. It should guarantee that every employee receives adequate data protection training. Additionally, they must develop and implement policies that protect all of the organization's data. It is the HR team's duty to make sure that data is gathered, examined, and interpreted appropriately, adhering to national and international regulations. It should also determine and put into effect data access controls for every employee. The department is responsible for assisting in the handling of employee-related internet security events under the direction of the HR manager. In order to manage such occurrences and lessen the impact of the attack, it can be very helpful to develop a crisis management plan in conjunction with other departments.¹⁵

The utilisation of computer technologies and strategies for preventing online attacks on the business are particularly significant aspects of human resources education.¹⁶ Although there are many factors to take into account when creating a successful cyber security policy, legal actions are crucial in stopping and thwarting cybercrime. Every aspect, including criminalisation, jurisdiction, procedural powers, international collaboration, and internet service provider duty, requires legislation. In particular, criminalization, the creation of specific criminal offences for common cybercrime acts, is the main focus of national

¹³ Mimecast (2025): *Human Risk Management, Mitigating insider threats through proactive Human Risk Management in cybersecurity*, <https://www.mimecast.com/content/human-risk-management-in-cyber-security/>.

¹⁴ Foxall, D. (2025): *Six basic HR data security threats in 2025*, <https://www.hrmsworld.com/hr-data-security-threats.html>.

¹⁵ Talkspirit (2024): *Best Practices for Ensuring HR Data Security*, <https://www.talkspirit.com/blog/best-practices-ensuring-hr-data-security>.

¹⁶ Baltezarevic, B., Milutinovic, O., Baltezarevic, R., & Baltezarevic, V. (2020). Digital storage and online mediated memory. *International Review*, (1-2), 39.

cybercrime laws. Nonetheless, nations are realising more and more that other areas require legislation.¹⁷

According to a recent IBM analysis, data breaches cost businesses over \$4.5 million a year. According to the survey, American businesses spend twice as much. This budget is used to purchase specialised security technologies and hire cyber security experts. Social engineering and third-party exposure rank among the current top cyberthreats, according to security studies. Because it contains so much employee data, the HR department is vulnerable to these risks. For this reason, HR managers must implement internet security rules that safeguard the entire organisation in addition to enhancing the security of HR data. Astra recently reported that around 2,200 cyberattacks occur per day. Additionally, Gartner estimates that around 30% of cyberattacks will use AI to increase attack efficacy. These studies demonstrate the importance of HR data security and the necessity of putting in place a successful HR strategy.¹⁸

In addition to human error, which is said to be the weakest link in data security (as shown in Verizon's 2024 Data Breach Investigations Report, human error accounts for 68% of data breaches), which is primarily brought on by sharing credentials, using weak passwords, or falling for phishing schemes. The following are additional serious risks to the security of HR data: a). Insider attacks (An inexperienced person may unintentionally jeopardise data security, whereas a disgruntled employee with access to sensitive data may steal or leak it. Approximately 60% of all data breaches are caused by insider threats, according to ISACA. b) One of the most rapidly expanding cyberthreats is still ransomware. Cybercriminals are attacking HR systems in an attempt to obtain private employee information and demand money to restore it. In addition to inciting more attacks, paying these ransoms might be against new laws intended to limit ransomware payments. According to the IBM Cost of a Data Breach Report, the average cost of a ransomware attack on a company worldwide increased to \$4.5 million in 2023. c) Risks associated with remote and hybrid work: Workers who work from home frequently use personal devices or unprotected Wi-Fi networks, which leaves important HR data vulnerable to cyberattacks. 74% of companies have had cyber issues connected to remote work technologies, according to a Tenable study.¹⁹

Like health and safety training, information security awareness training has long been viewed as a box to be checked off a list. Regardless of whether they actually understand or interact with the content, they view it as just another task to

¹⁷ Sandage, J. et al. eds. (2013): "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime*.

¹⁸ Talkspirit (2024): *Best Practices for Ensuring HR Data Security*, <https://www.talkspirit.com/blog/best-practices-ensuring-hr-data-security>.

¹⁹ Foxall, D. (2025): *Six basic HR data security threats in 2025*, <https://www.hrmsworld.com/hr-data-security-threats.html>.

finish. Many people are too busy, have strict deadlines to meet, or are just not interested in a training course that seems unrelated to their day-to-day jobs. Knowledge of information security can be interesting and essential to a company's risk management plan. We must go beyond conventional training techniques in order to do this.²⁰ Organisations should try to put in place a framework and plan that makes use of a variety of learning resources, such as interactive simulations and newsletters. Organisations ought to adopt the idea of human risk management, which has gained popularity in recent years.²¹

Strong cybersecurity is essential for businesses in the modern digital world to safeguard confidential information, reduce risks, and preserve operational integrity. It is crucial to put in place a tiered security framework. This strategy addresses weaknesses in an organization's infrastructure at various levels by combining several defensive techniques. Robust access controls significantly lower the danger of unauthorised data disclosure by limiting permissions based on job duties, especially through role-based access control (RBAC). Adherence to pertinent regulatory standards guarantees that security measures fulfil industry-specific and legal requirements, preventing fines and boosting credibility.²²

3. CONCLUSION

This paper underscores the key role of Human Resource Management (HRM) in cultivating a strong corporate security culture, drawing attention to the connections between human behavior, organizational values, and information security practices. By weaving together recruitment strategies, enhancing employee engagement, offering focused training, and assessing performance, HRM can have a significant impact on how employees understand and respond to security policies. The concept of Human Risk Management comes into play as a complementary framework designed to tackle specific behavioral vulnerabilities. This includes being susceptible to phishing, insider threats, and accidental data breaches, issues that can be more pronounced in remote and hybrid work situations.

The research indicates that relying solely on technical solutions won't cut it when it comes to keeping organizations secure. What's really needed is a human-centered approach to HR that's strategically aligned, which can help build resilience and

²⁰ Baltezarević, B., Baltezarević, R., & Baltezarević, V. (2018). Aktivnosti starijih osoba na onlajn društvenim mrežama. *Megatrend revija*, 15(3), 162.

²¹ Digitalxraid (2025): *The Future of Security Awareness: Integrating Human Risk and Security Awareness*, <https://www.digitalxraid.com/human-risk-management-security-awareness/>.

²² Law, B. (2025): *What are some examples of successful corporate security measures?*, <https://www.fixinc.io/blog/p/successful-corporate-security-measures>.

minimize human errors, one of the top culprits behind security breaches. According to the paper, it's crucial for us to move beyond the outdated checklist-style training. We should adopt more interactive and engaging learning experiences that continuously incorporate security awareness into our daily work culture.

There's been a noticeable uptick in interest in this field, but the existing literature still falls short when it comes to solid empirical research linking specific HRM practices to tangible security outcomes across various industries and cultural settings. Moving ahead, it's important for studies to focus on measuring the effectiveness of HR-driven security strategies, developing standardized metrics for evaluating security culture, and exploring how legal, technological, and organizational factors can either aid or obstruct the success of these initiatives.

By enhancing our grasp of the human aspect in cybersecurity through the perspective of HRM, organizations can foster more proactive, inclusive, and adaptable security cultures that are better prepared to tackle emerging threats.

Literature

- Al-Mekhlafi, A.-B. A. (2025): "Importance of Effective Human Resources Management in Creating a More Secure Work Environment by Improving Safety Culture", *International Journal of Intellectual Human Resource Management (IJIHRM)*, 5(01), 14-23.
- Al-Thunaihat, M. Y., Al-shawabkeh, A. A. & Al-baqor, K. K. (2020): "The Role of Human Resource Management Processes in Achieving Information Security: An Applied Study on Saudi Government Universities", *Management & Economics Research Journal*, 2(3), 1-23. DOI: 10.48100/merj.v2i3.107
- Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku“, *Megatrend Revija*, 17(4), 27-40. DOI: 10.5937/MegRev2004027B
- Baltezarević, B., Baltezarević, R., & Baltezarević, V. (2018). Aktivnosti starijih osoba na onlajn društvenim mrežama. *Megatrend revija*, 15(3), 157-172.
- Baltezarevic, B., Milutinovic, O., Baltezarevic, R., & Baltezarevic, V. (2020). Digital storage and online mediated memory. *International Review*, (1-2), 34-41.
- Digitalxraid (2025): *The Future of Security Awareness: Integrating Human Risk and Security Awareness*, <https://www.digitalxraid.com/human-risk-management-security-awareness/>.
- Foxall, D. (2025): *Six basic HR data security threats in 2025*, <https://www.hrmsworld.com/hr-data-security-threats.html>.

- Karlsson, M., Karlsson, F., Åström, J. & Denk, T. (2022): "The effect of perceived organizational culture on employees' information security compliance", *Information and Computer Security*, 30(3), 382-401.
- Kumah, P. (2022): "The Role of Human Resource Management in Enhancing Organizational Information Systems Security", in: *Research Anthology on Business Aspects of Cybersecurity* (pp.300-325).
- Law, B. (2025): *What are some examples of successful corporate security measures?*, <https://www.fixinc.io/blog/p/successful-corporate-security-measures>.
- Milovanović, S., Lukinović, M. & Baltezarević, R. (2018): "Lični brend i integrisano marketing komuniciranje", *Megatrend revija*, 15(1), 177-186. DOI: 10.5937/MegRev1801177M
- Mimecast (2025): *Human Risk Management. Mitigating insider threats through proactive Human Risk Management in cybersecurity*, <https://www.mimecast.com/content/human-risk-management-in-cyber-security/>.
- Petrosyan, A. (2025): *Human risk management in global organizations 2024*, https://www.statista.com/statistics/1622615/human-risk-management-global/?srsltid=AfmBOooug_aRonZEfEQYjDazd0Q1vLnuU-5Kv6BllQZoyl73Ksc3u46y.
- Pujer, K. (2017): "Zarządzanie rozwojem pracowników. Założenia teoretyczne i praktyczne egzemplifikacje", In: Buzowska, B., Paliga, R., Pujer, K.: *Zarządzanie personelem w organizacji. Wybrane problemy teorii i praktyki*. Wydawnictwo Exante, Wrocław.
- Riemenschneider, C. K., Burney, L. L., & Bina, S. (2023): "The influence of organizational values on employee attitude and information security behavior: The mediating role of psychological capital", *Information and Computer Security*, 31(2), 172-198.
- Robinson, K. (2024): *HRM: The Difference Between Human Risk and Resource Management in Cyber Security*, <https://www.metacompliance.com/blog/cyber-security-awareness/hrm-human-risk-and-resource-management>.
- Sandage, J. et al. eds. (2013): "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime*.
- Solomon, G., & Brown, I. (2021): "The influence of organisational culture and information security culture on employee compliance behaviour", *Journal of Enterprise Information Management*, 34(4), 1203-1228.
- Talkspirit (2024): *Best Practices for Ensuring HR Data Security*, <https://www.talkspirit.com/blog/best-practices-ensuring-hr-data-security>.

ULOGA UPRAVLJANJA LJUDSKIM RESURSIMA U UNAPREĐENJU KULTURE KORPORATIVNE BEZBEDNOSTI

Sažetak: Organizacije se sve više bore sa zadatkom zaštite svoje digitalne i fizičke imovine, posebno kako bezbednosne pretnje, kako iznutra tako i spolja, postaju sve složenije. Iako su tehnološka rešenja ključna, ljudsko ponašanje ostaje jedan od najznačajnijih i najranjivijih aspekata korporativnih bezbednosnih sistema. Ovaj rad ispituje ključnu ulogu upravljanja ljudskim resursima (HRM) u negovanju i jačanju čvrste korporativne bezbednosne kulture. Ispituje kako se različite HRM funkcije, uključujući regrutovanje, uvođenje u posao, obuku zaposlenih, sprovođenje politika i procenu učinka, mogu efikasno iskoristiti za oblikovanje ponašanja zaposlenih, smanjenje ljudskih grešaka i jačanje ukupne otpornosti organizacije. Ovaj rad predstavlja novo gledište na upravljanje ljudskim rizicima, koje nastoji da identifikuje, proceni i ublaži ranjivosti povezane sa ljudskim postupcima. Ovo uključuje probleme poput nasedanja na fišing prevare, insajderske pretnje i pogrešno rukovanje podacima. Posebno se bavi izazovima koji dolaze sa hibridnim i udaljenim radnim okruženjima, gde se bezbednosni rizici mogu povećati zbog širenja tehnologije i komunikacionih prepreka. Rad ističe koliko je važno uskladiti programe bezbednosne svesti sa ukupnom kulturom i vrednostima organizacije. Predlaže se udaljavanje od uobičajene obuke usmerene na usklađenost i umesto toga usvajanje angažovanijih pristupa usmerenih na ponašanje.

Ključne reči: upravljanje ljudskim resursima, Korporativna bezbednost, Ljudski rizici, Svest o sajber bezbednosti

ETIKA POSLOVANJA U CIVILNOM VAZDUHOPLOVSTVU

Apstrakt: *Savremeno društvo, zasnovano na ubrzanim komunikacijama, intenzivnoj razmeni informacija i dinamičnim poslovnim procesima, uslovalo je transformaciju poslovnog okruženja u poslednjim decenijama. Ove transformacije reflektuju se na zakonodavni okvir, na temeljne poslovne principe i etičke standarde. Predmet ovog rada jeste analiza etičkih aspekata poslovanja sa posebnim osvrtom na civilno vazduhoplovstvo kao oblasti od strateškog značaja. Civilno vazduhoplovstvo, nastalo početkom XX veka, u savremenom periodu doživljava intenzivnu ekspanziju, pri čemu etičke norme postaju neizostavan uslov njegovog održivog razvoja.*

Etičko poslovanje u ovom sektoru obuhvata zakonodavne obaveze, profesionalne standarde i moralne vrednosti koje se manifestuju kroz prioritizaciju bezbednosti, profesionalne odgovornosti, transparentnosti i zaštite prava korisnika. Međunarodni karakter vazduhoplovstva, kao i permanentni nadzor regulatornih tela, naglašavaju neophodnost striktno primene etičkih principa u svim segmentima: od tehničkog održavanja letelica i obuke kadra do neposredne interakcije sa potrošačima. Posebno mesto zauzima borba protiv korupcije i afirmacija kulture poverenja, budući da se ljudski život, ugled i legitimnost institucija neposredno povezuju sa etičkim integritetom aktera.

Polazeći od Etičkog kodeksa, kao ključnog regulatornog i vrednosnog instrumenta, osnovna paradigma poslovanja u civilnom vazduhoplovstvu jeste poštovanje potrošača i težnja ka zadovoljenju njihovih potreba. Time se etika pozicionira kao konstitutivni element bezbednosnog i poslovnog sistema, čime se potvrđuje da održivost i uspešnost civilnog vazduhoplovstva zavisi od jedinstva zakonodavnih, profesionalnih i etičkih načela.

Ključne reči: *civilno vazduhoplovstvo, etika poslovanja, bezbednost, profesionalna odgovornost, transparentnost, potrošači, korupcija, kultura poverenja, etički kodeks, zakonodavni okvir*

* Megatrend Univerzitet, Beograd – Pravni fakultet, Beograd, Srbija
E-mail: andjelka.racic@gmail.com

UVOD

Ukoliko se osvrenemo na izjavu Viljema Vanderbilta „*Neka je javnost prokleta, ja radim za svoje akcionare*“¹ u celosti oslikava jedna davno prevaziđeni način poslovnog delanja i poimanja.

Razvoj poslovne etike pratio je razvoj društva i menjao se u skladu sa društvenim prilikama. Tokom različitih istorijskih perioda menjali su se i pristupi vezani za moralna načela u poslovanju. Posebnu važnost poslovna etika dobija tokom devedesetih godina XX veka. To je vreme globalne ekonomske recesije, snažne konkurencije na svetskom tržištu, velikog smanjenja broja zaposlenih, procesa spajanja kompanija, ali i izražene mobilnosti radne snage, koja postaje međunarodna, raznovrsna i obrazovanja. Tokom navedenog prioda poslovna etika suočava se sa nizom društvenih i socijalnih problema nastalih kao posledica globalizacije i ubrzanog razvoja novih tehnologija. Ove promene direktno utiču i na prirodnu sredinu i na kvalitet života ljudi. Takvi izazovi nastavljaju da se razvijaju i početkom trećeg milenijuma, pa se među ključnim savremenim pitanjima poslovne etike ističu globalizacija, digitalizacija i ekološka kriza.

Danas je jasno da se neetičko ponašanje u poslovanju ne sme ni tolerisati ni nagrađivati. Umesto toga, formira se novi koncept poslovnog ponašanja koji u prvi plan stavlja zaštitu opštih društvenih interesa. To obuhvata stvaranje kvalitetnog radnog okruženja, u kojem su poslovni uspeh, konkurentnost i profit povezani sa zakonitim i odgovornim odlučivanjem. U savremenoj praksi sve se više vodi računa o odgovornosti u svim aspektima poslovanja, pa se poslovna etika razvija kao neizostavna disciplina, bez koje nije moguće ostvariti stabilan i dugoročno profitabilan rast.

Poslovna etika, međutim, nije samo prenošenje moralnih normi u poslovnu praksu, već se pre svega zasniva na principu odgovornosti.

Poseban značaj poslovna etika ima u civilnom vazduhoplovstvu. Ova oblast, koja je od vitalnog značaja za bezbednost putnika i očuvanje poverenja javnosti, podrazumeva strogu primenu etičkih principa u svim segmentima poslovanja – od održavanja i tehničke ispravnosti letelica, preko obuke i odgovornosti osoblja, do pružanja usluga korisnicima. Civilno vazduhoplovstvo posluje u međunarodnom okruženju i pod stalnim nadzorom regulatornih tela, što dodatno naglašava važnost etičkog ponašanja. Svaka odluka u ovom sektoru mora biti u skladu sa najvišim standardima bezbednosti, profesionalne odgovornosti i transparentnosti, jer se od njih direktno zavisi ljudski život, kao i ugled i uspešnost kompanije.

¹ Solomon Robert (2004): „Poslovna etika“, *Uvod u etiku*, Izdavačka kuća Zorana Stojanovića, Sremski Karlovci, Novi Sad, str. 506.

1. ETIKA POSLOVANJA

Poslovanje, kao razmena dobara, datira još od pre šest hiljada godina, kada su stari Sumeri vodili poslovne – trgovačke knjige. Međutim, lukrativno poslovanje, shvaćeno u savremenom modernom svetu, nije nosilo etička vrednovanja kao danas. Aristotel je razlikovao dva pojma poslovanja – *oikonikos* ili vođenje domaćinstva i *chermatisike*, poslovanje radi profita. Takvu delatnost Aristotel je smatrao neetičkom, ne nalazeći nijedan pozitivan etički element u njoj. Ovakvo poimanje poslovanja zadržano je do sedamnaestog veka, a ovom delatnošću su se većinom bavili ljudi sa margine društva.

Predvođena religijom i filozofijom, poslovna etika početkom novog veka zado-bija novi kolosek. Jedni od promotera nove ideje poslovanja bili su svakako Žan Calvin i Adam Smit. Njihove teorije nisu nastale preko noći. Novo poimanje poslovanja zasnivalo se na tradicijama koje su imale dugu istoriju. Jedna od njih bila je tradicija gildi, gde su za svaku delatnost postojali određeni kodeksi „poslovne etike“, i to mnogo godina pre nego što je poslovanje postalo osnovna i centralna investicija društva. Celokupan zaokret u shvatanju poslovanja iziskivao je promenu pristupa – od uvođenja etike, preko filozofskog pristupa, pa sve do uključivanja religije. Kao okidači za promenu pristupa svakako su dominantno uticali: urbanizacija društva, brzi napredak tehnologije, privatizacija porodičnih grupa kao potrošača, industrijski rast i prateći razvoj socijalnih struktura, potreba i želja stanovništva.

Nadalje, Meloun i Karnegi razvijali su poslovnu etiku dodatno naglašavajući njene vrline kroz koncept *noblesse oblige* bogataša. Na kraju, ključni doprinos pripada socijalistima i njihovoj „kontinuiranoj kritici amoralnosti poslovnog načina mišljenja“. Nakon učešća socijalista, poslovna etika širi svoje dimenzije – ne samo kritikujući već i ističući novi pristup mišljenju o profitu, širem kontekstu produktivnosti i društvene odgovornosti, te načinima na koje korporativno poslovanje može doprineti pojedincu, društvu i društvenom sistemu. Ipak, starovekovno mišljenje da je svako lukrativno poslovanje „nemoralan biznis“ i dalje je bilo prisutno.

Poslovna etika dobija zadatak da ukloni optužujuće mitove da je biznis isključivo zasnovan na ostvarivanju profita, zanemarujući činjenicu da je ovaj mit bio široko korišćen početkom prošlog veka u socijalističkim državnim uređenjima, s ciljem glorifikovanja socijalizma i mistifikacije kapitalizma. Nadalje, mit da je biznis isključivo uvećavanje profita akcionara, čime se pokreće mašina *perpetuum mobile*, zanemarujući društvo, pojedinca i njegove potrebe, minimizuje značaj poslovanja i širu mrežu delatnosti koja čini poslovni svet.

Biznis je društvena praksa, a ne delatnost izolovanih pojedinaca. Jedino u kulturi sa uspostavljenim skupom postupaka i očekivanja moguće je realizovati uspešan biznis. S tim u vezi, zadatak etike u poslovanju jeste da demistifikuje i

ukloni ideju biznisa kao izolovanog fenomena pojedinca i objasni okolnost da je biznis deo šire kulture, specijalizovana ćelija u organizmu koji se zove društvo.

Razvojem makroetike postavljaju se pitanja pravde, zakonitosti i prirode jednog društva, čime se uspostavlja socijalna i politička filozofija. Jedno od dominantnih pitanja jeste priroda prvobitne svojine – konkretno, da li ona u nekom smislu pretihodi društvenim konvencijama ili tržište kao takvo treba da se shvati isključivo kao dinamična, višeslojna društvena praksa, u kojoj su prava samo jedan sastojak? Takođe, da li je slobodno tržište pravično i pošteno? Šta je sa zaslugama, gde nikako nije zagarantovano da će vrline biti adekvatno nagrađene? Na ovaj način, makroetika daje doprinos shvatanju poslovanja kao velike slike poslovnog sveta – sa svim njegovim dijapazonima pozitivnog i negativnog uticaja na pojedinca i društvo u celini.

Svako poslovanje mora imati obavezu prema akcionarima, ali jednako tako i prema potrošačima i zajednici. Cilj korporacije jeste da služi javnosti – kako kroz pružanje usluga, tako i kroz izbegavanje nanošenja štete zajednici. Svako poslovanje ima obavezu da putem istraživanja dođe do određenih saznanja koja se tiču kvaliteta, ali i bezbednosti proizvoda i usluga koje pruža. S tim u vezi, svako lukrativno delovanje iziskuje prikladno informisanje korisnika o načinu korišćenja ponuđenih proizvoda, ali isto tako i upozorenja protiv mogućih zloupotreba ili nastupanja štete bilo koje druge vrste. Ovde se postavlja i pitanje etičnosti ophođenja samih potrošača. Danas možemo videti milionske tužbe protiv korporacija jer su nemarni potrošači sami sebi naneli štetu, koja teško da bi nastala da su iskazali minimalnu pažnju i oprez pri delovanju. Dakle, poslovanje je sistem uzajamnih prava i obaveza između potrošača i pružaoca usluga. Poslovni odnosi su multilateralni i nikada ne mogu biti jednostrano obojeni.

Nadalje, direktnim uticajem etike u poslovanje se uvodi element društvene odgovornosti. Poslovanje u savremenom društvu odavno je prevazišlo shvatanje da je jedina svrha preduzeća ostvarivanje profita. Iako je ekonomski rezultat i dalje primarni cilj svake poslovne organizacije, etika je svojim uticajem značajno promenila način na koji posmatramo svrhu i posledice poslovnih aktivnosti. Etika zahteva da se prilikom donošenja odluka i sprovođenja poslovnih strategija ne gleda isključivo na finansijsku dobit, već i na to kakve posledice te odluke imaju na zaposlene, zajednicu i životnu sredinu. Upravo na tom mestu pojavljuje se pojam društvene odgovornosti preduzeća (CSR – *Corporate Social Responsibility*).

Društvena odgovornost predstavlja obavezu preduzeća da deluje u skladu sa vrednostima i principima koji doprinose opštem dobru. To znači da se kompanije više ne mogu posmatrati samo kao ekonomski subjekti koji proizvode i razmenjuju dobra, već i kao društveni akteri koji imaju odgovornost prema zajednici. Na taj način, etika postaje pokretač promena u poslovnom svetu, jer ona uvodi moralne norme i principe kao kriterijum poslovnog uspeha.

Konkretno, društvena odgovornost se ogleda u nekoliko aspekata:

1. Odnos prema zaposlenima – etičko poslovanje podrazumeva poštene uslove rada, pravednu zaradu, mogućnosti za profesionalni razvoj i poštovanje ljudskog dostojanstva.
2. Odnos prema potrošačima – obaveza preduzeća je da ponudi proizvode i usluge koji su kvalitetni, sigurni i transparentno predstavljeni, bez manipulacije i obmane.
3. Odnos prema zajednici – od kompanija se očekuje da doprinesu razvoju sredine u kojoj posluju, bilo kroz zapošljavanje lokalnog stanovništva, ulaganje u obrazovanje, kulturu, zdravstvo ili humanitarne aktivnosti.
4. Odnos prema prirodi – ekološka odgovornost postaje ključni deo poslovne etike, jer se od kompanija zahteva racionalno korišćenje resursa, smanjenje zagađenja i ulaganje u održive tehnologije.

Sve ove dimenzije pokazuju da etika proširuje tradicionalno shvatanje poslovanja. Uspeh se ne meri isključivo bilansima i profitom, već i time koliko je kompanija doprinela stvaranju zdravijeg, pravednijeg i održivijeg društva. Time poslovanje dobija širi humanistički karakter i postaje most između ekonomskih ciljeva i društvenih vrednosti.

Može se reći da etika poslovanje pretvara u proces u kome je čovek u centru pažnje, a ne samo profit. Društvena odgovornost, uvedena kroz etičke principe, čini poslovanje održivim, moralno opravdanim i korisnim ne samo za vlasnike i zaposlene, već i za čitavu zajednicu.

2. VAZDUHOPLOVSTVO

Čovečanstvo je oduvek gajilo san o letenju i istraživanju neba. Letelice su prvobitno zamišljene kao sredstvo koje će povezati svet, ubrzati komunikaciju među narodima i otvoriti nove horizonte, ali istorija pokazuje da su one često korišćene i u ratne svrhe. Veza između razvoja avijacije i ratovanja prisutna je od samih početaka, pa je važno razmotriti kako su globalni sukobi oblikovali razvoj aviona i u kojoj meri su doprineli promeni ratnih strategija i taktika.

Avijacija je tokom nešto više od jednog veka prošla put od krhkih letelica braće Rajt do savremenih mlaznih aviona i satelitski vođenih sistema. Veliki ratovi ubrzali su njen razvoj, dok je civilno vazduhoplovstvo postalo ključna osovina globalne povezanosti. Danas, pored tehničkog i ekonomskog značaja, ovaj sektor nosi i ogromnu društvenu odgovornost – da čuva bezbednost putnika, unapređuje održivost i razvija etičke standarde.

Kroz integraciju regulative, tehnoloških inovacija i kulture poverenja, avijacija ostaje jedan od najdinamičnijih i najvažnijih sektora savremenog društva, a njen dalji razvoj u velikoj meri odrediće način na koji će čovečanstvo komunicirati, putovati i sarađivati u budućnosti.

2.1. Grane vazduhoplovstva

Tokom vremena razvile su se četiri osnovne grane avijacije:

1. Civilno vazduhoplovstvo – uključuje putnički i teretni transport, ali i privatne letove. Njena uloga je povezivanje regiona, olakšavanje trgovine i omogućavanje globalne mobilnosti.
2. Vojna vazduhoplovstvo – obuhvata lovce, bombardere, izviđače i transportne avione. Njena istorijska i savremena uloga presudna je za vojne operacije i odbranu.
3. Sportsko i rekreativn vazduhoplovstvo – obuhvata balone, jedrilice, ultralake avione i akrobatske letove. Ona čuva tradiciju i popularizuje letenje.
4. Eksperimentalno vazduhoplovstvo – namenjena testiranju novih tehnologija, od mlaznih i hipersoničnih letelica do bespilotnih sistema. Često se inovacije iz ovog sektora prenose na civilnu i vojnu primenu.

2.1.1. Civilno vazduhoplovstvo – definicija, značaj i razvoj

Civilno vazduhoplovstvo predstavlja nevojni segment avijacije koji obuhvata sve oblike civilnog i komercijalnog letenja. To je složen sistem koji uključuje aviokompanije, aerodrome, regulatorna tela i tehnološke inovacije. Ono je ključna infrastruktura savremenog globalnog društva, jer povezuje kontinente, države i gradove, omogućavajući protok ljudi, robe i ideja.²

Prema zakonodavstvu Republike Srbije, civilni vazduhoplovi su svi oni upisani u Registar civilnih vazduhoplova, dok se vojni, policijski i državni avioni vode u posebnim registrima. Civilno vazduhoplovstvo se deli na dva segmenta: komercijalno (redovne putničke i teretne linije) i opštu avijaciju (privatni i specijalizovani letovi, obuka pilota, gašenje požara, medicinski transport).

Istorijski gledano, prvi redovni putnički letovi uspostavljeni su u prvoj polovini XX veka. U početku privilegija bogatih, letenje je nakon Drugog svetskog rata postalo sve dostupnije, a širenje niskobudžetnih kompanija u XX i XXI veku dodatno je demokratizovalo vazdušni prevoz³.

Prvi avion teži od vazduha podigla su braća Rajt 1903. godine, čime je otvoren put kako za civilnu, tako i za vojnu primenu. Dok su civilni avioni u početku služili kao zabava entuzijasta i učesnika takmičenja, vojne sile su vrlo brzo prepoznale

² The World of Air Transport in 2023.

³ IATA Annual Review (2022): *Airline Industry Report*.

potencijal ove tehnologije. Već do Prvog svetskog rata formirane su posebne avijacijske jedinice.

U Prvom svetskom ratu, avioni su služili pre svega za izviđanje i korekciju artiljerijske vatre. Iako njihova uloga nije bila presudna zbog statičnog ratovanja, ubrzo su uvedeni i prvi bombarderi poput nemačkih modela Gotha G.V. i Zeppelin-Staaken R.VI. Njihov doprinos bio je više psihološki nego materijalni, ali su postavili temelje za razvoj velikih aviona kasnije korišćenih u civilnom i transportnom sektoru.

U međuratnom periodu tempo razvoja bio je sporiji, ali su inovacije u Nemačkoj, naročito kroz Luftwaffe, stvorile preduslove za primenu avijacije u Drugom svetskom ratu. Tada dolazi do punog izražaja značaj aviona u ratovanju – nemački lovci Messerschmitt Bf 109 i bombarderi Junkers Ju 87 (Štuke) odigrali su ključnu ulogu u blitzkrieg strategiji. S druge strane, saveznički strateški bombarderi poput B-17 i B-29 omogućili su razaranje neprijateljske industrije i ubrzali završetak rata.

Poseban značaj imale su tehnološke inovacije poput prvog mlaznog aviona Me 262 i raketa V-2. Iako nisu odlučile ratni ishod, one su oblikovale budući tehnološki razvoj – od mlaznih aviona do svemirskih letova.

Kada je u pitanju civilna avijacija, svakako da njene početke, razvoj i najviši stepen dostignuća je realizovan u SAD (Sjedinjenim Američkim Državama).

Naime, uprkos ograničenim tehničkim dostignućima nakon Prvog svetskog rata, rana civilna avijacija ostala je opasan posao. Uslovi letenja bili su teški usled nepostojanja mapa ni službi za koordinaciju leta. Piloti su leteli na visinama od 200 do 500 stopa iznad tla kako bi se orijentisali pomoću puteva i železnica, a navigacija za sletanje bile su lomače na zemlji, jer su jednine one pružale dovoljno svetlosti za “sigurano” sletanje. Smrtne nesreće bile su uobičajene.

Usvajanjem 1925 Zakona o poštanskom vazdušnom saobraćaju, omogućio je stvaranje profitabilne komercijalne avio-industrije, pa su aviokompanije poput Pan American Airways, Western Air Express i Ford Air Transport Service koje započele redovan putnički saobraćaj. Do sredine 1930-ih, četiri glavne aviokompanije koje su dominirale civilnim komercijalnim letovima tokom većeg dela 20. veka započele su sa radom: United, American, Eastern i Transcontinental and Western Air (TWA)⁴.

Radi povećanja stepena bezbednosti, porasta avio saobraćaja, pojedini operateri aerodroma, uveli su rani oblik kontrole letenja (ATC) zasnovan na vizuelnim signalima. Prvi kontrolori stajali su na pisti i mahali zastavicama kako bi komunicirali sa pilotima. Arči Lig, prvi „mašać zastavicama“ u sistemu, započeo je rad kasnih 1920-ih na aerodromu u Sent Luisu, Misuri.⁵

⁴ „The Rise of Airlines“, *Century of Flight*, Archived from the original on 23 November 2018, Retrieved 25 April 2014.

⁵ „A Brief History of the FAA“, *Federal Aviation Administration*.

Vremenim, lideri avio-industrije su zaključili da civilna avijacija ne može dostići svoj puni komercijalni potencijal bez federalnog angažovanja, posebno u domenu unapređenja i održavanja bezbednosnih standarda. Na njihov zahtev, 1926. godine donet je Zakon o vazdušnoj trgovini (Air Commerce Act)⁶, povereno je Sekretaru za trgovinu odgovornost podsticanje vazdušne trgovine, izdavanje i sprovođenje pravila vazdušnog saobraćaja, licenciranje pilota, sertifikovanje aviona, uspostavljanje vazdušnih koridora i održavanje i navigacionih uređaja. Dalji podsticaji civeiblog vazduhoplovstva su nastavljeni osnivanjem Aeronautička uprava (Aeronautics Branch) unutar Ministarstva trgovine, koje su preuzele glavnu odgovornost za nadzor avijacije.

Aeronautička uprava 1934 godine preimenuje Agenciju u Biro za vazdušnu trgovinu (Bureau of Air Commerce), čiji primarni cilj je bio podsticanje aviokompanija da osnuju prve centre kontrole letenja (u Njuarku, Klivlendu i Čikagu) za pružanje usluga en-route⁷ kontrole letenja. Već 1936. godine Biro je preuzeo ove centre.

Prvi kontrolori en-route letova pratili su položaj aviona pomoću mapa, tabli i malih olovničkih figura nazvanih „šrimps“. Nisu imali direktnu radio vezu sa avionima, već su koristili telefone za kontakt sa dispečerima, radio-operaterima i kontrolorima na aerodromima. Dok je federalna vlada preuzela kontrolu nad en-route saobraćajem, lokalne vlasti nastavile su da upravljaju tornjevima na aerodromima. Ibidem

Vremenom princip bezbednosti postaje dominantan, te kako bi se fokus stavio na bezbednost, predsednik Frenklin Ruzvelt 1938. godine potpisao je Zakon o civilnoj aeronautici (Civil Aeronautics Act)⁸, kojim je osnovana nezavisna Civilna aeronautička uprava (CAA) sa tročlanim Odborom za bezbednost. Ova institucija imala je ovlašćenja da istražuje nesreće, reguliše tarife aviokompanija i određuje rute.

Nadalje, tokom 1940 godine predsednik Ruzvelt podelio CAA deli I u dve agencije

- Civilna aeronautička administracija (u okviru Ministarstva trgovine) – nadležna za kontrolu letenja, sertifikaciju pilota i aviona, sprovođenje bezbednosnih pravila i razvoj vazdušnih puteva.
- Civilna aeronautička komisija (CAB) – zadužena za donošenje bezbednosnih propisa, istrage nesreća i ekonomske regulacije.

Na pragu Drugog svetskog rata, CAA je proširila svoj sistem kontrole letenja i na tornjeve aerodroma u svrhu nacionalne odbrane. Nakon rata, ova nadležnost postala je trajna. Šireći svoja isustva I saznanja iz SAD-a, civilna avijacija vremenom postala dominantni oblik vazduhoplovstva.

⁶ Zakon o vazdušnoj trgovini - United States Air Commerce Act 1926

⁷ Na putu ka odredištu; u tranzitu.

⁸ Agencija za civilno vazduhoplovstvo-Government Of The United States Civil Aeronautics Act 1938

I pred svih preduzetih mera bezbednosti, nakon teške nesreće iznad Velikog kanjona 1956. godine, u kojoj je poginulo 128 ljudi, nesprona je ostala neophodnost uvođenja većih mera bezbednosti u civilnom avio saobraćaju. Na inicijativu senatora Majka Monronija, 1958. donet je Zakon o federalnoj avijaciji (Federal Aviation Act)⁹, kojim je osnovana Federalna vazduhoplovna agencija kao nezavisno telo nadležno za bezbednost civilne avijacije.

U narednim decenijama Federalnu administraciju za avijaciju (FAA) je:

- preuzela veće odgovornosti u kontroli letenja, sertifikaciji i istraživanju nesreća,
- uvela ekološke standarde (buka, emisije),
- izgradila nove sisteme kontrole letenja i automatizacije,
- suočila se sa štrajkovima kontrolora letenja (PATCO 1981),
- razvila planove modernizacije Nacionalnog vazdušnog sistema (NAS Plan, kasnije NextGen),
- dobila nadležnosti za komercijalne svemirske letove (1995),
- i nakon terorističkih napada 11. septembra 2001. prenela nadležnosti za bezbednost na novu Transportation Security Administration (TSA).

FAA je uvela i Organizaciju za kontrolu saobraćaja (ATO) 2004. godine, sa fokusom na efikasnost i usluge korisnicima.

Zahvaljujući radu FAA tokom proteklih decenija, avijacija je postala najbezbedniji, najpouzdaniji i najefikasniji vid transporta u svetu. Sa programom NextGen, FAA i dalje radi na razvoju fleksibilnog i održivog sistema vazdušnog saobraćaja za 21. vek, sa naglaskom na bezbednost, kapacitet, efikasnost i zaštitu životne sredine.

Tehnološki napredak obezbedio je modernije, štedljivije i tiše avione, precizne navigacione sisteme i digitalizovane procese kontrole letenja. Istovremeno, veliki izazov postaje održivost – smanjenje emisije gasova, primena biogoriva i ulaganje u zelene tehnologije.

2.1.1.a Pružanje usluga u vazdušnoj plovodbi – primer SMATSA

Usluge u vazdušnoj plovodbi predstavljaju ključni segment transportnog sistema, koji zahteva visok nivo stručnosti, koordinacije i poštovanja zakonskih regulativa. U Republici Srbiji, pružanje ovih usluga reguliše se kroz zakonodavni okvir koji nalaže da svi pružaoci usluga poseduju odgovarajuće sertifikate, uz ispunjavanje strogih tehničkih i organizacionih standarda, sa decaidnom usalgašenošću sa međunarnornopravnim standardima.

Primer dobre prakse u ovom sektoru je organizacija SMATSA doo, koja svoj rad temelji na principima najvišeg nivoa bezbednosti i kvaliteta, kao i na

⁹ Zakon o federalnoj avijaciji - STATUTE-72-Pg731.pdf

transparentnom i odgovornom pružanju svojih usluga. Posvećenost bezbednosti i kvalitetu ogleda se u efikasnom i održivom poslovanju, otvorenom pristupu korisnicima i nediskriminatornom tretmanu svih zainteresovanih strana, čime se gradi poverenje i jača međunarodni ugled organizacije.

Osnovu uspešnog funkcionisanja čini integrisan sistem menadžmenta, koji uključuje tehničke kapacitete, stručnost zaposlenih i procese upravljanja rizicima. Identifikacija potencijalnih opasnosti, procena rizika i implementacija preventivnih mera omogućavaju donošenje pravovremenih odluka i ostvarivanje postavljenih ciljeva u bezbednom i kontrolisanom okruženju.

Pored bezbednosti, SMATSA pridaje veliku važnost zaštiti životne sredine. Aktivnosti organizacije usmerene su na prevenciju zagađenja, očuvanje prirodnih resursa i minimiziranje negativnog uticaja na klimu, vodu, vazduh i zemljište. Očuvanje zdravlja i sigurnosti zaposlenih, kao i radne sredine, tretira se kao prioritet.

Efikasan sistem izveštavanja predstavlja ključni deo menadžmenta. U njemu su definisani principi horizontalne i vertikalne komunikacije, obavezno i dobrovoljno prijavljivanje događaja, s ciljem unapređenja bezbednosti kroz razmenu iskustava, a ne kažnjavanje pojedinaca. Prijavljivanje obuhvata širok spektar situacija – od incidenata i povreda na radu do potencijalnog ekološkog uticaja – čime se podstiče proaktivno učešće zaposlenih.

Najviše rukovodstvo ima odgovornost da osigura usklađenost politike menadžmenta sa potrebama organizacije i međunarodnim standardima, kao i da kontinuirano promoviše kulturu bezbednosti i kvaliteta. Poseban značaj pridaje se regrutaciji i kontinuiranoj obuci zaposlenih, kao i podizanju njihove svesti o važnosti sistema menadžmenta.

Jedan od najvažnijih elemenata uspeha jeste razvijena kultura poverenja (Just Culture), u kojoj se greške posmatraju kao prilike za učenje, a zaposlenima je omogućeno da prijavljuju pretnje i incidente bez straha od neosnovanih sankcija. Jasno su definisane granice prihvatljivog ponašanja, čime se održava balans između zaštite zaposlenih i odgovornosti za postupke.

Kroz integrisan menadžment, efikasan sistem izveštavanja i kulturu poverenja, SMATSA doo potvrđuje svoju ulogu kao pouzdana i odgovorna organizacija. Posvećenost stalnom unapređenju, otvorenoj komunikaciji i bezbednom poslovanju čini osnovu održivog razvoja i kontinuiranog doprinosa sigurnosti vazdušnog saobraćaja.

3. CIVILNO VAZDUHOPLOVSTVO, ETIČNOST POSTUPANJA- PROFESIONALNA ODGOVORNOST I LJUDSKI RESURSI

Etika u civilnom vazduhoplovstvu ogleda se u prioritetu bezbednosti, profesionalnoj odgovornosti, transparentnosti i nediskriminaciji korisnika usluga. Posebno važan segment čini borba protiv korupcije i razvoj kulture poverenja.

S tim u vezi, prema Etičkom kodeks¹⁰ kao osnovna paradigma istakunto je poštovanje potrošača i težnja zadovoljenju njihovih potreba, kao i odnos privrednog subjekta prema potrošačima. Konkretizujući dužnosti civilnog vazduhoplovstva prema potrošačima, uočava se da je prvi zadatak poštovanje poslovne etike i uvažavanje potrošača kao ravnopravnih poslovnih partnera. Korisnik usluga civilnog vazduhoplovstva nije samo korisnik usluge, već i partner u poslovnom procesu, čije zadovoljstvo direktno utiče na reputaciju i uspeh kompanije.

Drugi važan aspekt odnosi se na zabranu diskriminacije. Korisnici usluga civilnog vazduhoplovstva moraju biti ravnopravno tretirani u pogledu kvaliteta, cene i uslova pružanja usluge. Jednaka dostupnost i transparentnost uslova poslovanja osnovni su preduslov poštovanja dostojanstva svakog korisnika. Civilna avijacija ima obavezu da poštuje sve ugovorene i pravne standarde, naročito one koji se odnose na bezbednost i zdravlje korisnika usluga. Ovi standardi predstavljaju ne samo zakonski okvir, već i moralnu obavezu zaštite ljudskog života, što u vazduhoplovstvu zauzima primarno mesto.

Nadalje, privrednim subjektima strogo je zabranjeno da odbiju prodaju proizvoda koji je izložen ili na drugi način pripremljen za prodaju, kao i da odbiju pružanje usluga koje je moguće izvršiti. Takvo postupanje narušava osnovna prava korisnicima usluga civilnog vazduhoplovstva i stvara nepoverenje na tržištu. Takođe, nedozvoljeno je uslovljavanje prodaje jednog proizvoda kupovinom drugog, odnosno pružanja usluge zavisno od prihvatanja dodatnih usluga. Ovakva praksa smatra se manipulativnom i predstavlja direktno kršenje slobode izbora korisnika usluga. Još jedan od najvažnijih segmenata u zaštiti korisnika odnosi se na zabranu prevare i obmanjivanja kroz reklamiranje. Reklama ima funkciju da informiše i približi proizvod ili uslugu javnosti, ali nikako da dovede potrošača u zabludu. Obmanjivanje se može ispoljiti na više načina: davanjem nepotpunih ili lažnih informacija, prikrivanjem podataka od suštinskog značaja, kao i kreiranjem slike koja potrošača navodi na pogrešnu odluku. Među oblicima obmanjujuće reklame posebno se izdvaja preterano predstavljanje sopstvenih proizvoda, isticanje privrednog subjekta kao jedinog distributera ili proglašavanje svojih proizvoda najboljim bez stvarnih dokaza. Nedozvoljeno je i plasiranje ponuda bez jasnih i potpunih informacija. Pored toga, moralno je i zakonski neprihvatljivo

¹⁰ Kodeks poslovne etike, *Sl. Glasnik RS*, br. 1/2006 - Kodeks poslovne etike.

iskorišćavanje neiskustva, lakovernosti, straha ili stanja nužde potrošača. Obmanjujuće reklamiranje može se manifestovati i kroz poređenje sa konkurentima na način koji povređuje njihov ugled, kao i kroz isticanje nižih cena ili sposobnosti koje dovode u pitanje kredibilitet konkurencije. Takođe, reklame koje stvaraju zabunu u pogledu identiteta reklamera, njegovih prava, priznanja ili profesionalnih kompetencija, narušavaju tržišnu ravnotežu i ozbiljno ugrožavaju poverenje javnosti. Posebno je važno istaći da reklamiranje ne sme povrediti nacionalna, verska i druga osećanja potrošača, niti sme vređati javni moral. Oglašavanje mora biti u skladu sa etičkim standardima i društvenim vrednostima, jer u suprotnom postaje izvor konflikta i nepoverenja.

Dakle, zabrane sadržane u čl. 52 i 53 Kodeska¹¹ decidino ukazuju da se tržište ne može graditi na manipulaciji i obmani, već isključivo na poštovanju potrošača, transparentnosti i fer konkurenciji. Samo dosledna primena ovih principa omogućava održiv poslovni razvoj i očuvanje poverenja u civilno vazduhoplovstvo.

Treba istaći, takođe, da neblagovremeno postupanje po žalbi korisnika usluga je suprotno etičkim pravilima, te s tim u vezi, pružalac usluga, ukoliko utvrdi da je žalba korisnika usluga opravdana, u obavezi da zameni reklamiranu robu, refundira novčana sredstva korniku usluga ili ponudi drugi istovrsni proizvod.

Kako je savremeni svet globalno povezan svim sistemima mobilne komunikacije, to je i pružanje usluga i prodaja na daljini, postalo svakodnevni oblik poslovanja i u okviru civilnog vazduhoplovstva. Do samo pre par decenija, ovakav oblik poslovanja je bio nezamisliv. Iako pun izazova, poslovanje na daljinu, danas je jedno od dominantnih oblika poslovanja savaremenog tržišta. Svakao da je i u ovom domenu bilo nepohodno kako zakonodavno tako i etičko uređenje. Između ostalog se ističe da svaki pružalac usluga u okviru civilnog vazduhoplovstva na daljinu je obavezi da obezbedi sigurnost transakcija, posebno u pogledu podataka o kreditnim i platnim karticama, kao i da nedvosmislena i nepromenljiva ponuda sadrži sve bitne zanačajne elemente, koji se tiču cene, rokova isporuke i reklamacije.

Svakako da poslovna etika civilnog vazduhoplovstva obihvata i obavezu društvenog razvoja, a koji se, izmenju osatlogh ogledaju u direktnom podsticanju zaposlenih za aktivnim učestovanjem u društvenom životu, obezbeđivanju informacija o svom poslovanju (osim onih koje se tiču poverljivosti određenih podataka), saradnju sa medijim, udruženjima, državnim organima. Primenom navedenih etičkih pravila u okviru poslovanja civilnog vazduhoplovstva realizuje se stabilnot tržišta, poverenje u civilno vazduhoplovstvo, a čime se omogućava njegov dalji tehnološki razvoj, a time i kvalitet usluga u ponudi.

Sa daljem unapređenjem civilnog vazduhoplovstva usko je vezana i slobodna konkurencija, koja predstavlja osnovni stub tržišne ekonomije, jer osigurava fer

¹¹ Ibidem.

uslove za poslovanje, podstiče inovacije i doprinosi optimalnoj raspodeli resursa. Jedan od ključnih aspekata zaštite konkurencije je zabrana nekorektnih oblika konkurentske utakmice, uključujući zloupotrebu monopolskog položaja, damping, korupciju, neetičko pribavljanje informacija o konkurentima i širenje neistinitih informacija. Ove radnje ne samo da narušavaju ravnotežu tržišta, već direktno ugrožavaju poverenje potrošača i drugih privrednih subjekata. Prikupljanje informacija o konkurentima dopušteno je samo zakonitim i etičkim sredstvima. Svaka zloupotreba, uključujući podmićivanje, lažno predstavljanje ili neadekvatno korišćenje poverljivih podataka, predstavlja ozbiljno kršenje profesionalnih normi i zakonskih propisa. Pored toga, zabranjeno je ugrožavati ugled drugih privrednih subjekata ili podražavati njihove proizvode i usluge na način koji može stvoriti zabunu kod kupaca. Ovakvim delanjem naruštava se sigurnost u civilno vazduhoplovstvo i njeno poslovanje, a što za direktnu posledicu ima smanjenje usluga civilnog vazduhoplovstva, a time i njenu devastaciju. Konkretno svaki oblik zloupotrebe dominantnog položaja, zaključivanje monopolističkih sporazume, preduzimanje radnje koje su oblik neloyalne konkurencije, smatra se neetičkim i van pravila „dobre prakse“ poslovanja u okviru civilnog vazduhoplovstva. Posebno su problematične radnje koje dovode do ograničavanja tržišta, špekulacije ili favorizovanja sopstvenih interesa na štetu drugih učesnika. Zakonska regulativa jasno definiše da su ovakve prakse štetne ne samo za pojedinačne subjekte, već i za čitavu ekonomiju, jer sprečavaju ravnomeran razvoj i pravičnu tržišnu utakmicu. Održavanje slobodne konkurencije zahteva od privrednih subjekata kontinuiranu pažnju na etičke i zakonske norme. Transparentno i odgovorno poslovanje, poštovanje konkurentnih pravila i fer odnosa sa tržištem stvaraju dugoročne koristi, ne samo u obliku reputacije i poverenja, već i kroz održiv rast i razvoj. Privredni subjekti koji se pridržavaju ovih principa doprinose zdravoj ekonomiji, stimulisanju inovacija i zaštiti interesa potrošača. U konačnom, zaštita slobodne konkurencije nije samo zakonska obaveza, već i moralna odgovornost svakog privrednog subjekta. Samo kroz poštovanje etičkih normi i zakonskih propisa moguće je stvoriti fer, transparentno i održivo tržište, na kojem svi učesnici imaju jednake šanse za uspeh.

Kao što je već više puta nevedeno u okviru rada, civilno vazduhoplovstvo u okviru svog poslovanja pružanja usluga, poseban značaj u zaštiti životne sredine, a koje se ogledaju u primeni zakonskih i podzakonskih odredaba kojima se decidno reguliše ovo polje. Bliže rečeno, aktivno delovanje u okviru zaštite životne sredine u domenu civilnog vazduhoplovstva obuhvata širenje svesti o značaju zaštite životne sredine i to većim stepenom tehnologizacije procesa rada, finansiranjem sistemom naučnoistraživačkog i tehnološkog razvoja, kao i popularizacijom zaštite životne sredine.

Članom 84 Kodeska¹² je decindo istaknuto da privredni subjekt je dužan da ispunjava obaveze iz propisa o zaštiti životne sredine i u tom cilju preduzima neročito sledeće mere:

1. primenjuje i sprovodi propisane standarde o zaštiti životne sredine;
2. postavlja zaštitu životne sredine kao jedan od ciljeva svoje poslovne aktivnosti;
3. teži korišćenju obnovljivih prirodnih resursa;
4. upotrebljava proizvode, procese, tehnologije i prakse koji u manjoj meri ugrožavaju životnu sredinu;
5. preduzima mere prevencije ili otklanja posledice ugrožavanja životne sredine;
6. vodi na propisani način evidenciju o potrošnji sirovina i energije, ispuštanju zagađujućih materija i energije, klasifikaciji, karakteristikama i količinama otpada, kao i o drugim podacima, i dostavlja ih nadležnim organima;
7. pojačano kontroliše rad postrojenja koja mogu predstavljati rizik ili prouzrokovati opasnost po životnu sredinu i zdravlje ljudi;
8. predviđa posledice svojih poslovnih aktivnosti u odnosu na životnu sredinu i uvažava ih prilikom donošenja poslovnih odluka;
9. zahteva od poslovnih partnera da poštuju propisane standarde zaštite životne sredine;
10. obaveštava javnost o svim problemima u vezi sa zaštitom životne sredine koji se javljaju u njegovom poslovanju.

U slučaju da ipak nastupi zagađenje, bilo svojom aktivnošću ili propustom, subjekti civilnog vazuhoplovstva su u obavezi da odmah preduzme mere za smanjenje štete i sprečavanje dodatnih rizika. Ukoliko šteta ne može biti otklonjena, privredni subjekt i lice koje je odgovorno za postupke moraju nadoknaditi vrednost uništenih ili oštećenih dobara. Razlog ovakovog zakonskog opredeljenja -kažnjavanje privrednih subjekata civilnog vazuhoplovstva, uspostavljeno je radi realizacije primarnog cilja – podsticanje vođenja računa o svojim aktivnostima i preventivnog delovanje radi izbegavanja štete. Održivo poslovanje podrazumeva ravnotežu između ekonomskog uspeha i zaštite prirode. Privredni subjekti koji poštuju pravila o zagađenju životne sredine doprinose očuvanju prirodnih resursa, zdravom životu ljudi i dugoročnom razvoju društva. Pažljivo i odgovorno upravljanje resursima pokazuje da privredni interesi i ekologija mogu i moraju ići ruku pod ruku.

3.1. (Ne)Poštovanje poslovne etike poslovnog vazuhoplovstav

U savremenom poslovnom okruženju, pa tako i u poslovanja u okviru civilnog vazuhoplovstva, etičko ponašanje zaposlenih i organa privrednih subjekata postaje sve važnije za očuvanje poverenja, transparentnosti i društvenog razvoja.

¹² Ibidem.

Kodeksi poslovne etike služe kao vodiči koji definišu standarde profesionalnog ponašanja i odgovornosti.

Aдекватna primena Kodeks poslovne etike, kao i niza zakonskih i podzakonskih akata, obavezuje sve zaposlene i članove upravnih organa da se pridržavaju utvrđenih pravila. Naime, tokom procesa zapošljavanja, osnovno je da lica budu upoznata sa osnovnim principima Kodeksa, što omogućava dosledno ponašanje i izbegavanje etičkih konflikata. U situacijama kada postoji nejasnoća u tumačenju pravila, neusaglašene starne se upućuju na mirno rešavanje spora - arbitražu. U poslovnom okruženju, sukobi između kompanija ili unutar njih su često neizbežni, posebno kada se radi o složenim ugovorima ili međunarodnoj trgovini. Tradicionalni sudski postupci mogu biti spori, skupi i birokratski. Upravo zbog toga, arbitraž postaje sve važniji način rešavanja sporova, jer omogućava brže, fleksibilnije i stručnije donošenje odluka, uz očuvanje profesionalnih odnosa između strana. Jedna od ključnih prednosti arbitraže je brzina. Za razliku od dugotrajnih sudskih postupaka, arbitraž omogućava da se sporovi reše u dogovorenim rokovima, što je posebno važno za poslovne subjekte koji ne mogu sebi da priušte odlaganje poslovnih odluka. Takođe, arbitraž nudi fleksibilnost u organizaciji postupka, što omogućava da se prilagodi specifičnostima konkretnog slučaja. Pored navedenog, arbitraž obezbeđuje poverljivost procesa, što znači da detalji spora ne postaju javni. Ova privatnost štiti poslovne tajne i reputaciju kompanija.

Arbitraž igra ključnu ulogu u modernom poslovnom svetu, jer omogućava efikasno, stručno i diskretno rešavanje sporova. Njena primena doprinosi očuvanju poslovnih odnosa, smanjenju rizika i održavanju stabilnog i predvidljivog poslovnog okruženja. U uslovima globalnog tržišta, arbitraž postaje nezamenljiv instrument za kompanije koje žele da upravljaju sporovima na profesionalan i efektivan način.

Pored prispitivanja etičkog postupanja na relaciji pružaoca usluga i korisnika istih, za primenu etičkog poslovanja zainteresovani su i nadležni organi privredne komore, koji obezbeđuju poštovanje pravila i reaguju u slučaju neetičkog ponašanja, kao i sud časti koji ima višestruku ulogu: može odlučivati kao prvostepeni ili drugostepeni organ, zavisno od složenosti slučaja i teritorijalnog opsega.

Dakle, poslovni subjekti u civilnom vazduhoplovstvu imaju obavezu da:

1. upoznaju zaposlene i članove organa sa Kodeksom;
2. preduzmu konkretne mere za usklađivanje ponašanja sa etičkim normama;
3. osiguraju da poslovne aktivnosti budu u skladu sa pravilima etike.

Poslovna etika nije samo formalni dokumenti, već temelj odgovornog i profesionalnog poslovanja. Njihova primena doprinosi očuvanju integriteta, izgradnji poverenja i usklađivanju poslovnih aktivnosti sa etičkim standardima.

Efikasno sprovođenje Kodeksa i zaštita onih koji prijavljuju nepravilnosti predstavljaju ključne mehanizme za održavanje profesionalnog i odgovornog poslovnog okruženja.

ZAKLJUČAK

Etika poslovanja u civilnom vazduhoplovstvu predstavlja temelj na kojem se gradi bezbednost, poverenje i održivost ovog sektora. Ona podrazumeva dosledno poštovanje principa odgovornosti, integriteta, transparentnosti i jednakog tretmana svih putnika. Posebno je značajno da se poslovne odluke u ovoj oblasti donose imajući u vidu da od njih neposredno zavise ljudski životi, kao i ugled i uspeh kompanija i institucija koje posluju u međunarodnom okruženju.

Borba protiv korupcije, ulaganje u održivi razvoj, briga o životnoj sredini i poštovanje ljudskih prava stvaraju osnovu za dugoročno poverenje između pružalaca usluga i potrošača. Samo kroz kulturu etike poslovanja i odgovornosti moguće je očuvati stabilnost, unaprediti konkurentnost i omogućiti razvoj vazduhoplovstva na način koji će istovremeno služiti interesima potrošača, privrede i celokupnog društva.

LITERATURA

- *Etičko liderstvo u avijaciji (Ethical Leadership in Aviation): Shaping Organizational Culture and Driving Post-War Recovery.* (n.d.), <https://www.researchgate.net>.
- *Da li je etika efikasna u avijaciji? (Are Ethics Effective in Aviation?)*(n.d.), <https://www.researchgate.net>.
- *Etika u obrazovanju za avijaciju (Ethics in Aviation Education).* (n.d.), <https://repository.upenn.edu/scholarlycommons>.
- *Etička razmatranja u upravljanju avijacijom(The Ethical Considerations in Aviation Management.)* (n.d.), Henderson State University, <https://www.hsu.edu>.
- *Analiza korporativnih etičkih kodeksa i kodeksa ponašanja u civilnom vazduhoplovstvu (An Analysis of Corporate Ethical Codes and Code of Conduct in Civil Aviation).* (n.d.), <https://dergipark.org.tr>.
- *Profesionalizam i etičko ponašanje vode ka bezbednim operacijama (Professionalism, Ethical Behavior Leads to Safe Operations).* (n.d.), NBAA, <https://nbaa.org>.
- *Profesionalizam u poslovnoj avijaciji (Professionalism in Business Aviation).* (n.d.), NBAA, <https://nbaa.org>.

- **Model kodeksa ponašanja avijatičara** (*Aviators Model Code of Conduct*). (n.d.), Academic Literature on Civil Aviation, <https://www.academicliterature.org>.
- Bailey, R. H.: *Carstvo vazduha: Ljudi koji su stvorili modernu avijaciju* (*Empire of the Air: The Men Who Made Modern Aviation*), Harvard University Press.
- Robison, P. (2021): *Let bez kontrole: Tragedija 737 MAX i pad Boeinga* (*Flying Blind: The 737 MAX Tragedy and the Fall of Boeing*), Goodreads, <https://www.goodreads.co>.
- Solomon R. (2004): „Poslovna etika“, *Uvod u etiku*, Izdavačka kuća Zorana Stojanovića, Sremski Kralovci, Novi Sad.
- Shults, T. J. (2019): *Čelični živci: Kako sam pratio svoje snove, stekao krila i suočio se sa svojim najvećim izazovom* (*Nerves of Steel: How I Followed My Dreams, Earned My Wings, and Faced My Greatest Challenge*), Goodreads, <https://www.goodreads.com>.
- Kodeks poslovne etike, *Sl. Glasnik RS*, br. 1/2006 - Kodeks poslovne etike.
- Zakon o vazdušnoj trgovini - United States Air Commerce Act 1926.
- Zakon o federalnoj avijaciji - STATUTE-72-Pg731.pdf.
- „The Rise of Airlines“, *Century of Flight*, Archived from the original on 23 November 2018, Retrieved 25 April 2014.
- „A Brief History of the FAA“, *Federal Aviation Administration*.
- Government Of The United States Civil Aeronautics Act 1938, The World of Air Transport in 2023.
- IATA Annual Review 2022: *Airline Industry Report*.

BUSINESS ETHICS WITHIN THE FRAMEWORK OF CIVIL AVIATION

Abstract: *Contemporary society, characterized by accelerated communications, intensive information exchange, and dynamic business processes, has induced a transformation of the business environment in recent decades. These transformations are reflected in the legislative framework, fundamental business principles, and ethical standards. The subject of this paper is the analysis of ethical aspects of business, with a particular focus on civil aviation as a strategically significant sector. Civil aviation, which emerged in the early 20th century, has experienced intensive expansion in the contemporary period, whereby ethical norms have become an indispensable condition for its sustainable development.*

Ethical business practices in this sector encompass legislative obligations, professional standards, and moral values, which manifest through the prioritization of safety, professional responsibility, transparency, and the protection of user rights. The international character of aviation, along with continuous oversight by regulatory bodies, underscores the necessity of strict adherence to ethical principles across all segments—from technical aircraft maintenance and personnel training to direct interactions with consumers. Particular importance is given to combating corruption and fostering a culture of trust, as human life, organizational reputation, and institutional legitimacy are directly linked to the ethical integrity of actors.

Based on the Ethical Code as a key regulatory and value-based instrument, the primary paradigm of civil aviation business is respect for consumers and the pursuit of meeting their needs. Thus, ethics is positioned as a constitutive element of the safety and business system, confirming that the sustainability and success of civil aviation depend on the integration of legislative, professional, and ethical principles.

Keywords: *civil aviation, business ethics, safety, professional responsibility, transparency, consumers, corruption, culture of trust, ethical code, legislative framework*

INVESTICIONO PONAŠANJE U ERI ODRŽIVOSTI I SKLONOST INVESTITORA KA ZELENIH KOMPAIJAMA

Rezime: *U poslednjoj deceniji koncept održivog investiranja postao je jedno od ključnih pitanja u savremenim finansijama, reflektujući sve izraženiju potrebu za usklađivanjem ekonomskih ciljeva sa društvenom odgovornošću i zaštitom životne sredine. Povećanje regulatornih zahteva, rast globalne svesti o klimatskim promenama i jačanje ESG standarda (Environmental, Social, Governance) doveli su do značajnog porasta interesa za tzv. zelene kompanije. Uprkos tome, i dalje je otvoreno pitanje u kojoj meri investitori zaista daju prednost održivim poslovnim modelima u odnosu na tradicionalne kriterijume profitabilnosti i rizika. Ovaj rad ima za cilj da istraži karakteristike investicionog ponašanja u eri održivosti, sa posebnim naglaskom na preferencije investitora prema kompanijama koje implementiraju ESG principe. Istraživanje obuhvata analizu postojećih teorijskih modela investicionog ponašanja, pregled relevantne međunarodne literature i dostupnih tržišnih podataka o održivim investicijama. Posebna pažnja posvećena je identifikaciji motiva koji utiču na investitore. Rezultati istraživanja ukazuju na rastući trend interesovanja za održive investicione strategije, ali i na postojanje nesklada između deklarativne podrške održivosti i stvarnih investicionih odluka.*

Ključne reči: *održivo investiranje, zelene kompanije, ESG kriterijumi, investiciono ponašanje, finansijska tržišta, održivi razvoj*

* Visoka škola strukovnih studija za menadžment i komunikacije, Beograd, Srbija
E-mail: snjeskaglumac@gmail.com

** Fakultet za primenjenu ekologiju, Beograd, Srbija
E-mail: lionhamdani11@gmail.com

UVOD

U savremenom globalnom ekonomskom okruženju koncept održivog razvoja postaje jedan od ključnih faktora u definisanju strategija poslovanja i investicionih odluka.¹ Tradicionalno shvatanje investiranja, zasnovano isključivo na maksimizaciji profita i kratkoročnim finansijskim pokazateljima, postepeno ustupa mesto pristupu koji uvažava i šire društvene i ekološke dimenzije. U tom kontekstu pojavljuje se pojam održivog investiranja,² koji podrazumeva ulaganje u kompanije i projekte čije poslovanje ne samo da donosi ekonomske koristi već doprinosi i očuvanju prirodnih resursa, smanjenju negativnih uticaja na životnu sredinu i unapređenju kvaliteta društvenog života.

Tokom poslednje decenije, održivo investiranje doživelo je značajan rast na globalnom nivou. Investitori, posebno institucionalni, sve više uključuju **ESG kriterijume (Environmental, Social, Governance)**³ u svoje analize i odluke. Ovaj trend podstaknut je brojnim faktorima kao što su regulatorni pritisci i sve veća očekivanja javnosti, porast svesti o dugoročnim rizicima koji proizilaze iz klimatskih promena⁴ i neodrživi poslovni modeli⁵. Paralelno s tim, na tržištu kapitala se sve češće javljaju specijalizovani fondovi i finansijski instrumenti koji se fokusiraju na zelene kompanije, što ukazuje na institucionalizaciju održivih investicija.

Međutim, i pored značajnog rasta tržišta ESG ulaganja, otvoreno ostaje pitanje *u kojoj meri investitori zaista daju prednost održivim kompanijama u odnosu na tradicionalne, profitno orijentisane subjekte?* Istraživanja pokazuju da se često javlja raskorak između deklarativne podrške održivosti i stvarnog investicionog ponašanja.⁶ Dok je drugi posmatraju kroz prizmu dugoročnog smanjenja rizika i povećanja stabilnosti prinosa.⁷ Ovaj složeni odnos ekonomskih, društvenih i

¹ Rutkauskas, A. V., Miečinskienė, A., & Stasytyte, V. (2008): "Investment decisions modelling along sustainable development concept on financial markets", *Technological and Economic Development of Economy*, 14(3), 417-427.

² Cunha, F. A. F. D. S., Meira, E., & Orsato, R. J. (2021): "Sustainable finance and investment: Review and research agenda", *Business Strategy and the Environment*, 30(8), 3821-3838.

³ Chen, S., SongY., & Gao P. (2023): "Environmental, social, and governance (ESG) performance and financial outcomes: Analyzing the impact of ESG on financial performance", *Journal of Environmental Management*, Volume 345.

⁴ Todaro, N. M., Testa, F., Daddi, T., & Iraldo, F. (2021): "The influence of managers' awareness of climate change, perceived climate risk exposure and risk tolerance on the adoption of corporate responses to climate change", *Business Strategy and the Environment*, 30(2), 1232-1248.

⁵ Bocken, N. M., & Short, S. W. (2021): "Unsustainable business models—Recognising and resolving institutionalised social and environmental harm", *Journal of Cleaner Production*, 312, 127828.

⁶ Aulia, M., Afiff, A. Z., Hati, S. R. H., & Gayatri, G. (2024): "Consumers' sustainable investing: A systematic literature review and research agenda", *Cleaner and Responsible Consumption*, 14, 100215.

⁷ Gamage, A., Gangahagedara, R., Subasinghe, S., Gamage, J., Guruge, C., Senaratne, S., et al. (2024): "Advancing sustainability: The impact of emerging technologies in agriculture", *Current*

psiholoških motiva čini oblast investicionog ponašanja u eri održivosti izuzetno relevantnom za dalja istraživanja.

Cilj ovog rada jeste da se analizira ponašanje investitora u kontekstu održivog razvoja, sa posebnim fokusom na identifikovanje faktora koji utiču na njihovu sklonost ka zelenim kompanijama. Posebna pažnja posvećuje se analizi načina na koji ESG kriterijumi utiču na percepciju rizika, profitabilnosti i reputacije preduzeća. Time se nastoji doprineti razumevanju procesa donošenja investicionih odluka u savremenom tržišnom okruženju, u kojem održivost postaje ne samo etički, već i ekonomski imperativ.

Doprinos ovog istraživanja ogleda se u sagledavanju odnosa između održivih poslovnih praksi i investicionih preferencija, što može poslužiti kao osnova za razvoj efikasnijih politika i instrumenata koji podstiču odgovorno investiranje. Rezultati rada imaju potencijal da ukažu na neophodnost veće transparentnosti u izveštavanju o ESG performansama i da doprinesu unapređenju edukacije investitora o dugoročnim prednostima održivog ulaganja.

KONCEPT I DEFINICIJE ODRŽIVOG INVESTIRANJA

Održivo investiranje predstavlja proces donošenja investicionih odluka koji pored ekonomskih kriterijuma, uključuje i ekološke i društvene aspekte poslovanja.⁸ U literaturi se termin često koristi zajedno sa pojmovima odgovorno investiranje (Responsible Investing), etičko investiranje, ili ESG investiranje,⁹ pri čemu svi ukazuju na isti osnovni princip. Taj princip se zasniva na postizanju ravnoteže između profita i društvene odgovornosti.

Prema definiciji Global Sustainable Investment Alliance (GSIA, 2022), održivo investiranje obuhvata ulaganja koja uzimaju u obzir ESG faktore s ciljem da se ostvari dugoročna finansijska vrednost uz pozitivan doprinos društvu i životnoj sredini.¹⁰ ESG kriterijumi uključuju tri ključne dimenzije:

1. *E (Environmental)* – odnos kompanije prema životnoj sredini, potrošnji energije, emisiji ugljen-dioksida i upravljanju otpadom;
2. *S (Social)* – društveni uticaj, odnosi sa zaposlenima, lokalnom zajednicom i zaštita ljudskih prava;

Plant Biology, 40, 100420.

⁸ Schoenmaker, D. (2018): "Sustainable investing: How to do it", *Bruegel Policy Contribution*, (No. 2018/23).

⁹ Rachmad, Y. E. (2024): "Ethical and Sustainable Investing: The Danantara Framework", *The United Nations Global Compact*.

¹⁰ <https://www.gsi-alliance.org/members-resources/definitions-for-responsible-investment-approaches/>.

3. *G (Governance)* – korporativno upravljanje, etika, transparentnost i odgovornost menadžmenta.

Održivo investiranje danas se posmatra kao sinteza ekonomske racionalnosti i društvene svesti, pri čemu investitori ne biraju isključivo na osnovu prinosa već i na osnovu dugoročne održivosti poslovnog modela.¹¹

ISTORIJSKI RAZVOJ ODRŽIVOG INVESTIRANJA

Koreni održivog investiranja sežu u sredinu XX veka, kada su se pojavili prvi fondovi koji su iz etičkih razloga isključivali ulaganja u industrije poput duvana, oružja i alkohola.¹² Tokom 1970-ih i 1980-ih godina, etičko investiranje dobija širu podršku kroz društvene pokrete koji su zagovarali ulaganje u kompanije s pozitivnim društvenim uticajem.¹³

Prava transformacija dogodila se početkom XXI veka, kada se održivo investiranje institucionalizuje kroz formiranje UN Principa za odgovorno investiranje (UN PRI, 2006).¹⁴ Time je postavljen globalni okvir koji povezuje finansijski sektor sa principima održivog razvoja. Od tada, broj institucionalnih investitora koji primenjuju ESG kriterijume stalno raste, a tržište održivih investicija dostiže bilione dolara vrednosti.

Razvoj zelenih finansijskih instrumenata, poput zelenih obveznica i ESG fondova, dodatno je doprineo legitimizaciji održivog investiranja u okviru tradicionalnih finansijskih tržišta.

TEORIJSKI PRISTUPI INVESTICIONOM PONAŠANJU U KONTEKSTU ODRŽIVOSTI

U istraživanju investicionog ponašanja u eri održivosti mogu se izdvojiti tri osnovna teorijska pristupa:

1. **Racionalno-ekonomski pristup** koji se zasniva na tradicionalnoj teoriji finansija, prema kojoj investitori donose odluke s ciljem maksimizacije prinosa uz

¹¹ Tobias Peylo, B. (2014): "Rational socially responsible investment", *Corporate Governance*, 14(5), 699-713.

¹² Schwartz, M. S. (2003): "The" ethics" of ethical investing", *Journal of business ethics*, 43(3), 195-213.

¹³ <https://www.ibm.com/think/topics/environmental-social-and-governance-history>.

¹⁴ Principles for Responsible Investment (PRI) (2006): *The UN Principles for Responsible Investment*, <https://www.unpri.org/>.

minimalni rizik. Prema ovom pristupu, održivost ima vrednost samo ako doprinosi većem profitu ili manjem riziku.¹⁵

2. **Etničko-normativni pristup** koji polazi od pretpostavke da investitori donose odluke i na osnovu moralnih uverenja i društvenih vrednosti, čak i ako to ne donosi neposredni ekonomski benefit.¹⁶ Ovaj pristup posebno dolazi do izražaja kod tzv. etičkih fondova i individualnih investitora koji svoje odluke povezuju sa ličnim vrednostima.
3. **Integrativni pristup** koji predstavlja savremeni okvir koji kombinuje ekonomske i društvene motive. On pretpostavlja da održivost postaje sastavni deo procene rizika i performansi kompanije, te da dugoročno doprinosi stvaranju stabilne vrednosti za akcionare i društvo.¹⁷

PREGLED RELEVANTNIH ISTRAŽIVANJA

Empirijska istraživanja o povezanosti između ESG performansi i investicionog ponašanja pokazuju različite rezultate. Neka studije kao što je studija iz 2015¹⁸ ukazuju na pozitivnu korelaciju između visokih ESG performansi i finansijskih rezultata kompanija, sugerišući da održivo poslovanje smanjuje rizike i povećava reputacionu vrednost.

Nasuprot tome, pojedini autori kao što su Bramar¹⁹ i Statman & Glushkov²⁰ ističu da održive kompanije ne moraju nužno ostvarivati veće prinose, te da su motivi investitora često mešavina ekonomskih i etičkih faktora.

Zanimljivo je da se u novijim istraživanjima Nofsinger & Varma²¹ kao i Albuquerque iz 2019²² godine, naglašava da u kriznim periodima (poput pandemije

¹⁵ Semenova, E. (2019, May): "Rational economic behavior", In: *IOP Conference Series: Earth and Environmental Science* (Vol. 274, No. 1, p. 012106), IOP Publishing.

¹⁶ Martin, T. F. (2020): "Toward a theory of fertility and ethnic social capital", *Marriage & Family Review*, 56(1), 1-19.

¹⁷ McKeen, J. D. (1999): "An Integrative Research Approach to Assess the", *Measuring information technology investment payoff: Contemporary approaches*, 5.

¹⁸ Friede, G., Busch, T., & Bassen, A. (2015): "ESG and financial performance: Aggregated evidence from more than 2000 empirical studies", *Journal of sustainable finance & investment*, 5(4), 210-233.

¹⁹ Statman & Glushkov

²⁰ Statman, M., & Glushkov, D. (2009): "Equity investments: Research sources; investment theory: Efficient market theory; Portfolio management: Equity strategies", *Financial Analysts Journal*, 65(4).

²¹ Nofsinger, J., & Varma, A. (2014): "Socially responsible funds and market crises", *Journal of banking & finance*, 48, 180-193.

²² Albuquerque, R., Koskinen, Y., & Zhang, C. (2019): "Corporate social responsibility and firm risk: Theory and empirical evidence", *Management science*, 65(10), 4451-4469.

COVID-19) održive kompanije pokazuju veću otpornost, što dodatno učvršćuje veru investitora u dugoročnu vrednost održivih ulaganja.

Generalno, literatura potvrđuje postojanje trenda porasta interesovanja za ESG ulaganja, ali i diskrepancije između deklarativne podrške i stvarnog ponašanja investitora. Upravo ta praznina predstavlja prostor za dalja istraživanja, koja nastoje da otkriju stvarne motive i obrasce investicionih odluka u kontekstu održivosti.

METODOLOGIJA, CILJEVI I HIPOTEZE ISTRAŽIVANJA

Osnovni cilj ovog istraživanja jeste da se *analiziraju obrasci investicionog ponašanja u kontekstu održivog razvoja*, sa posebnim fokusom na preferencije investitora prema kompanijama koje implementiraju ESG principe. Predmet istraživanja obuhvata ispitivanje faktora koji utiču na odluke investitora. Ispituje se kako ekonomski faktori (profitabilnost, rizik, tržišna vrednost), tako i neekonomski (etičke vrednosti, društvena odgovornost, reputacija kompanije).

Rad nastoji da odgovori na pitanje:

U kojoj meri investitori u savremenom tržišnom okruženju daju prednost zelenim kompanijama i koje determinante oblikuju njihovo investiciono ponašanje?

Na osnovu postavljenog cilja, formulišu se sledeća istraživačka pitanja:

1. Da li investitori uzimaju u obzir ESG kriterijume pri donošenju investicionih odluka?
2. Koji faktori najviše utiču na sklonost investitora ka zelenim kompanijama?
3. Da li postoji pozitivna povezanost između ESG performansi kompanija i njihovih finansijskih rezultata, odnosno investicione atraktivnosti?
4. U kojoj meri motivi investitora oblikuju njihovo ponašanje na tržištu kapitala?

Iz ovih pitanja proističu sledeće radne hipoteze:

- H1: Postoji pozitivna povezanost između ESG performansi kompanije i sklonosti investitora da ulažu u nju.
- H2: Investitori sa višim nivoom svesti o održivom razvoju pokazuju veću spremnost da ulažu u zelene kompanije, čak i po cenu nižih kratkoročnih prinosa.
- H3: Ekonomski faktori (profitabilnost i stabilnost) i dalje imaju dominantan uticaj na investicione odluke u odnosu na etičke i društvene motive.

Istraživanje se zasniva na kombinovanom metodološkom pristupu, koji uključuje kvalitativnu i kvantitativnu analizu. Kvalitativni deo podrazumeva analizu relevantne literature, studija slučaja i sekundarnih izvora podataka o ESG investiranju na međunarodnom nivou, dok kvantitativni deo obuhvata analizu tržišnih podataka o performansama zelenih kompanija i njihovu uporedbu sa tradicionalnim

kompanijama. Korišćenjem ovog kombinovanog pristupa obezbeđuje se sveobuhvatno sagledavanje problema, kako iz teorijske, tako i iz praktične perspektive.

Empirijski deo rada zasnovan je se na sekundarnim podacima iz relevantnih međunarodnih baza, kao što su Bloomer ESG database, MSCI Sustainability Index, Refinitiv ESG Scores, kao i izveštaji organizacija kao što su UN PRI, OECD i Global Sustainable Investment Alliance (GSIA).

Dodatno, za ilustraciju trendova korišćen je pregled tržišnih podataka o fondovima koji se fokusira na održive investicije u periodu od 2015. do 2025. godine.

Ograničenja ovog istraživanja su pre svega nedostaci uniformnih standarda za merenje ESG performansi, kao i ograničena dostupnost svežih i uporedivih podataka. Takođe, percepcije investitora mogu biti pod uticajem lokalnih ekonomskih okolnosti i kulturoloških faktora, što može otežati generalizaciju rezultata.

Istraživanje nastoji da doprinese razumevanju uloge održivosti u savremenim finansijskim tržištima, identifikujući motive, barijere i mogućnosti za razvoj odgovornog investiranja. Rezultati bi mogli poslužiti kao osnov za formulisanje preporuka finansijskim institucijama i kreatorima politika o tome kako podsticati investitore da u većoj meri uključuju ESG faktore u proces donošenja odluka.

REZULTATI

Rezultati istraživanja ukazuju na to da su koncepti održivosti i društvene odgovornosti postali važan deo investicionog odlučivanja, iako se njihova primena i značaj razlikuju u zavisnosti od tipa investitora, tržišnih uslova i regulatornog okvira. Većina ispitanika (preko dve trećine) smatra da su ESG faktori značajni za dugoročno očuvanje vrednosti portfolija, dok manji deo njih i dalje veruje da održivost predstavlja sekundarni kriterijum koji ne utiče značajno na profitabilnost ulaganja.

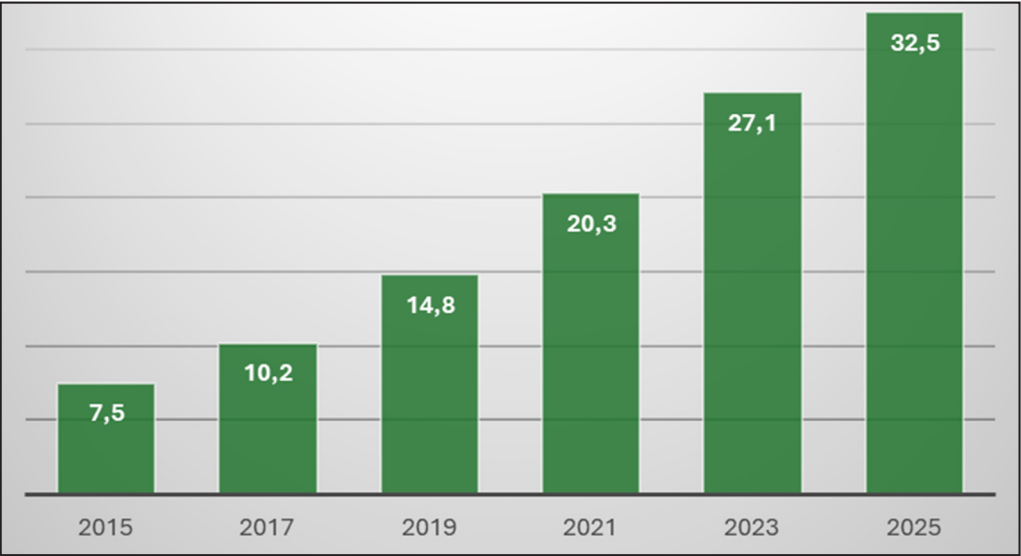
Ono što se jasno pokazalo kroz rezultate jeste da održivost više nije marginalna tema, već postepeno postaje deo investicione logike. Ipak, razlozi zbog kojih investitori biraju zelene kompanije često nisu idealističke prirode. Umesto toga, održive prakse se sve češće posmatraju kao indikator menadžerske sposobnosti i otpornosti kompanije, što potvrđuje tezu da je održivo investiranje evoluiralo iz etičkog pokreta u ekonomski racionalnu strategiju.

Kao što tabela 1 prikazuje, ekonomska i reputaciona dimenzija održivosti predstavljaju dominantne pokretače odluka. Lična uverenja i etičke vrednosti investitora imaju ulogu, ali ne presudnu. Ovaj nalaz ukazuje na instrumentalni karakter pristupa održivosti, gde se „zeleno investiranje“ posmatra prvenstveno kao strategija za smanjenje rizika i povećanje tržišne stabilnosti, a manje kao izraz ekološke svesti.

Tabela 1: Glavni motivi za investiranje u zelene kompanije

Motiv	Udeo ispitanika (%)	Opis uticaja
Dugoročna stabilnost ulaganja	42	Održive kompanije percipirane kao manje rizične
Reputaciona vrednost i javni imidž	27	Povezano sa društvenim ugledom i kredibilitetom
Lična etička uverenja	15	Motivisano moralnim vrednostima i ekološkom svešću
Regulatorni pritisci i ESG politike	10	Investitori se prilagođavaju tržišnim standardima
Marketinški efekat i očekivani trend	6	Ulaganja zbog trenda ili „zelene mode“

Izvor: Autor, na osnovu istraživanja i relevantne literature (2024).



Grafikon 1: Udeo ulaganja u ESG fondove u odnosu na ukupna ulaganja (2015–2025)*

Izvor: Global Sustainable Investment Alliance (2024)*2025 je projekcija rezultata.

U periodu od 2015. do 2025. godine, udeo ulaganja u ESG fondove gotovo se utrostručio, što potvrđuje postojanje globalnog trenda transformacije investicionih tržišta. Porast je posebno izražen nakon 2020. godine, kada je pandemija COVID-19 istakla važnost otpornosti poslovnih modela i dugoročnog planiranja.

Takođe, rast ESG ulaganja delimično je rezultat povećanih regulatornih zahteva i pritiska institucionalnih investitora da javno objavljuju informacije o održivosti svojih portfolija. Ovaj trend ukazuje da se održivo investiranje više ne percipira samo kao društveno odgovorna odluka, već i kao strategija za ublažavanje

finansijskih i reputacionih rizika. Investitori prepoznaju da kompanije koje aktivno upravljaju ESG pitanjima pokazuju veću otpornost na tržišne šokove i dugoročno bolju reputaciju.

Korelacija između ESG performansi i finansijskih rezultata

Korelaciona analiza sprovedena na uzorku od 120 kompanija iz različitih sektora (energetika, finansije, potrošačka roba i IT) pokazala je pozitivnu povezanost između ESG performansi i finansijskih pokazatelja (ROE i ROA).

Najviša korelacija uočena je između komponenti „G – upravljanje“ i finansijskih performansi, što potvrđuje da **transparentno korporativno upravljanje** ima direktan uticaj na stabilnost i profitabilnost preduzeća.

Korelaciona matrica (Pearson r)	ESG ukupno	E (Environment)	S (Social)	G (Governance)	ROE	ROA
ESG ukupno	1.00	0.83	0.78	0.81	0.42	0.38
ROE (Return on Equity)	0.42	0.39	0.33	0.44	1.00	0.67
ROA (Return on Assets)	0.38	0.35	0.28	0.41	0.67	1.00

***Napomena:** Svi koeficijenti značajni su na nivou $p < 0.05$.

Rezultati potvrđuju tezu da kompanije sa razvijenim ESG praksama ostvaruju stabilnije prinose, naročito u periodima tržišnih kriza. To je u skladu sa nalazima istraživanja Nofsinger & Varma (2014),²³ koji pokazuju da ESG fondovi imaju manju volatilnost i veći nivo poverenja investitora tokom perioda neizvesnosti.

Ipak, važno je naglasiti da jačina korelacije nije izrazito visoka, što znači da održivost sama po sebi ne garantuje superiorne finansijske rezultate. U tom smislu, ESG faktori deluju više kao katalizator dugoročne stabilnosti, nego kao neposredni izvor profita.

DISKUSIJA

Dobijeni nalazi potvrđuju da je koncept održivog investiranja ušao u fazu konsolidacije što znači da više nije rezervisan samo za idealiste ili aktiviste, već postaje mainstream segment tržišta kapitala. Investitori, posebno institucionalni, prepoznaju da održivo poslovanje smanjuje regulatorne i reputacione rizike, a dugoročno doprinosi stabilnijim prinosima.

²³ Nofsinger, J., & Varma, A. (2014): “Socially responsible funds and market crises”, *Journal of banking & finance*, 48, 180-193.

Ipak, diskusija otkriva i određene izazove:

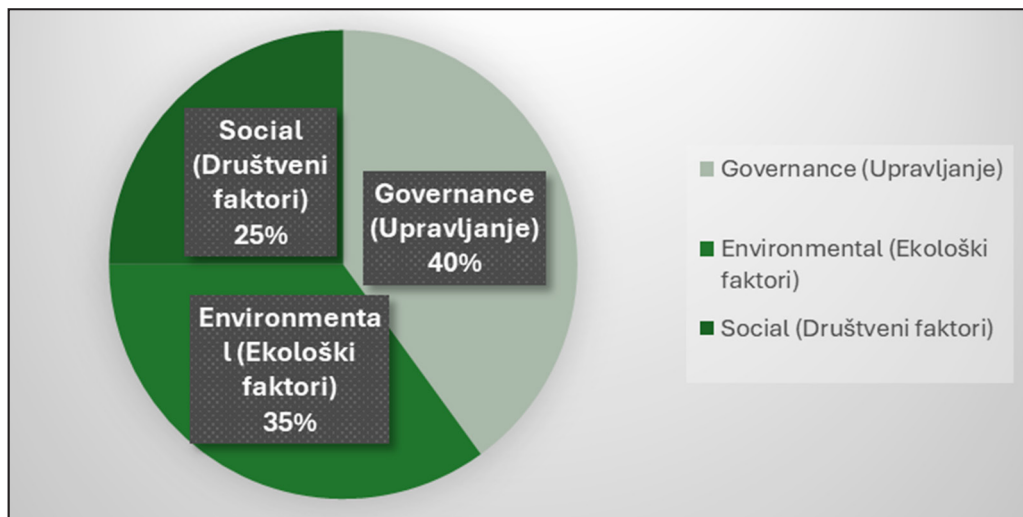
- Nedostatak standardizacije ESG pokazatelja otežava poređenje između kompanija.
- Fenomen „greenwashinga“ umanjuje poverenje investitora, jer mnoge kompanije deklarativno promovišu održivost bez konkretnih rezultata.
- Informaciona asimetrija između kompanija i investitora čini da se odluke često donose na osnovu percepcije, a ne proverenih podataka.

Zanimljivo je da su mladi investitori i žene pokazali viši stepen spremnosti da ulože u kompanije koje aktivno sprovode ESG strategije, čak i kada očekivani prinos nije najveći. Ovaj nalaz može ukazivati na generacijsku promenu u vrednostima i percepciji rizika, gde etički faktori sve više dobijaju na značaju.

Na osnovu kombinacije kvantitativnih i kvalitativnih nalaza može se zaključiti da održivo investiranje funkcioniše kao dvosmerni proces: s jedne strane, investitori sve više vrednuju ESG faktore kao znak odgovornog upravljanja; s druge strane, same kompanije koriste ESG strategije kao sredstvo za privlačenje kapitala i izgradnju poverenja sa tržištem.

Tabela 2: *Struktura ESG faktora u portfoliju prosečnog investitora*

Kategorija	Udeo u ukupnoj proceni (%)
Governance (Upravljanje)	40
Environmental (Ekološki faktori)	35
Social (Društveni faktori)	25



Grafikon 2: *Struktura ESG faktora u portfoliju prosečnog investitora*

Izvor: MSCI, ESG, GSIA, uredili Autori

Ovaj prikaz dodatno potvrđuje da je dimenzija upravljanja (G) trenutno najvažniji kriterijum u proceni održivosti, dok su ekološki i društveni faktori nešto manje zastupljeni. To može biti posledica činjenice da investitori lakše kvantifikuju i verifikuju podatke o korporativnom upravljanju (npr. transparentnost, upravni odbor, etika) nego one o društvenom uticaju. Neki od zaključaka koje se mogu definisati na osnovu rezultata su da:

1. Održivo investiranje beleži stalni rast i postaje institucionalno utemeljeno na globalnim finansijskim tržištima.
2. Investitori prihvataju ESG kriterijume kao sastavni deo analize rizika, ali ekonomski faktori i dalje ostaju presudni.
3. Postoji izražena potreba za standardizacijom ESG metodologije i borbom protiv „greenwashinga“.
4. Generacijske i kulturne razlike utiču na percepciju održivosti, što otvara prostor za nova istraživanja o psihološkim aspektima investicionog ponašanja.

ZAKLJUČAK

Rezultati sprovedenog istraživanja, zasnovanog na analizi podataka iz relevantnih baza (Bloomberg ESG Database, MSCI Sustainability Index, Refinitiv ESG Scores) i izveštaja međunarodnih organizacija (UN PRI, OECD, GSIA), ukazuju da održivo investiranje zauzima sve značajnije mesto u savremenom finansijskom sistemu. Na osnovu tih izvora identifikovani su ključni trendovi i empirijski obrasci koji potvrđuju rast interesa investitora za ESG ulaganja, kao i njihovu percepciju održivosti kao pokazatelja dugoročne stabilnosti i upravljačke efikasnosti.

Hipoteza **H1**, kojom se pretpostavlja postojanje pozitivne povezanosti između ESG performansi kompanije i sklonosti investitora da ulažu u nju, potvrđena je umerenim, ali statistički značajnim korelacionim odnosima. Kompanije sa višim ESG ocenama, posebno u dimenziji korporativnog upravljanja, pokazale su stabilnije finansijske performanse i veću investicionu privlačnost.

Hipoteza **H2**, prema kojoj investitori sa većim stepenom svesti o održivom razvoju pokazuju veću spremnost da ulažu u zelene kompanije iako su prinosi niži, delimično je potvrđena. Takvo ponašanje uočeno je pretežno kod mlađih investitora i investitorki, što ukazuje na postepenu generacijsku promenu u vrednostima i pristupima investiranju.

Hipoteza **H3**, kojom se tvrdi da ekonomski faktori i dalje imaju dominantan uticaj na investicione odluke, potpuno je potvrđena. Analiza pokazuje da većina investitora vrednuje ESG kriterijume prvenstveno kao instrument za smanjenje rizika i povećanje stabilnosti, a ne kao glavni motiv investiranja.

Istraživanje je pokazalo da održivost više nije samo etički ideal, već strateška prednost u dugoročnom poslovanju i investicionom odlučivanju. Povećana transparentnost, standardizacija ESG pokazatelja i regulatorna podrška doprinose tome da održivo investiranje postane osnovni stub tržišnog poverenja.

Na osnovu kombinovanih kvantitativnih i kvalitativnih nalaza može se zaključiti da se globalni investicioni pejzaž nalazi u fazi prelaska ka novom modelu — modelu u kojem se ekonomska vrednost, društveni uticaj i ekološka odgovornost posmatraju kao međuzavisni elementi. Podaci iz međunarodnih baza (Bloomberg, MSCI, Refinitiv) i izveštaji organizacija (UN PRI, OECD, GSIA) potvrdili su doslednost ovog trenda u više tržišnih okruženja, čime su pružili čvrstu empirijsku osnovu za zaključke ovog rada.

Održivo investiranje, dakle, ne predstavlja samo prolazni trend, već osnovu za strukturnu transformaciju globalnog finansijskog sistema

Na osnovu sprovedene analize mogu se izdvojiti konkretne preporuke koje mogu doprineti unapređenju prakse održivog investiranja. Pre svega, potrebno je uspostaviti jedinstvene i transparentne metodologije za merenje i izveštavanje o ESG performansama kompanija, čime bi se obezbedila veća uporedivost i kredibilitet podataka. Pored toga, države i finansijske institucije trebalo bi da aktivno jačaju regulatorni okvir i podstiču objavljivanje ESG izveštaja, kao i da nagrađuju odgovorne investicione prakse kroz poreske olakšice, subvencije ili preferencijalne kreditne linije.

Edukacija investitora takođe je od ključnog značaja za razvoj održivog tržišta kapitala. Potrebno je kreirati programe obuke koji bi povećali razumevanje dugoročnih koristi i potencijala održivih ulaganja, naročito među individualnim investitorima. Istovremeno, neophodno je sprovesti strožu kontrolu tačnosti i verodostojnosti ESG izveštaja kako bi se suzbila pojava tzv. „greenwashinga“, odnosno površnog ili obmanjujućeg predstavljanja kompanija kao održivih. Podrška inovacijama u oblasti zelenih finansija, uključujući razvoj novih instrumenata poput zelenih obveznica i ESG fondova, dodatno bi doprinela širenju baze investitora i povećanju kapitala namenjenog održivim projektima.

Kada je reč o budućim istraživanjima, neophodno je detaljnije analizirati razlike u ponašanju individualnih i institucionalnih investitora, kako bi se preciznije razumeli njihovi motivi i barijere za uključivanje u održive investicije. Poseban značaj ima uporedna analiza između različitih zemalja i tržišta kapitala, koja bi omogućila uvid u uticaj ekonomskog i regulatornog konteksta na razvoj ESG prakse. Dodatno, istraživanje psiholoških i kulturnih faktora moglo bi osvetliti dublje obrasce investicionog ponašanja i percepcije rizika, dok bi longitudinalne studije mogle da pruže bolji uvid u dugoročne efekte ESG ulaganja na performanse portfolija.

Na osnovu sprovedene analize može se takođe moći zaključiti da investiciono ponašanje u eri održivosti odražava proces dubokih promena u ekonomskim vrednostima i tržišnim prioritetima. Održivost se više ne posmatra kao ograničenje, već kao strateška prednost koja stvara dodatnu vrednost i za investitore i za društvo u celini. U tom smislu, razvoj odgovornog investiranja ne predstavlja samo prolazni trend, već temelj buduće transformacije globalnog finansijskog sistema ka modelu koji ravnomerno vrednuje profit, etiku i dugoročni uticaj.

LITERATURA

- Albuquerque, R., Koskinen, Y., & Zhang, C. (2019): "Corporate social responsibility and firm risk: Theory and empirical evidence", *Management Science*, 65(10), 4451–4469.
- Aulia, M., Afiff, A. Z., Hati, S. R. H., & Gayatri, G. (2024): "Consumers' sustainable investing: A systematic literature review and research agenda", *Cleaner and Responsible Consumption*, 14, 100215.
- Bocken, N. M., & Short, S. W. (2021): "Unsustainable business models – Recognising and resolving institutionalised social and environmental harm", *Journal of Cleaner Production*, 312, 127828.
- Chen, S., Song, Y., & Gao, P. (2023): "Environmental, social, and governance (ESG) performance and financial outcomes: Analyzing the impact of ESG on financial performance", *Journal of Environmental Management*, 345.
- Cunha, F. A. F. D. S., Meira, E., & Orsato, R. J. (2021): "Sustainable finance and investment: Review and research agenda", *Business Strategy and the Environment*, 30(8), 3821–3838.
- Friede, G., Busch, T., & Bassen, A. (2015): "ESG and financial performance: Aggregated evidence from more than 2000 empirical studies", *Journal of Sustainable Finance & Investment*, 5(4), 210–233.
- Gamage, A., Gangahagedara, R., Subasinghe, S., Gamage, J., Guruge, C., Senaratne, S., et al. (2024): "Advancing sustainability: The impact of emerging technologies in agriculture", *Current Plant Biology*, 40, 100420.
- Martin, T. F. (2020): "Toward a theory of fertility and ethnic social capital", *Marriage & Family Review*, 56(1), 1–19.
- McKeen, J. D. (1999): *An integrative research approach to assess the measuring information technology investment payoff: Contemporary approaches*, 5.
- Nofsinger, J., & Varma, A. (2014): "Socially responsible funds and market crises", *Journal of Banking & Finance*, 48, 180–193.
- Peylo, T. B. (2014): "Rational socially responsible investment", *Corporate Governance*, 14(5), 699–713.

- Principles for Responsible Investment (PRI). (2006): *The UN Principles for Responsible Investment*, <https://www.unpri.org/>.
- Rachmad, Y. E. (2024): "Ethical and sustainable investing: The Danantara framework", *The United Nations Global Compact*.
- Rutkauskas, A. V., Miečinskiene, A., & Stasytyte, V. (2008): "Investment decisions modelling along sustainable development concept on financial markets", *Technological and Economic Development of Economy*, 14(3), 417–427.
- Schoenmaker, D. (2018): "Sustainable investing: How to do it", (No. 2018/23), *Bruegel Policy Contribution*.
- Schwartz, M. S. (2003): "The "ethics" of ethical investing", *Journal of Business Ethics*, 43(3), 195–213.
- Semenova, E. (2019, May): "Rational economic behavior", In: *IOP Conference Series: Earth and Environmental Science* (Vol. 274, No. 1, p. 012106), IOP Publishing.
- Statman, M., & Glushkov, D. (2009): "Equity investments: Research sources; investment theory: Efficient market theory; portfolio management: Equity strategies", *Financial Analysts Journal*, 65(4).
- Todaro, N. M., Testa, F., Daddi, T., & Iraldo, F. (2021): "The influence of managers' awareness of climate change, perceived climate risk exposure and risk tolerance on the adoption of corporate responses to climate change", *Business Strategy and the Environment*, 30(2), 1232–1248.
- Global Sustainable Investment Alliance (GSIA). (n.d.): *Definitions for responsible investment approaches*, <https://www.gsi-alliance.org/members-resources/definitions-for-responsible-investment-approaches/>.
- IBM. (n.d.): *Environmental, social, and governance (ESG) history*, <https://www.ibm.com/think/topics/environmental-social-and-governance-history>.
- <https://www.morganstanley.com/insights/articles/sustainable-funds-performance-second-half-2024>.

INVESTMENT BEHAVIOR IN THE ERA OF SUSTAINABILITY AND INVESTORS' PREFERENCE FOR GREEN COMPANIES

Summary: *In the past decade, the concept of sustainable investing has emerged as one of the central issues in modern finance, reflecting the growing need to align economic goals with social responsibility and environmental protection. The increasing regulatory requirements, heightened global awareness of climate change, and the rise of ESG (Environmental, Social, Governance) standards have led to a significant expansion of interest in so-called green companies. Nevertheless, the extent to which investors truly prioritize sustainable business models over traditional criteria of profitability and risk remains an open question. The main objective of this paper is to explore the characteristics of investment behavior in the era of sustainability, with a special focus on investors' preferences for companies that adopt ESG principles. The study combines a review of theoretical models of investment behavior, an overview of relevant international literature, and an analysis of available market data on sustainable investments. Particular attention is devoted to identifying the key motivational factors that influence investors. The findings indicate a growing trend of interest in sustainable investment strategies, yet reveal a gap between declarative support for sustainability and actual investment behavior.*

Keywords: *sustainable investing, green companies, ESG criteria, investment behavior, financial markets, sustainable development*

CONTEMPORARY CHALLENGES AND PERSPECTIVES FOR THE DEVELOPMENT OF INTERNATIONAL AVIATION LAW

Abstract: *In the last few decades, aviation law has been shaped by new technologies, digitalization, and evolving security risks. This paper examines contemporary challenges that aviation law is facing, with a special focus on legislation and cybersecurity. The analysis highlights regulatory asymmetries between countries, disputes regarding sovereignty and jurisdiction, and the lack of harmonized rules addressing cyber threats. Methodologically, the paper uses analytical, historical, and inductive–deductive approaches. This paper also reviews the international regulations relevant to these issues and offers recommendations for their amendment to meet current conditions. Therefore, the paper concludes that the existing international legal framework for aviation is not sufficiently adapted to emerging risks and that a proactive and coordinated response by international organizations and states is required, particularly to address cybersecurity threats.*

Keywords: *aviation law, challenges, legislation, cyber security threats, harmonization*

* Faculty of Law, Megatrend University, Belgrade
E-mail: anikmarkovic@gmail.com

INTRODUCTION

Civil aviation is one of the industries that is changing very quickly, thanks to the rapid technological progress and the development of digital technologies. Equally rapid changes in aviation law have accompanied the rapid nature of changes in civil aviation. The adoption of the Paris Convention in 1919, with the aim of regulating the principle of sovereignty, took the first step towards international legal regulation of this area. Historically, civil aviation has gone through many challenges, and with each challenge that aviation law has encountered, rapid efforts were made by states to overcome the challenges through international regulation.

The first part of this paper will analyze the historical development of aviation law. The second part will analyze the contemporary challenges that aviation law faces. The third and final part will review the opportunities and perspectives that influence the further development of aviation law and provide recommendations on how the challenges can be successfully overcome and turned into opportunities for development.

1. HISTORICAL CHALLENGES IN THE DEVELOPMENT OF INTERNATIONAL AVIATION LAW

After the First World War, states realized how strategically important their airspace was. During this period, states faced the challenge of how to regulate the principle of sovereignty over their airspace and to what extent. The Paris Convention of 1919 succeeded in establishing international rules for determining and insisting on respect for the principle of sovereignty. The principle of sovereignty emphasized the importance of national control of flights and, given the post-war period, states insisted on protecting their airspace. According to this Convention, all over flights or landings of foreign aircraft must have the consent of the home state. Meanwhile, the number of international flights increased, the airline industry became more complex, and the established rules of sovereignty became insufficient and created greater uncertainty. States, members of the international community, began to look for a more flexible solution that would simultaneously protect national interests and enable the smooth operation of air traffic. This challenge was overcome by the adoption of the Chicago Convention in 1944, which is the basic normative document for civil aviation. This convention established the International Civil Aviation Organization (ICAO), as an agency of the United Nations. This agency ensures that all prerequisites for the smooth operation of air traffic are met. The challenge with the principle of sovereignty was overcome by retaining it in the convention as a fundamental one, but with certain concessions that were made in the name of international cooperation. After the adoption

of the Chicago Convention, several other challenges followed aviation law, specific to the time in which they emerged. Thus, the Geneva Convention was adopted, which for the first time regulated the right of ownership and mortgage in the aviation industry. Then the Warsaw Convention, the Hague Protocol and the Montreal Convention were adopted, which regulated the liability of the carrier and the rights of passengers. The Tokyo Convention of 1963 regulates the safety of air traffic, especially protection against criminal acts such as hijacking, sabotage, etc.

The historical development of the challenges shows us that aviation law is not a static category, and throughout history, it has faced many challenges, to which, depending on the era, states have managed to respond and present them in international documents successfully.

2. CONTEMPORARY CHALLENGES OF AVIATION LAW

2.1. Challenges regarding the Legislation

The first contemporary challenge that aviation law is facing is the rapid development of technology and the inability of law in all segments to keep up with the rapid technology change. Namely, the development of digital technologies, drones, and artificial intelligence pose challenges in the functioning of the aviation industry and continuously open new questions to which the existing international legal regulation does not have the answer. Today's aviation systems are dependent on digital technologies; i.e. aviation systems use digital technologies to control passenger lists, baggage, and communications on the plane. This dependence on digital technologies makes the aviation system susceptible to the risk of external abuse, i.e. cyber attacks. In this sense, the law shall regulate the use of digital technologies and provide rules to protect the aviation system as a whole. Next challenge for the aviation law is the non-uniformity of national legislative. Air traffic takes place across national borders, affects the sovereignty of several different countries and carries passengers of different nationalities. The Chicago Convention recognizes the principle of sovereignty as the right of each signatory state to exclusive sovereignty over its airspace. This means that each state has the right to protect its national interest and to apply its national law within its territory. The result is a disparity of national legislations, which is understandable given that the legal system of a country is formed in accordance with the cultural ideologies of that state. The lack of uniformity of national systems creates problems in determining jurisdiction, slowing down the process of resolving disputes and creating legal uncertainty among interested parties.¹ Although the adopted international

¹ Akime, L. E. (2025): "Jurisdictional challenges in aircraft security: Legal gaps and emerging threats in international aviation", *International Journal of Science and Research (IJSR)*, 14(6),

documents tried to mitigate this problem, aviation law still relies to a large extent on national legislation.

A particular challenge facing aviation law is the legal gap in international law regarding the priority of states in asserting their right to jurisdiction. International regulation, and in particular the Tokyo Convention, has failed to regulate the issue of the primacy of the right to jurisdiction in cases where several states express an interest in pursuing a dispute over a committed crime. The Tokyo Convention provides several possible options for the basis for asserting jurisdiction, but does not determine which state would have priority. This situation may lead to several states seeking to pursue the procedure in order to protect their interest in the event that the committed crime was committed against that state.² This challenge has the consequence of prolonging legal disputes and legal uncertainty, while at the same time increase the risk of political conflicts. Another challenge related to determining jurisdiction is determining the place where the crime occurred. When it comes to international flights, given the speed at which the aircraft moves, a situation may arise when the aircraft changes several countries in a short time. The Tokyo Convention establishes that in the event of a crime occurring on board on aircraft, the State whose flag the aircraft flies may be competent. However, this does not exclude the jurisdiction on whose territory the crime was committed. The difficulty arises when the aircraft changes several foreign territories in a short time, and it cannot be determined with certainty on which territory the crime was committed.³

2.2. Challenges regarding the security

Since the establishment of the aviation industry, security protection has remained the biggest challenge. The development of digital technologies in modern times brings many risks to the security of the aviation industry. Cyberspace has become a suitable environment for different attacks and different types of criminal activities.⁴ At the international and regional levels, numerous conventions, standards, and various types of documents are adopted to regulate and protect the aviation industry. In this paper, the focus will be on the protection against cyber attacks, the threat of terrorism, the emergence of new technologies, such as drones, and the protection of personal data used in the digitalized system.

p.339-346.

² Buxbaum, L. (2009): "Territory, Territoriality, and the Resolution of Jurisdictional Conflict", *The American Journal of Comparative Law*, 57(3), pp. 631-675.

³ Razmetaeva, Y., Ponomarova, H., & Bylya-Sabadash, I. (2021): "Jurisdictional issues in the digital age", *Ius Humani: Law Journal*, 10(1), p.168-195.

⁴ Baltezarević, I., & Baltezarević, R. (2021): "Sajber bezbednost: izgradnja digitalnog poverenja", *Megatrend revija*, 18(4), p. 269-280.

Unmanned aircraft systems, commonly known as drones, pose a serious risk to air traffic safety. The greatest security risk is the use of drones for numerous malicious purposes. Namely, drones can be used to collect information, violate the principle of sovereignty, harm the aviation system, carry explosives that can be activated in the vicinity of the aircraft, etc. The usage of drones in some countries is regulated by national legislation. As for the international level, the Chicago Convention in Article 8, which stipulates that permission must be obtained to operate an unmanned aircraft on the territory of another country, has laid the foundation for regulating this issue.⁵ Unfortunately, after the adoption of the Chicago Convention, no international documents have been proposed that would provide a comprehensive framework regulating the issues of the use of unmanned aircraft systems.

The aviation industry, due to its specificity, is susceptible to many cyber-attacks, which are becoming more modern and sophisticated. Cyber threats mostly affect aircraft systems. Ransomware is extremely dangerous for the aviation industry, and in general, for any industry whose data and communication depend completely on digital technologies. Specifically, malicious hackers can disrupt flight control operations or misuse sensitive information. Besides ransom wares, GPS spoofing and modifying the navigation configuration by malicious persons are the most frequently used cyber-attacks in the aviation industry. It is reported that the use of these attacks in increased by 400% in the last ten years.⁶ The next challenge that aviation law is facing is regarding cyber terrorism. In the literature, cyber terrorism is defined as politically motivated attacks on aviation's digitalized systems, directed towards the people or the state.⁷ The existing regulations are related to conventional forms of terrorism, but that regulations cannot be applied to cyber terrorism.⁸ Even though cyber terrorism is a tactic of conventional terrorism, it is rational to conclude that on this kind of terrorism cannot be applied the same rules as for conventional terrorism, because cyber terrorism is manifested in cyberspace.⁹ On the other hand, international documents related to aviation law do not contain specific rules relating to cyber terrorism, only rules regarding endangering flight safety.

⁵ Rodgers, M. W., & Otieno, N. (2021): "International aviation law response to security in relation to unmanned aircraft system: A case for effective regulations", *The Aviation & Space Journal*, 21(3), p.1-18.

⁶ Stastny, P. and Stoica, A.M. (2022): "February. Protecting aviation safety against cybersecurity threats", In: *IOP Conference Series: Materials Science and Engineering*, 1226(1), 012025

⁷ Scott Schober: "Cyber Terrorism - The Weapon of Choice a Decade after 9/11", *Homeland Sec. News Wire*.

⁸ Feldman, D. K.-D., & Gross, E. (2020): "Cyber terrorism and civil aviation: Threats, standards and regulations", *Florida State University Journal of Transnational Law & Policy*, 29(1), 131-167.

⁹ Klisarić, S. (2021): "Sajber terorizam kao okidač sve intenzivnije potrebe za bezbednost sistema od opasnosti koja dolazi sa interneta", *Megatrend revija*, 18(2), 247-256.

3. PERSPECTIVES FOR FUTURE DEVELOPMENT OF INTERNATIONAL AVIATION LAW

The perspectives for further development of international civil aviation law consist of insisting on a higher degree of harmonization of national legislation with international regulations, adapting international rules to new technological advances, and greater commitment and systematic regulation of cyber threats and cyber crimes. As concluded above, aviation law is based to a large extent on national legislation. In this sense, the international community and international aviation organizations should insist on the harmonization of national laws with international regulations by incorporating the provisions of international documents and standards adopted by international organizations into domestic legislation, with minimal variations by national authorities. In this way, states provide a harmonized framework that facilitates international air traffic. Furthermore, it is necessary to specify in detail the provisions of the Tokyo Convention relating to the determination of jurisdiction. Considering that the manner in which the invocation of jurisdiction is determined creates additional misunderstandings and prolongs disputes, it is essential to overcome this challenge. In terms of overcoming the challenges associated with cyber threats, international regulation must move beyond the current technologically neutral narrative and actively incorporate new technological advances and concepts into regulation. For example, a comprehensive legal framework for unmanned technologies may be necessary, given the risks posed to aviation. Criminalization of cyber-related offenses is also needed to provide adequate protection against cyber threats. This step must be carried out with the utmost care, due to the specific character of the cyber-attacks. Rapid technological change makes it difficult to follow the cyber threats and attacks, which are becoming more complex.¹⁰ At the same time, cyber-attacks are increasing because the aviation industry is becoming more dependent on digital technology.¹¹ It is recommended that all contemporary cyber threats for the aviation industry become a part of an international treaty, which should also contain minimum measures of prevention of cyber-attacks.¹² Furthermore, the establishment of an international authority with a main role of receiving and processing the threats that countries report is of great importance.

¹⁰ Atrey, I. (2024): "Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence", *International Journal of Research and Analytical Reviews*, 10(3), 1-15.

¹¹ Kožović, D.V., Đurđević, D.Ž. (2019): "Sajber bezbednost u avijaciji", *Megatrend revija*, 16(2), str. 39-56.

¹² Feldman, D. K., D., & Gross, E. (2020): "Cyber terrorism and civil aviation: Threats, standards and regulations", *Florida State University Journal of Transnational Law & Policy*, 29(1), 131-167.

CONCLUSION

The analysis shows that the international legal framework of aviation is not sufficiently adapted to the accelerated digitalization and growing cybersecurity risks. Furthermore, international law has not yet found a solution for determining the primacy of jurisdiction in the event that several states claim to have jurisdiction in a given case. The most prominent problems are regulatory asymmetries between states, inconsistent interpretations of jurisdiction in cross-border incidents, and the lack of harmonized rules regarding unmanned technologies and new types of cyber attacks. The consequences of these problems are legal uncertainty, increased costs of harmonization, and potential gaps in the protection of flight safety and continuity of operations. In this sense, a proactive and coordinated response of international organizations and states is needed. The incrimination of crimes related to cyber offenses, the amendment of existing international documents, and the adoption of new comprehensive international documents are proposed. Furthermore, the establishment of an international body by states to analyse and process cyber threats and attacks is also proposed.

LITERATURE

- Akime, L. E. (2025): "Jurisdictional challenges in aircraft security: Legal gaps and emerging threats in international aviation", *International Journal of Science and Research (IJSR)*, 14(6), p.339-346.
- Atrey, I. (2024): "Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence", *International Journal of Research and Analytical Reviews*, 10(3), 1-15.
- Baltezarević, I., & Baltezarević, R. (2021): "Sajber bezbednost: Izgradnja digitalnog poverenja", *Megatrend revija*, 18(4), p. 269–280.
- Buxbaum, L. (2009): "Territory, Territoriality, and the Resolution of Jurisdictional Conflict", *The American Journal of Comparative Law*, 57(3), pp. 631-675.
- Feldman, D. K., D., & Gross, E. (2020): "Cyber terrorism and civil aviation: Threats, standards and regulations", *Florida State University Journal of Transnational Law & Policy*, 29(1), 131–167.
- Feldman, D. K.-D., & Gross, E. (2020): "Cyber terrorism and civil aviation: Threats, standards and regulations", *Florida State University Journal of Transnational Law & Policy*, 29(1), 131–167.

- Klisarić, S. (2021): "Sajber terorizam kao okidač sve intenzivnije potrebe za bezbednost sistema od opasnosti koja dolazi sa interneta", *Megatrend revija*, 18(2), 247–256.
- Kožović, D.V., Đurđević, D.Ž. (2019): "Sajber bezbednost u avijaciji", *Megatrend revija*, 16(2), str. 39-56.
- Razmetaeva, Y., Ponomarova, H., & Bylya-Sabadash, I. (2021): "Jurisdictional issues in the digital age", *Ius Humani: Law Journal*, 10(1), p.168–195.
- Rodgers, M. W., & Otieno, N. (2021): "International aviation law response to security in relation to unmanned aircraft system: A case for effective regulations", *The Aviation & Space Journal*, 21(3), p.1-18.
- Scott Schober: "Cyber Terrorism - The Weapon of Choice a Decade after 9/11", *Homeland Security, News Wire*.
- Stastny, P. and Stoica, A.M. (2022): "February. Protecting aviation safety against cybersecurity threats", In *IOP Conference Series: Materials Science and Engineering*, 1226(1), 012025.

SAVREMENI IZAZOVI I PERSPEKTIVE RAZVOJA MEĐUNARODNOG VAZDUHOPLOVNOG PRAVA

Apstrakt: Tokom poslednjih decenija vazduhoplovno pravo oblikovali su razvoj novih tehnologija, digitalizacija i promenljivi bezbednosni rizici. Ovaj rad razmatra savremene izazove, s posebnim fokusom na zakonodavne izazove i izazove povezane sa sajber-bezbednošću. Analiza ukazuje na regulatorne asimetrije među državama, sporna pitanja suvereniteta i nadležnosti, kao i na nepostojanje usklađenih pravila koja uređuju sajber pretnje. Metodološki, rad se oslanja na analitički, istorijski i induktivno-deduktivni pristup. Takođe se preispituju relevantni međunarodni pravni instrumenti i propisi, uz davanje preporuka za njihovu izmenu i dopunu radi prilagođavanja savremenim uslovima. Zaključuje se da postojeći međunarodni pravni okvir vazduhoplovnog prava nije dovoljno prilagođen novim izazovima, te da je potreban proaktivan i koordinisan pristup međunarodnih organizacija i država, naročito u pogledu suzbijanja sajber-bezbednosnih pretnji.

Ključne reči: vazduhoplovno pravo, izazovi, zakonodavstvo, sajber-bezbednosne pretnje, harmonizacija

ANALYSIS OF THE LEGAL REGULATION OF THE REPUBLIC OF SERBIA ON CIVIL AVIATION AND ITS COMPLIANCE WITH INTERNATIONAL REGULATIONS

Abstract: *Civil aviation is one of the fastest-growing industries and is dependent on rapid technological progress. Rapid technological progress requires a high level of legal regulation and fast adaptation of legal regulations in order to maintain safety and the smooth operation of international air traffic. Aviation law is characterized by a complex set of national legislative frameworks adopted by states, and national legislative frameworks shall be harmonized with each other through the adoption of international legal documents. In Serbia, the national legal framework relating to civil aviation is largely harmonized with the international one, which is important for its European integration. This paper aims to analyze the existing legal regulation relating to aviation legislation in the Republic of Serbia and analyze the degree of harmonization with international regulations. Also, this paper provides recommendations for future development of the civil aviation Law in Serbia.*

Keywords: *aviation law, Serbian aviation law, international law, harmonization*

* Faculty of Law, Megatrend University, Belgrade
E-mail: anikmarkovic@gmail.com

INTRODUCTION

The specific nature of the aviation industry and its international character allow this industry to be viewed primarily through the prism of international law, and then through national legislation. Unlike many other industries, aviation cannot function effectively only within the limits of a state's legal framework. The international dimension of the aviation industry requires the existence of strict rules and standards that go beyond the borders of a single state. For the smooth functioning of global air traffic, the existence of generally accepted international legal rules and international organizations¹, as well as the existence of national regulations, harmonized with international ones, is of essential importance. At the same time, national legislation has a central role when carefully aligned with international standards. This balance allows countries to maintain sovereignty over their airspace while ensuring that their aviation sector represents an integral part of the global system. For Serbia, the alignment of the national legislative with the international one has particular importance. Positioned at the Central part of the Balkan Peninsula, the country is directly on a crossroad of international and regional air routes. As part of its path toward integration into the EU, Serbia has adopted reforms for the harmonization of its aviation legislation with international and EU standards. These reforms also enhance the competitiveness of the domestic aviation sector and establish Serbia's credibility as an equal partner in international aviation. This paper analyses the most significant laws and bylaws of the Republic of Serbia and their degree of compliance with international regulations. Furthermore, potential legal shortcomings and proposals for addressing them are examined.

1. LEGAL REGULATION OF CIVIL AVIATION IN SERBIA

Historically, the Kingdom of Serbia was among the first European countries to establish a legal framework for civil aviation. In 1913, the Kingdom of Serbia adopted the Regulation on Air Traffic. With this regulation, the Republic of Serbia laid the groundwork for civil aviation regulation. For this research, this paper will only analyse the current laws in force in Serbia. The *Air Traffic Law* of the Republic of Serbia² is the main law governing civil aviation in the country. It establishes the basic principles of aviation law. In its introductory part, the law defines key terms

¹ Danilović, N. (2019): "Međunarodne organizacije i njihova uloga subjekata međunarodnog prava", *Megatrend Revija*, 16(2), p. 95-114.

² "The Air Traffic Law of the Republic of Serbia", *Official Gazette of the Republic of Serbia*, No. 73/2010 with amendments and supplements.

with a focus on the concept of airspace and sovereignty.³ This Law shall apply to aircraft while they are on the territory of the Republic of Serbia, except when otherwise provided for by a ratified international agreement.⁴ According to Article 2 of the Law, the rules of the law shall apply to civil aircraft registered in Serbia, while located on the foreign territory, only if it is not contrary to the regulations of the state on whose territory the aircraft is located or to a ratified international agreement. The entry of a foreign aircraft into Serbian airspace without following instructions from air traffic control or contrary to conditions set in the approval of the competent authority or flight plan is considered a violation of Serbian airspace. Also, foreign unmanned aircraft cannot be present in the airspace of the Republic of Serbia without the approval of the Directorate. If the unmanned aircraft is present in the airspace of Serbia without proper permission, that could be considered a violation of the airspace. Additionally, the law covers rules for aircraft registration and mandates the creation of a national register for all registered aircraft. A large part of the law addresses airport and heliport operation, the services provided there, and aims to establish uniform standards for airports in Serbia. It also sets safety standards to protect passengers, cargo, and baggage. The law's next section aligns with international regulations on air traffic safety, outlining measures for cooperation among security agencies in preventing illegal acts, including passenger and baggage control. An important part of the law is the establishment of the State Directorate for Civil Aviation, which supervises operators' activities. The Civil Aviation Directorate of the Republic of Serbia is established as a public agency, founded by the Government of the Republic of Serbia. The Directorate performs state administration tasks entrusted to it by the Law on Air Transport of the Republic of Serbia. Provisions of the Law authorize the directorate to issue permits, conduct inspections, and impose sanctions on legal and natural persons who violate the law.

Another important law, which regulates civil aviation in Serbia, is the *Law on Obligations and Basic Ownership Relations in Air Traffic*.⁵ This law was adopted in 2011 and aims to regulate the obligations and legal relations between entities in air traffic. Part of the law also deals with ownership relations, i.e., it regulates the establishment of ownership over aircraft. The provisions of the law regulate the registration of ownership rights and rights of liens in the appropriate regis-

³ Elenkov, M. P., Beriša, H. A., & Barišić, I. I. (2019): "Challenges of the implementation of the concept of flexible use of airspace in the Republic of Serbia", *Military Technical Courier*, 67(2), 374–402.

⁴ "The Air Traffic Law of the Republic of Serbia", *Official Gazette of the Republic of Serbia*, No. 73/2010 with amendments and supplements.

⁵ "Law on Obligations and Basic Ownership Relations in Air Traffic", *Official Gazette of the Republic of Serbia*, No. 87/2011, 66/2015

ters, as well as the possibility of seizing aircraft to settle claims. A large part of the provisions refer to contracts for the transportation of passengers, luggage, and belongings, aircraft leasing, and concluding contracts for air traffic insurance.⁶ An important contract provided for in the Law on Obligations and Basic Ownership Relations in Air Traffic is the Air Carriage Contract. This contract is later divided into a contract for air transport of goods and a contract for air transport of passengers and luggage. With this contract, the carrier undertakes to transport a passenger or item from the point of departure to the destination at the agreed time, and the customer/passenger to pay the agreed or appropriate fare.⁷ The key participants are distinguished: the customer (concludes a contract with the carrier), the sender (presents the item for transport), the recipient (authorized person to collect the item at the destination), the carrier (has the right to the fare), and the right holder (can assert claims against the carrier). According to the Law⁸, transportation is divided into international and domestic. International transportation requires a special international regime, and stronger state control and special customs regulations apply.

The Law on Investigation of Accidents in air, rail, and water transport was adopted in 2018. It aims to investigate serious accidents in air, rail, and water transport⁹:

- (1) which occurred on the territory of the Republic of Serbia, and are carried out in accordance with the international obligations of the Republic of Serbia,
- (2) that happened to aircraft registered in the Republic of Serbia or managed by a company based in the Republic of Serbia, and that happened outside the territory of the Republic of Serbia, if such an investigation is not conducted by another country,
- (3) regarding which the Republic of Serbia is authorized or, in accordance with international rights and obligations, is able to appoint an authorized representative in order to participate as a country of registration, a country of use, a country of design, a country of production or a country that provides information, facilities or experts at the request of the country conducting the investigation,
- (4) in the case when the Republic of Serbia is enabled to appoint a representative in an investigation led by another state on the basis of a special interest due to deaths and serious physical injuries to its citizens,

⁶ Baltezarević, V. (2017): *Primena pravnih propisa u oblasti civilnog vazduhoplovstva*, Beograd, Univerzitet "John Nesbitt", p.54.

⁷ Ibid.

⁸ "Law on Obligations and Basic Ownership Relations in Air Traffic", *Official Gazette of the Republic of Serbia*, No. 87/2011, 66/2015.

⁹ "Law on Accident Investigations for Aviation, Railways and Waterborne Transport", *Official Gazette of the Republic of Serbia*, No. 66/2015, 83/2018.

- (5) on questions concerning the timely provision of information on all persons and dangerous cargo in an aircraft that has suffered an accident or serious accident, as well as assistance to victims of an aviation accident or serious accident and their relatives;

The main purpose of this law is to conduct an investigation procedure in the event of serious aircraft accidents, in order to ensure the safety of air traffic. The provisions of the Law provide for the establishment of the Accident Investigation Center and determine its competencies. The Law advocates for transparency in the work of the Center by introducing the obligation that all conclusions from the investigations be available to the public. The investigation and the results of the investigation by the Center do not represent a basis for initiating criminal proceedings, but serve as guidelines for preventing the recurrence of such an incident.

In addition to the above-mentioned laws, which are considered the basis of the legal regulation of civil aviation in Serbia, there are also numerous bylaws that regulate the legal matter in more depth.

2. ANALYSIS OF THE DEGREE OF COMPLIANCE OF SERBIAN LEGAL REGULATIONS WITH INTERNATIONAL REGULATIONS

The legislative framework of the Republic of Serbia shows a high degree of compliance with international rules. The Air Traffic Law has incorporated the basic rules of aviation law established by the Chicago Convention, in particular the provisions relating to the regulation of the principle of sovereignty and the protection of air traffic safety. In addition to the rules of the Chicago Convention, the provisions of the Air Traffic Law are in accordance with the standards established by the International Civil Aviation Organization (ICAO). The Law on Obligations and Basic Property Ownership in Air Transport shows compliance of the provisions with the provisions of the Geneva Convention, which relate to the right of ownership and lien rights over aircraft. This law, especially the part relating to insurance and compensation of operators, is aligned with the provisions of the Montreal Convention.¹⁰ The Law on the Investigation of Accidents and Serious Incidents in Air, Rail, and Water Transport has incorporated the best practices and standards recommended by the international organization ICAO regarding the investigation of incidents and aircraft accidents. By establishing the Accident Investigation Center, Serbia demonstrates that air traffic safety is a fundamental

¹⁰ Petrović, G. (2023): "Chapter Serbia", *The Aviation Law Review, Law Business Research*, p. 280–300.

principle and that it fully complies with the regulations established by the international community. In addition to compliance with international regulations, Serbia, as a member of the European Common Aviation Area (ECAA), is obliged to harmonize its own legislation with the European one. The general conclusion is that Serbia demonstrates a high level of compliance of its national legislation with international frameworks. At the same time, Serbia, with the provisions of its national legislation, treats domestic and foreign operators equally in terms of their responsibility in protecting passengers and in the safe conduct of air traffic. Despite the high level of compliance, there are still certain aspects where Serbia should improve. The rapid change in aviation regulation, which is a result of rapid technological progress, requires greater promptness in the implementation of new rules in national legislation. In this sense, cyber threats, the emergence of drones, cyber terrorism, and the promotion of environmental protection are only partially covered in national legislation in Serbia. It is recommended to work on improving this aspect through the adoption of modern legal solutions¹¹, which will position Serbia not only as a passive recipient of norms but as an active member of the international community participating in the establishment of new international legal rules.

3. RECOMMENDATIONS FOR FURTHER DEVELOPMENT OF AVIATION LAW IN SERBIA

The development of aviation law in the Republic of Serbia should be observed from an international legal perspective, as well as from a European Union and regional perspective. The basic and most important recommendation is the harmonization of domestic legislation with the standards and regulations set by the International Civil Aviation Organization. Given that the Republic of Serbia is on the European path, harmonization with the rules of the European Union and the regulations set by the European Aviation Safety Agency is of utmost importance.

Additionally, the Republic of Serbia needs to strengthen the legal framework related to digitalization, technological progress, and cyber threats. The issue regarding cyber threats is regularly discussed internationally, but it seems that cybercriminals are always one step ahead by finding different and creative ways to exceed security measures in order to carry out their criminal activities.¹² Although

¹¹ Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2021): "Cybersecurity challenges in the aviation industry: A review of current and future trends", *Information*, 13(3), Article 146

¹² Baltezarević, I., & Baltezarević, R. (2021): "Sajber bezbednost: izgradnja digitalnog poverenja", *Megatrend revija*, 18(4), p. 269–280.

the risks associated with cyber threats in aviation cannot be eliminated, they can be mitigated by implementing good cybersecurity legislation and good practices.¹³ Furthermore, it is necessary to incorporate legal rules related to the regulation of the use of drones and the protection of passengers' personal data.

Another important aspect is the adoption of strict legal rules regarding the sustainability of aviation and its environmental aspects of aviation. Following the European and global trends, the national legislation should provide a comprehensive legislative framework related to reducing CO2 emissions, fuel consumption, and the types of fuel used. In the following period, it is expected that the states and the airlines will introduce innovative technologies and modern business models to meet environmental protection requirements, which can be taken as an example of the path that should be followed in the future.

Finally, it is necessary to strengthen regional cooperation among the Western Balkan countries in order to exchange best practices and resources. By working together, countries can improve the regulatory framework and work together to reduce harmful gases and achieve competitive and sustainable aviation.

CONCLUSION

The legal regulation in the Republic of Serbia relating to civil aviation shows that Serbia is oriented towards harmonization with international law. Analysis of the basic laws- the Law on Aviation, the Law on Obligations and Basic Ownership Relations in Aviation, and the Law on Investigation of Accidents and Serious Incidents, shows that Serbia has created a comprehensive legal framework, which undoubtedly ensures stable and efficient functioning of the aviation sector. Compliance with international regulations is evident in the legal texts of the Laws. The Republic of Serbia has harmonized its national legislation through the application of the basic principles of the Chicago Convention, the Montreal Convention, the Geneva Convention, as well as the application of the standards of the International Civil Aviation Organization. In order to strengthen its position as a reliable partner of the international community, it is recommended to regularly update the norms in the national legislation and invest in adopting new modern solutions in aviation aspects that are not sufficiently addressed by international law.

¹³ Kožović, D.V., Đurđević, D.Ž. (2019): "Sajber bezbednost u avijaciji", *Megatrend revija*, 16(2), p. 39-56.

LITERATURE

- Baltezarević, I., and Baltezarević, R. (2021): "Sajber bezbednost: izgradnja digitalnog poverenja", *Megatrend revija*, 18(4), p. 269–280.
- Baltezarević, V. (2017): *Primena pravnih propisa u oblasti civilnog vazduhoplovstva*, Beograd, Univerzitet "John Nesbitt".
- Danilović, N. (2019): „Međunarodne organizacije i njihova uloga subjekata međunarodnog prava“, *Megatrend Revija*, 16(2), p. 95-114.
- Elenkov, M. P., Beriša, H. A., and Barišić, I. I. (2019): "Challenges of the implementation of the concept of flexible use of airspace in the Republic of Serbia“, *Military Technical Courier*, 67(2), 374–402.
- Kožović, D.V., Đurđević, D.Ž. (2019): "Sajber bezbednost u avijaciji“, *Megatrend revija*, 16(2), p. 39-56.
- „Law on air traffic“, *Official Gazette of Serbia*, no. 73/10, 57/11, 93/12, 45/15, 66/15 – other laws, 83/18, 9/20 and 62/23.
- „Law on investigation of accidents and serious incidents in air, railway and water transport“, *Official Gazette of Serbia*, no. 66/2015 and 83/2018.
- „Law on Obligations and Basic Property Relations in Air Traffic“, *Official Gazette of Serbia*, no. 87/2011 and 66/2015.
- Petrović, G. (2023): „Chapter Serbia, The Aviation Law Review“, *Law Business Research*, p. 280-300.
- Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., and Bellekens, X. (2021): „Cybersecurity challenges in the aviation industry: A review of current and future trends“, *Information*, 13(3), Article 146.

ANALIZA PRAVNE REGULATIVE REPUBLIKE SRBIJE U OBLASTI CIVILNOG VAZDUHOPLOVSTVA I NJENE USKLAĐENOSTI SA MEĐUNARODNIM PROPISIMA

Sažetak: *Civilno vazduhoplovstvo predstavlja jednu od najbrže rastućih privrednih grana, čiji se razvoj u velikoj meri oslanja na dinamičan tehnološki napredak. Upravo takav napredak nameće potrebu za visokim nivoom pravne regulative i za brzom adaptacijom postojećih pravnih normi, kako bi se obezbedila bezbednost i nesmetano funkcionisanje međunarodnog vazdušnog saobraćaja. Vazduhoplovno pravo odlikuje složen skup nacionalnih zakonodavnih okvira koje države usvajaju, a koji se moraju međusobno usklađivati putem prihvatanja međunarodnih pravnih akata. U Republici Srbiji nacionalni pravni okvir u oblasti civilnog vazduhoplovstva u značajnoj meri je usklađen sa međunarodnim, što je od posebnog značaja u procesu evropskih integracija. Cilj ovog rada jeste analiza postojeće pravne regulative koja se odnosi na vazduhoplovno zakonodavstvo u Republici Srbiji, kao i ocena stepena njene harmonizacije sa međunarodnim propisima. Ovaj rad nudi i preporuke za budući razvoj pravnog okvira u oblasti civilnog vazduhoplovstva u Republici Srbiji.*

Ključne reči: *vazduhoplovno pravo, vazduhoplovno pravo u Srbiji, međunarodno pravo, harmonizacija*

Ivana Baltezarević*
<https://orcid.org/0000-0003-4605-1420>

UDC: 323.23:004.89

Vesna Baltezarević**
<https://orcid.org/0000-0002-8325-6620>

DOI: 10.5937/MegRev2502169B

Radoslav Baltezarević***
<https://orcid.org/0000-0001-7162-3510>

Original scientific paper

Received 14.09.2025.

Approved 16.10.2025.

AI-DRIVEN SOCIAL BOTS IN POLITICAL CAMPAIGNS AND THEIR ROLE IN SHAPING OPINION, MANIPULATION AND MOBILISATION****

Abstract: *Modern political campaigns are increasingly leveraging advanced digital tools, particularly social bots, ingenious automated programmes powered by artificial intelligence (AI) that imitate human behaviour on social media. Their ability to engage with users in real time, spread political messages, and influence public discussions makes them a powerful force in shaping opinions. These bots do more than just push particular political agendas; they can also distort how users perceive issues, create a false sense of widespread support, and deepen divisions among voters. Furthermore, social bots foster selective exposure by encouraging users to interact solely with information that supports their current beliefs, potentially leading to the formation of ideological echo chambers. This paper examines how state-of-the-art language processing and data-driven learning methods allow these bots to be more convincing and less detectable, presenting a significant challenge to democratic systems. It also looks into the role of bots in spreading disinformation and shaping media narratives and highlights specific cases of political manipulation involving bots in both authoritarian and democratic contexts. The conclusion stresses that, given the growing sophistication of these technologies, a comprehensive response is crucial, one that encompasses legislative measures, technological innovations, and user education to protect the integrity of public discourse.*

Keywords: *Social bots, Political campaigns, Public opinion manipulation, Artificial Intelligence.*

* Institute for Political Studies, Belgrade, Republic of Serbia
E-mail: ivana.baltezarevic@ips.ac.rs

** Megatrend University, Belgrade
E-mail: vesnabal@gmail.com

*** Institute of International Politics and Economics, Belgrade, Republic of Serbia
E-mail: radoslav@diplomacy.bg.ac.rs

**** The paper presents findings of a study developed as a part of the research project “Serbia and challenges in international relations in 2025”, financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and conducted by Institute of International Politics and Economics, Belgrade during year 2025.

1. INTRODUCTION

While the development of artificial intelligence (AI) and machine learning (ML) has undoubtedly given us many advantages in modern life, it has also made it much more difficult to think independently about politics. Digital disinformation is becoming more common, and we must be vigilant to make sure we are able to make wise decisions.¹ Artificial intelligence is increasingly being used for purposes that go beyond technical functionality, including psychological influence through automated communication channels.²

While artificial intelligence is being used in military operations to automate drones and robotic systems,³ its application in digital spheres (particularly through social bots) is equally worrying. One of the most important instruments for disseminating political propaganda on social media are bots designed to mimic human appearance and behaviour.⁴ Social bots have several potential uses in political debate, but arguably the most notable is amplification: the capacity to produce and/or extensively disseminate vast volumes of online information to support causes and magnify messages. By encouraging hashtags or “likes,” for instance, social bots can make topics trend, giving the appearance that a person or concept is widely supported (or opposed).⁵ High-level algorithms enable the prediction of data through data extraction and analysis, which can help in making better decisions.⁶

Along with spreading inaccurate or dubious information, it has been proposed that these actions may have the following effects: stifle genuine grassroots or minority interest movements; give fictitious legitimacy to fringe ideas by giving them the appearance of broad support; and perhaps even overload important information channels with spam, noise, and propaganda during public emergencies and

¹ Melanson Ricciardone, S. (2024): *How AI bots spread misinformation online and undermine democratic politics*, <https://theconversation.com/how-ai-bots-spread-misinformation-online-and-undermine-democratic-politics-234915>.

² Pashentsev, E. & Sebekin, S. (2023): “Metaverses, artificial intelligence and challenges to psychological security”, *Politika nacionalne bezbednosti*, 25(2), 33-57. DOI: 10.5937/pnb25-46760

³ Đorić, M. & Glišin, V. (2023): “The use of artificial intelligence in the Russo-Ukrainian war”, *Politika nacionalne bezbednosti*, 25(2), 59-76. DOI: 10.5937/pnb25-47369

⁴ Woolley, S. C. (2020): “Bots and Computational Propaganda: Automation for Communication and Control”, In: J. A. Tucker & N. Persily (Eds.), *Social Media and Democracy* (pp. 89-110), Cambridge University Press.

⁵ Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., Quinn, S. C., & Dredze, M. (2018): “Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate”, *American Journal of Public Health*, 108(10), 1378-1384. DOI: 10.2105/AJPH.2018.304567

⁶ Baltezarević, R. (2023): “Uticaj veštačke inteligencije na globalnu ekonomiju”, *Megatrend revija*, 20(3), 13-24. DOI: 10.5937/MegRev2303013B

crisis events. In all situations, the public interchange of ideas and information is seriously threatened by the possible abuse of modern technologies.⁷

In political communication, selective exposure refers to people's propensity to look for information that supports their pre-existing opinions. Social bots can amplify this behaviour to further polarise public opinion and create ideological echo chambers.⁸ These days, bots can and will pose as real people, make friends with other users, and gradually (over the course of days, weeks, or months) have conversations that are sensitive to each user's feelings, attitudes, and speech patterns in an effort to convert, radicalise, or otherwise sway their vote. Studies have already shown that Large Language Models (LLMs) are more adept than people at uprooting deeply held beliefs.⁹

Different industries are affected by bot traffic in different ways. Malicious bots were responsible for almost half of the online traffic in the telecom and ISP, community and society, and computing and IT sectors. Not all bot traffic, however, is perceived negatively. Some of these programmes aid consumers in their internet search by monitoring website performance or indexing websites for search engines.¹⁰ The modern social bot is a notable technological feat since it can now influence public opinion, spread information, and blend in with human crowds on social networking sites to bypass human detection.¹¹

However, social bots need to be trained on large datasets in order to function well and fulfil their intended function. By analysing annotated data, such as linguistic patterns, user interaction sequences, sentiment signals, and topical relevancy, these bots are trained to imitate human behaviour. Both supervised learning with labelled examples and reinforcement learning, in which bots get better over time depending on feedback loops, are used in training. A social bot is significantly more credible and persuasive when it has access to more varied and high-quality data.¹²

⁷ Woolley, S. C. (2016): "Automating power: Social bot interference in global politics", *First Monday*, 21(4). DOI: 10.5210/fm.v21i4.6161

⁸ Baltezarević, R. & Baltezarević, I. (2022): "Selective exposure in political communication", *Megatrend revija*, 19(3), 303-315 DOI: 10.5937/MegRev2203303B

⁹ Salvi, F., Ribeiro, M. H., Gallotti, R., & West, R. (2024): "On the conversational persuasiveness of large language models: A randomized controlled trial", *arXiv preprint*, arXiv:2403.14380.

¹⁰ Bianchi, T. (2025): *Global share of human and bot web traffic 2013-2024*, <https://www.statista.com/statistics/1264226/human-and-bot-web-traffic-share/>.

¹¹ Salge, C. A. de L., Karahanna, E., & Thatcher, J. B. (2022): "Algorithmic Processes of Social Alertness and Social Transmission: How Bots Disseminate Information on Twitter", *MIS Quarterly*, 46(1). DOI: 10.25300/MISQ/2021/15598

¹² LXT (2025): *Social Bots*, <https://www.lxt.ai/ai-glossary/social-bots/>.

2. LITERATURE REVIEW

While some social bots are simple, others may imitate human behaviour and respond to users instantly. Here are some examples of bot types: a) Chatbots: These bots, which can be found on messaging applications, social media sites, and websites, provide customer support, answer queries, and carry-on discussions. b) Web crawlers (spiders): Are bots that collect information from websites, primarily to assist search engines in indexing content. c) Shopping bots: These assist customers in keeping tabs on costs, verifying inventory, and obtaining limited-edition goods. d) Gaming Bots: In games, bots frequently take the place of actual players to assist users with practice or multiplayer gameplay. e) Malicious Bots: Created with malicious purpose, these bots propagate spam, steal information, or initiate DDoS assaults. Lastly, e) Social Media Bots: These automate actions like liking, commenting, and following. While some are used for spam or fake popularity, others assist in account management.¹³

Social bots are generally understood to be automated, algorithm-driven agents that may function and communicate on social networking sites in an anonymous manner. They are made to collect data online in order to generate social media activity and profiles that resemble those of people.¹⁴ In wider terms, a social bot can be thought of as a super-ordinate concept that encapsulates several kinds of (semi-)automatic agents. Through one- or many-sided contact in online media, these agents are made to accomplish a given goal.¹⁵

Journalists, activists, and political opponents can all be harassed by bots. Bots will only become more and more popular as instruments for disseminating political propaganda on social media because of the extra layer of anonymity they offer and their capacity to scale online communication. Political bots can now more easily learn from their surroundings and apply what they discover in their interactions as well as other subjects thanks to advancements in artificial intelligence (AI), which makes them more difficult to identify.¹⁶

With the aim of engaging in phishing activities or influencing the measurement of important metrics associated with phenomena like usage, interest, and

¹³ Oestreicher, G. (2025): *Social Media Bots: The Good and The Bad*, <https://metricool.com/social-media-bots/>.

¹⁴ Howard, P.N., Woolley, S. & Calo, R. (2018): "Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration", *Journal of Information Technology & Politics*, 15(2), 81–93. DOI: 10.1080/19331681.2018.1448735

¹⁵ Grimme, C., Preuss, M., Adam, L., & Trautmann, H. (2017): "Social bots: Human-like by means of human control?", *Big Data*, 5(4), 279–293.

¹⁶ Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016): "The rise of social bots", *Communications of the ACM*, 59(7), 96–104. DOI: 10.1145/2818717

popularity, these tools are increasingly being used to both create and disseminate information within social networks. In addition to functioning only within social networks, current iterations of social bots are notable for their capacity to imitate human behaviour, such as patterns and language, while evading detection.¹⁷

Numerous academics and observers have identified the possibility that social bots could skew public sentiment measurements, which are crucial for responsive governments, as a serious danger to the efficient operation of democracy.¹⁸ However, new social bots that employ AI to create their posts can look like the poster next door, whereas early social bots could be easily identified by their posting history, which would demonstrate the limited range of their content. When built with the goal of influencing a particular human audience, “sleeper social bots” can converse with individuals in real time while imitating the human users they are intended to represent. During the Cold War, the idea of the “sleeper agent” gained popularity as a result of fears of Communist infiltration and the subversive agent who may pose as a patriot. A sleeper spy remained “asleep” until the time came to take action, be it stealing confidential data or committing a horrible crime.¹⁹ An algorithm that basically describes their behaviour and online activities is offered to social bots, along with a technical basis that allows them to create a profile and interact and connect with the platform’s API (Application Programming Interface). These operations can differ in their ultimate goal and intelligence level.²⁰

In a variety of political events and regimes, bots have been observed to be active. China and Russia are examples of authoritarian regimes that have used them against both their own and other nations’ citizens. Bot design and administration can be sponsored and supported by a variety of interest groups in democratic systems, including lobbyists, political actors, and other agents with political affiliations.²¹

Due to changes in the social media ecosystem and a decline in support for academic research, studying social bots has recently become much more challenging. Since most social bot research uses data from Twitter (now X), the future is unclear because the companies have altered its price policy, making it unaffordable for

¹⁷ Crothers, B. (2019): “Internet bots are getting better at imitating humans”, *New York Post*, <https://nypost.com/2019/04/22/internet-bots-are-getting-better-at-imitating-humans/>.

¹⁸ Stella, M., Ferrara, E., & Domenico, M. D. (2018): “Bots increase exposure to negative and inflammatory content in online social systems”, in *Proceedings of the National Academy of Sciences*, 115(49), 12435–12440. DOI: 10.1073/pnas.1803470115

¹⁹ Ossa, V. (2022): “Fiction, 9/11, and the Sleeper Agent”, In V. Ossa: *The Sleeper Agent in Post-9/11 Media* (pp. 9–78), Springer International Publishing. DOI: 10.1007/978-3-031-11516-5_2

²⁰ Assenmacher, D., Clever, L., Frischlich, L., Quandt, T., Trautmann, H. & Grimme, C. (2020): “Demystifying Social Bots: On the Intelligence of Automated Social Media Actors”, *Social Media + Society*, 6(3), 205630512093926. DOI: 10.1177/2056305120939264.

²¹ Woolley, S., & Howard, P. (2017): “Computational propaganda worldwide: Executive summary”, *Computational Propaganda Project*.

academic users to access its API (Application Programming Interface).²² Approximately 23 million social bots use Twitter (now X), making up 8.5% of all users.²³ Furthermore, social bots are responsible for more than two-thirds of tweets. A Pew study examined 1.2 million tweets in English over a 47-day period. The results showed that 66% of the tweets were likely the result of suspected bots.²⁴ The current state of social bot intelligence, or their ability to generate content, is often unclear; this is because bots are hard to detect. The research states that disseminating pre-made posts, sharing already-written pieces, or looking for information to share online are ways to emulate human behaviour.²⁵

According to Melanson Ricciardone, bot tweets and human tweets shared 75% similarity on March 14, 2019, and by March 28, that percentage had risen to 92%. The similarity persisted even when the frequency of emotive terms in human tweets declined over time. This demonstrates the strong resemblance between content produced by bots and humans. Since machine learning and generative AI technologies are meant to mimic human conduct, sometimes bots just mimic human behaviour.²⁶

In order to more closely resemble human behaviour, some of them even have artificial sleep-wake cycles. Even though they are designed to function alone, they can have a lot of power when combined. Indeed, it is believed that social bots influenced the 2016 Brexit vote and even the US presidential election. It's critical to comprehend how these bots function in our digital ecosystem, particularly when creating AI models that can distinguish between information produced by bots and human content. A step towards developing more precise and dependable AI applications is to improve these models using machine learning datasets.

According to a recent BBC news report, Reform UK's polling has increased as a result of many posts that may have been created by malevolent bots. The BBC made the decision to investigate this further and contacted the individuals behind accounts that were obviously attempting to inflate the popularity of Reform UK.

²² Kupferschmidt, K. (2023): *Twitter's plan to cut off free data access evokes 'fair amount of panic' among scientists*, <https://www.science.org/content/article/twitters-plan-cut-free-data-access-evokes-fair-amount-panic-among-scientists>.

²³ De Lima Salge, C. A., and N. Berente (2017): "Is that social bot behaving unethically?", *Communications of the ACM*, 60(9), 29-31.

²⁴ Pew Research Center (2018): *Q&A: How Pew Research Center identified bots on Twitter*, <https://www.pewresearch.org/fact-tank/2018/04/19/qa-how-pew-research-center-identified-bots-on-twitter>.

²⁵ Appling, S., & Briscoe, E. (2017): "The perception of social bots by human and machine", In: V. M. Z. Rus (Ed.): *FLAIRS 2017—Proceedings of the 30th International Florida Artificial Intelligence Research Society Conference* (pp. 20-25), Association for the Advancement of Artificial Intelligence.

²⁶ Melanson Ricciardone, S. (2024): *How AI bots spread misinformation online and undermine democratic politics*, <https://theconversation.com/how-ai-bots-spread-misinformation-online-and-undermine-democratic-politics-234915>.

The inquiry came to the conclusion that many of these accounts were fraudulent in response to worries about foreign meddling in past elections. They have made use of networks of what users refer to as “bots” or “troll farms,” and social media companies label “inauthentic accounts.”²⁷

The researchers came to the conclusion that none of the social media sites they examined offered enough security and oversight to shield users from malevolent bot behaviour. It is maintained that in order to safeguard the public from malevolent bots, legislation, financial incentive programmes, user education, and technology advancements are required.²⁸ In any event, a variety of factors influence how well social bots communicate and manipulate politics. Bots spread political messages (propaganda or fake news) in large quantities, giving the impression that a particular idea is more widely accepted than it actually is. This undoubtedly makes the message more visible and may persuade users that it is factual or pertinent. It follows logically that a large number of social bots supporting a particular political narrative can give the impression that the public has already made up its mind, which shapes public opinion. The volume of interactions generated by bots can compel the media to focus on a certain subject. Parties and politicians occasionally respond to these popular subjects, which frequently elicit intense emotional responses, without realising that they are bot campaigns.

Disseminating false information online can have extremely harmful effects. There are numerous real-world instances where the propagation of false information sparked street riots and violent incidents that even resulted in fatalities.²⁹

3. CONCLUSION

The growing role of social bots in political campaigns is turning into a significant challenge for maintaining transparency, honesty, and respect in discussions. These bots can effortlessly mimic human behaviour, quickly spread political messages, and sway public opinion on different issues, making them a powerful tool in the realm of digital propaganda. It's really troubling how they manage to create a misleading sense of agreement. This just exacerbates the divisions and silences the true voices that deserve to be heard in our online community.

²⁷ Daley, S. (2024): *Information Warfare: Political Bots on Social Media*, <https://www.complycube.com/en/information-warfare-political-bots-on-social-media/>.

²⁸ Techxplore (2024): *AI bots easily bypass some social media safeguards, study reveals*, <https://techxplore.com/news/2024-10-ai-bots-easily-bypass-social.html>.

²⁹ Baltezarević, R., Baltezarević, I. & Ravić, N. (2023): “Confirmation bias in digital communication: the tendency of consumers to favor information that confirms their pre-existing beliefs”, *Megatrend revija*, 20(2), 25–35. DOI: 10.5937/MegRev2302026B

The progress we've achieved in artificial intelligence (AI) and machine learning (ML) has given rise to bots that are growing more complex, making them more difficult to detect. They're getting really good at swaying users' emotions and opinions. While they used to be easily recognised due to their repetitive and simplistic nature, today's bots can engage in personalised chats, respond in real time, and truly impact people's political perspectives.

The existence of social bots in both authoritarian and democratic environments, coupled with their potential to impact political events like elections and referendums, emphasises the critical need for a well-rounded response. This should involve implementing stricter regulations, creating advanced detection tools for bots, and raising awareness among users about the risks these entities present to democracy and society in general.

With the gap between reality and the virtual world becoming less clear, it's vital to ensure our digital public spaces are secure. To effectively address the misuse of social bots and preserve the core values of democracy, we need a collective approach that brings together governments, tech firms, researchers, and the public.

LITERATURE

- Appling, S., & Briscoe, E. (2017): "The perception of social bots by human and machine", In: V. M. Z. Rus (Ed.), *FLAIRS 2017— Proceedings of the 30th International Florida Artificial Intelligence Research Society Conference* (pp. 20-25), Association for the Advancement of Artificial Intelligence.
- Assenmacher, D., Clever, L., Frischlich, L., Quandt, T., Trautmann, H. & Grimme, C. (2020): "Demystifying Social Bots: On the Intelligence of Automated Social Media Actors", *Social Media + Society*, 6(3), 205630512093926. DOI: 10.1177/2056305120939264.
- Baltezarević, R. & Baltezarević, I. (2022): "Selective exposure in political communication", *Megatrend revija*, 19(3), 303-315. DOI: 10.5937/MegRev2203303B
- Baltezarević, R. (2023): "Uticaj veštačke inteligencije na globalnu ekonomiju", *Megatrend revija*, 20(3), 13-24. DOI: 10.5937/MegRev2303013B
- Baltezarević, R., Baltezarević, I. & Ravić, N. (2023): „Confirmation bias in digital communication: The tendency of consumers to favor information that confirms their pre-existing beliefs“, *Megatrend revija*, 20(2), 25-35. DOI: 10.5937/MegRev2302026B
- Bianchi, T. (2025): *Global share of human and bot web traffic 2013-2024*, <https://www.statista.com/statistics/1264226/human-and-bot-web-traffic-share/>.

- Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., Quinn, S. C., & Dredze, M. (2018): "Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate", *American Journal of Public Health*, 108(10), 1378–1384. DOI: 10.2105/AJPH.2018.304567
- Crothers, B. (2019): "Internet bots are getting better at imitating humans", *New York Post*, <https://nypost.com/2019/04/22/internet-bots-are-getting-better-at-imitating-humans/>.
- Daley, S. (2024): *Information Warfare: Political Bots on Social Media*, <https://www.complycube.com/en/information-warfare-political-bots-on-social-media/>.
- De Lima Salge, C. A., and N. Berente (2017): "Is that social bot behaving unethically?", *Communications of the ACM*, 60(9), 29–31.
- Đorić, M. & Glišin, V. (2023): "The use of artificial intelligence in the Russo-Ukrainian war", *Politika nacionalne bezbednosti*, 25(2), 59–76. DOI: 10.5937/pnb25-47369
- Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016): "The rise of social bots" *Communications of the ACM*, 59(7), 96–104. DOI: 10.1145/2818717
- Grimme, C., Preuss, M., Adam, L., & Trautmann, H. (2017): "Social bots: Human-like by means of human control?", *Big Data*, 5(4), 279–293.
- Howard, P.N., Woolley, S. & Calo, R. (2018): "Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration", *Journal of Information Technology & Politics*, 15(2), 81–93. DOI: 10.1080/19331681.2018.1448735.
- Kupferschmidt, K. (2023). *Twitter's plan to cut off free data access evokes 'fair amount of panic' among scientists*, <https://www.science.org/content/article/twitters-plan-cut-free-data-access-evokes-fair-amount-panic-among-scientists>.
- LXT (2025): *Social Bots*, <https://www.lxt.ai/ai-glossary/social-bots/>.
- Melanson Ricciardone, S. (2024): *How AI bots spread misinformation online and undermine democratic politics*, <https://theconversation.com/how-ai-bots-spread-misinformation-online-and-undermine-democratic-politics-234915>.
- Oestreicher, G. (2025): *Social Media Bots: The Good and The Bad*, <https://metri-cool.com/social-media-bots/>.
- Ossa, V. (2022): "Fiction, 9/11, and the Sleeper Agent", In: V. Ossa: *The Sleeper Agent in Post-9/11 Media* (pp. 9–78), Springer International Publishing. DOI: 10.1007/978-3-031-11516-5_2
- Pashentsev, E. & Sebekin, S. (2023): "Metaverses, artificial intelligence and challenges to psychological security", *Politika nacionalne bezbednosti*, 25(2), 33–57. DOI: 10.5937/pnb25-46760
- Pew Research Center (2018): "Q&A: How Pew Research Center identified bots on Twitter", <https://www.pewresearch.org/fact-tank/2018/04/19/qa-how-pew-research-center-identified-bots-on-twitter>.

- Salge, C. A. de L., Karahanna, E., & Thatcher, J. B. (2022): “Algorithmic Processes of Social Alertness and Social Transmission: How Bots Disseminate Information on Twitter”, *MIS Quarterly*, 46(1). DOI: DOI: 10.25300/MISQ/2021/15598
- Salvi, F., Ribeiro, M. H., Gallotti, R., & West, R. (2024): “On the conversational persuasiveness of large language models: A randomized controlled trial”, *arXiv preprint*, arXiv:2403.14380.
- Stella, M., Ferrara, E., & Domenico, M. D. (2018): “Bots increase exposure to negative and inflammatory content in online social systems”, in *Proceedings of the National Academy of Sciences*, 115(49), 12435–12440. DOI: 10.1073/pnas.1803470115
- Techxplore (2024): *AI bots easily bypass some social media safeguards, study reveals*, <https://techxplore.com/news/2024-10-ai-bots-easily-bypass-social.html>.
- Woolley, S. C. (2016): “Automating power: Social bot interference in global politics”, *First Monday*, 21(4). DOI: 10.5210/fm.v21i4.6161
- Woolley, S. C. (2020): “Bots and Computational Propaganda: Automation for Communication and Control”, In: J. A. Tucker & N. Persily (Eds.): *Social Media and Democracy* (pp. 89–110), Cambridge University Press.
- Woolley, S., & Howard, P. (2017): “Computational propaganda worldwide: Executive summary”, *Computational Propaganda Project*.

DRUŠTVENI BOTOVI VOĐENI VEŠTAČKOM INTELIGENCIJOM U POLITIČKIM KAMPANJAMA I NJIHOVA ULOGA U OBLIKOVANJU MIŠLJENJA, MANIPULACIJI I MOBILIZACIJI

Sažetak: *Moderne političke kampanje sve više koriste napredne digitalne alate, posebno društvene botove, genijalne automatizovane programe pokretane veštačkom inteligencijom (VI) koji imitiraju ljudsko ponašanje na društvenim mrežama. Njihova sposobnost da komuniciraju sa korisnicima u realnom vremenu, šire političke poruke i utiču na javne diskusije čini ih moćnom silom u oblikovanju mišljenja. Ovi botovi rade više od pukog promovisanja određenih političkih agendi; oni takođe mogu da iskrive način na koji korisnici doživljavaju probleme, stvore lažni osećaj široke podrške i prodube podele među biračima. Štaviše, društveni botovi podstiču selektivnu izloženost podstičući korisnike da interaguju isključivo sa informacijama koje podržavaju njihova trenutna uverenja, što potencijalno dovodi do formiranja ideoloških eho komora. Ovaj rad ispituje kako najsavremenije metode obrade jezika i učenja zasnovane na podacima omogućavaju ovim botovima da budu ubedljiviji i manje uočljivi, predstavljajući značajan izazov za demokratske sisteme. Takođe se ispituje uloga botova u širenju dezinformacija i oblikovanju medijskih narativa i ističu konkretni slučajevi političke manipulacije u kojima su uključeni botovi, kako u autoritarnom tako i u demokratskom kontekstu. U zaključku se naglašava da je, s obzirom na rastuću sofisticiranost ovih tehnologija, ključan sveobuhvatan odgovor, koji obuhvata zakonodavne mere, tehnološke inovacije i edukaciju korisnika kako bi se zaštitio integritet javnog diskursa.*

Ključne reči: Društveni botovi, Političke kampanje, Manipulacija javnim mnjenjem, Veštačka inteligencija

Danilo Izgarević*
<https://orcid.org/0009-0000-0785-3055>

Mirjana Ristić**
<https://orcid.org/0009-0001-3877-0153>

Marko Stanojević***
<https://orcid.org/0009-0007-7241-5503>

UDC: 343.983:004
343.3/7::004

DOI: 10.5937/MegRev2502181I

Original scientific paper

Received 06.07.2025.

Approved 07.10.2025.

DARK WEB FORENSICS, INFORMATION SECURITY, AND THE INVESTIGATION OF ILLICIT DIGITAL FOOTPRINTS

Abstract: *The dark web is like a secretive nook of the Internet, tucked away from the usual search engines and only reachable through specialized networks like Tor or I2P. In this murky realm, privacy and encryption serve a dual purpose, facilitating both legitimate communications that prioritize privacy and a variety of illegal activities, including drug and weapon trafficking, financial scams, data breaches, and cyber exploitation. The dark web presents a unique set of challenges due to its complex nature and anonymity, making life tough for digital investigators. They need to navigate through encrypted systems, deal with unpredictable data, and tackle complex international laws. This paper takes a closer look at dark web forensics, revealing how investigators can identify, extract, and preserve digital evidence in this secretive space. This highlights the importance of open-source intelligence, blockchain analysis, machine learning, and network forensics as essential tools for uncovering criminal activities and tracking illegal digital footprints. Furthermore, the study addresses the ethical and legal challenges of infiltration, surveillance, and evidence gathering in anonymous networks, stressing the importance of maintaining procedural integrity and respecting privacy rights. The paper wraps up by recommending strategic approaches to enhance international collaboration, facilitate better data sharing, and establish uniform forensic protocols to effectively combat cybercrime linked to the dark web.*

Keywords: Dark Web Forensics, Information Security, Cybercrime, Digital Footprints, Online Anonymity

* E-mail: daniloizgarevic@gmail.com

** E-mail: ristic85@yahoo.com

*** E-mail: stanojevic.marko799@gmail.com

INTRODUCTION

The dark web, which represents the hidden and anonymized sections of the Internet, has become a vital frontier for illegal digital activities, posing a significant challenge for forensic investigations. As a part of the larger deep web, the dark web is accessed through specialized networks like Tor and I2P, utilizing encryption technologies that intentionally hide user identities, network paths, and infrastructure details.¹ In this obscure world, cybercriminals engage in a range of unlawful activities, including drug and weapon trafficking, financial fraud, ransomware deployment, and the sale of stolen data. They exploit the anonymity available on the network, all while leaving behind a trail of complex digital footprints.²

Forensic practitioners are up against a unique set of challenges when they investigate these environments. The volatile nature of dark-web sessions, the encryption of traffic, the temporary platforms, and the global nature of hosting infrastructure all create a landscape where traditional digital-forensic workflows may not suffice.³ Navigating the digital footprints in this area is no easy feat, primarily because of anonymizing services, cryptocurrency transactions, and the ever-shifting strategies employed by threat actors.⁴ As hidden services evolve and move away from traditional indexing and forensic visibility, the techniques for discovering, preserving, analyzing, and correlating evidence require specialized frameworks and advanced technical methods.⁵

Lately, the dark web has become a hotbed for illicit activities, with its scale, sophistication, and impact on society growing at an alarming rate. Reports show that millions of compromised data records, everything from personal information to corporate credentials are regularly bought and sold on dark-web marketplaces. This highlights not only the vastness of these ecosystems but also the huge digital footprints they leave behind.⁶

¹ Gupta, A., Maynard, S. B., & Ahmad, A. (2021): “*The dark web phenomenon: A review and research agenda*”, *arXiv preprint*, arXiv:2107.04490, <https://arxiv.org/abs/2107.04490>.

² Brinson, R., Wimmer, H., & Chen, L. (2022): “*Dark web forensics: An investigation of tracking dark web activity with digital forensics*”, In: *Interdisciplinary Research in Technology and Management (IRTM) Conference Proceedings*, IEEE. DOI: 10.1109/IRTM54583.2022.9791646

³ Ibid

⁴ Vaghela, H., Varshney, N., & Jain, R. (2025): “*Leveraging AI and ML to innovate forensic frameworks for the identification of illicit operations and extraction of digital artifacts within deep web and dark web environments*”, *Journal of Digital Security and Forensics*, 2(1), 20–35. DOI: 10.29121/DigiSecForensics.v2.i1.2025.43

⁵ Ruiz Ródenas, J. M., Pastor-Galindo, J., & Gómez Mármol, F. (2024): “*A general and modular framework for dark web analysis*”, *Cluster Computing*, 27, 4687–4703. DOI: 10.1007/s10586-023-04189-2

⁶ de-Marcos, L., Medina-Merodio, J. A., & Štapić, Z. (2025): “*Methodologies for data collection and analysis of dark web forum content: A systematic literature review*”,

The enormous and fragmented nature of this data complicates forensic investigations, making it essential to swiftly acquire, correlate, and contextualize various artifacts to reconstruct user behavior and pinpoint accountability.⁷

There's been a noticeable shift in research towards creating advanced methodological frameworks that combine artificial intelligence (AI), machine learning (ML), and modular system architectures, specifically tailored for investigating the dark web.⁸ Additionally, AI-driven models have shown encouraging results in identifying illicit communication patterns and classifying hidden-service content.⁹ These innovations empower practitioners to convert fragmented and anonymized evidence into structured intelligence. Nevertheless, a major challenge remains: bridging the gap between these cutting-edge analytical tools and legally admissible forensic workflows, particularly regarding evidential integrity, cross-jurisdictional collaboration, and ethical considerations.¹⁰

The purpose of this review is to offer a detailed overview of dark-web forensics and the investigation of illegal digital footprints. It will explore the architecture and threat landscape of the dark web, discuss forensic techniques and technological innovations such as traffic classification, blockchain analytics, and AI-based evidence correlation, and examine the ethical and legal issues that are crucial to dark-web investigations. Through a careful examination of existing literature and the identification of significant research gaps, this paper aims to further both the academic field and practical uses of forensic science in the dark web.

Electronics, 14(21), 4191. DOI: 10.3390/electronics14214191

⁷ Brinson, R., Wimmer, H., & Chen, L. (2022): "Dark web forensics: An investigation of tracking dark web activity with digital forensics", In: *Interdisciplinary Research in Technology and Management (IRTM) Conference Proceedings*, IEEE. DOI: 10.1109/IRTM54583.2022.9791646

⁸ Ruiz Ródenas, J. M., Pastor-Galindo, J., & Gómez Mármol, F. (2024): "A general and modular framework for dark web analysis", *Cluster Computing*, 27, 4687–4703. DOI: 10.1007/s10586-023-04189-2

⁹ Vaghela, H., Varshney, N., & Jain, R. (2025): "Leveraging AI and ML to innovate forensic frameworks for the identification of illicit operations and extraction of digital artifacts within deep web and dark web environments", *Journal of Digital Security and Forensics*, 2(1), 20–35. DOI: 10.29121/DigiSecForensics.v2.i1.2025.43

¹⁰ Gupta, A., Maynard, S. B., & Ahmad, A. (2021): "The dark web phenomenon: A review and research agenda", *arXiv preprint*, arXiv:2107.04490, <https://arxiv.org/abs/2107.04490>.

FOUNDATIONS AND LITERATURE REVIEW

As digital technologies continue to evolve, they are redefining the fabric of our electronic society.¹¹ This shift influences not just the legitimate interactions we have online but also the tactics used for conducting and tracing illegal activities. Getting a handle on how users behave in digital environments, particularly those who are tech-savvy, is crucial for forensic investigations.¹² These technologically adept individuals often take advantage of new tools and platforms, like anonymizing networks, cryptocurrencies, and decentralized marketplaces, for both lawful and unlawful activities. By analyzing these behavioral trends, investigators can better predict risks, identify digital traces, and track down illegal activities on the dark web.

When gathering evidence for criminal investigations, law enforcement relies heavily on forensic science. The prosecution of criminals is supported by this evidence, which may establish guilt or innocence. When law enforcement is attempting to ascertain if someone is guilty, forensic investigation is essential. New tools and chances to assist law enforcement in their digital investigations have emerged as a result of technology advancements. The goal of digital forensics is to “collect, examine, analyse, and report” evidence using a variety of tools.¹³

Due to a number of current technologies, including encryption, which offer more anonymity to avoid discovery by law authorities, criminals are depending more and more on the dark web. Law enforcement personnel must be well-versed in the dark web’s operations. They should be able to recognise the crime, link the evidence to it, obtain, gather, and store the evidence while upholding a correct chain of custody, and then present the evidence in court. Artefacts such as cryptocurrency wallets, encryption keys, virtual private networks (VPNs), and dark web addresses must be recognised by investigators. They should also be able to piece together the digital evidence jigsaw and recognise how goods and services are supplied. Digital evidence should be collected using the proper digital forensic procedures

¹¹ Safieddine, F., & Baltezarević, R. (2016): “*Advances in technologies evolving new dimensions in e-society*”, In: V. Baltezarević, R. Baltezarević, & B. Baltezarević (Eds.): *The Internet as a tool of modern business and communication* (pp. 43-75), Lap Lambert Academic Publishing Saarbrücken – Germany.

¹² Kwiatek, P., Papakonstantinidis, S., & Baltezarević, R. (2021): “*Digital Masters’ Entrepreneurial Mindset: A Comparative Study in Emerging Market*”, U S. Rezaei, J. Li, S. Ashourizadeh, V. Ramadani i S. Gërguri-Rashiti (Ur.): *The Emerald Handbook of Women and Entrepreneurship in Developing Economies* (str. 295-315), Emerald Publishing Ltd.

¹³ Brinson, R., Wimmer, H., & Chen, L. (2022): “*Dark web forensics: An investigation of tracking dark web activity with digital forensics*”, In: *Interdisciplinary Research in Technology and Management (IRTM) Conference Proceedings*, IEEE. DOI: 10.1109/IRTM54583.2022.9791646

to minimise unintentional data change; investigators must be educated to do live forensics in order to collect data before suspects turn off their devices.¹⁴

As previously mentioned, Tor and I2P are two well-known anonymity networks that facilitate more secure and private online communication. By directing traffic across a number of servers run by volunteers, both networks conceal the user's IP address and offer some anonymity. However, their functionality, implementation, and design vary greatly. Tor uses a global network of volunteer computers called relays or routers to route internet traffic.¹⁵ Every user's data is encrypted several times, with a network node representing each encryption layer. The procedure is known as "onion routing" because this arrangement resembles the layers of an onion. Tor makes use of a number of directory servers that offer a list of relays together with their current statuses. These servers aid in creating a route through the network that stays clear of unreliable or non-operational nodes, maintaining the network's efficiency and integrity.¹⁶

I2P does not rely on centralised directory servers and is completely autonomous, in contrast to Tor. I2P creates a peer-to-peer distributed network using a decentralised strategy to improve privacy and prevent any one point of failure. As a client and a server, each node performs two functions.¹⁷ Beyond Tor's onion routing, I2P uses garlic routing, which bundles several messages together to improve anonymity. In I2P, messages go via unidirectional tunnels, which have distinct inbound and outward routes. While the outbound tunnel is used for sending communications, the incoming tunnel is utilised for receiving them. To further safeguard user anonymity, tunnels are periodically redistributed at random.¹⁸

Malware, ransomware, phishing kits, botnets, exploit kits, remote access Trojans, keyloggers, password stealers, spyware, and advanced persistent threats (APTs) are just a few of the numerous tools that cybercriminals employ. They usually use sophisticated social engineering techniques to obtain unauthorised access by taking advantage of software flaws and zero-day vulnerabilities. To conceal their identities and locations,

¹⁴ UN (2025): *Darknet investigations*, <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/darknet.html> (01.11.2025).

¹⁵ AlSabah, M., & Goldberg, I. (2016): "Performance and security improvements for Tor: A survey", *ACM Computing Surveys*, 49(2), Article 32. DOI: 10.1145/2946802

¹⁶ McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008): "*Shining light in dark places: Understanding the Tor network*", In: N. Borisov & I. Goldberg (Eds.): *Privacy Enhancing Technologies – 8th International Symposium, PETS 2008, Leuven, Belgium, July 23-25, 2008, Proceedings* (Vol. 5134, pp. 63-76), Springer. DOI: 10.1007/978-3-540-70630-4_5

¹⁷ Yin, H., & He, Y. (2019, March 15–16): "*I2P anonymous traffic detection and identification*", In *Proceedings of the 5th International Conference on Advanced Computing & Communication Systems (ICACCS 2019), Coimbatore, India* (pp. 157–162), IEEE. DOI: 10.1109/ICACCS.2019.8728517

¹⁸ Magán-Carrión, R., Abellán-Galera, A., Maciá-Fernández, G., & García-Teodoro, P. (2021): "*Unveiling the I2P web structure: A connectivity analysis*", *Computer Networks*, 194, 108158. DOI: 10.1016/j.comnet.2021.108158

cybercriminals also regularly use anonymising tools like VPNs and proxies. The dark web's underground marketplaces facilitate cybercrime by giving users access to hacking tools, services, and credentials that have been stolen. Because of the highly targeted, elusive, and destructive nature of cyberattacks caused by this combination of technological know-how and purposeful deception, forensic tools and techniques must constantly evolve in order to successfully respond to and mitigate these threats.¹⁹

With the rise of more advanced dark web marketplaces and hidden services, we really need to step up our game with forensic techniques to pinpoint and link digital evidence. Network traffic analysis, particularly when used alongside machine learning algorithms, has proven to be an essential tool for uncovering patterns that point to illegal activities. Traffic classification models can differentiate between normal and suspicious behavior, even in encrypted settings, which helps investigators uncover hidden communications and link them to potential threat actors.²⁰ These approaches enhance traditional digital forensics, enabling a more proactive strategy in anticipating and combating cybercrime.

Investigating the dark web has made blockchain analysis a key player in uncovering the truth. As cryptocurrencies are often involved in illegal dealings on secretive marketplaces, tracing the movement of these digital assets can bring to light financial trails that would otherwise be kept under wraps. Investigators use techniques like clustering, transaction graph analysis, and heuristic methods to pinpoint suspicious wallets and connect them to illegal activities. This method not only aids in financial investigations but also provides crucial insights into the broader organized cybercriminal networks.²¹

New research is showcasing the exciting blend of artificial intelligence and automated reasoning within digital forensics workflows. AI-powered tools, like natural language processing for scraping dark web forums and supervised learning for classifying threats, are becoming essential for sifting through massive amounts of diverse data. These methods significantly boost investigators' capabilities to spot hidden communications, categorize criminal content, and foresee potential threats before they spiral out of control.²² Using AI can really take a load off the manual tasks and boost the

¹⁹ Akshat, & Chitra B. T. (2025): "Digital forensics and cybercrime investigation: An extensive exploration into the digital frontier", *International Journal of Creative Research Thoughts (IJCRT)*, 13(6), 796–807. ISSN 2320-2882.

²⁰ AlSabah, M., & Goldberg, I. (2016): "Performance and security improvements for Tor: A survey", *ACM Computing Surveys*, 49(2), Article 32. DOI: 10.1145/2946802

²¹ Brinson, R., Wimmer, H., & Chen, L. (2022): "Dark web forensics: An investigation of tracking dark web activity with digital forensics", In: *Interdisciplinary Research in Technology and Management (IRTM) Conference Proceedings*, IEEE. DOI: 10.1109/IRTM54583.2022.9791646

²² Magán-Carrión, R., Abellán-Galera, A., Maciá-Fernández, G., & García-Teodoro, P. (2021): "Unveiling the I2P web structure: A connectivity analysis", *Computer Networks*, 194, 108158. DOI: 10.1016/j.comnet.2021.108158

accuracy and consistency of forensic analyses, which is crucial for building evidence that stands strong in court.

Another vital research area is the identification and preservation of transient data. Dark web services typically use time-sensitive URLs, session-based communications, and temporary marketplaces, which create a dynamic and unpredictable evidence landscape. Forensic acquisition tools need to be capable of conducting live captures without altering or contaminating the evidence, all while maintaining the chain of custody. Well-designed frameworks support the real-time collection of volatile memory, network traffic, and endpoint artifacts, ensuring that forensic evidence remains intact for later analysis and court cases.²³

Recent developments in AI-driven dark web forensics are really making waves, especially with the combination of deep learning models and automated correlation engines. These innovative systems can dive into various types of data, like text, transactions, and user behavior, to spot patterns of criminal activity that were previously hidden. Techniques like graph neural networks (GNNs) and anomaly detection algorithms are increasingly utilized to map out relationships between users, services, and illegal transactions across various platforms, which significantly enhances investigative efficiency.²⁴ Moreover, AI-enhanced predictive models are being designed to identify upcoming threat campaigns. This allows law enforcement and security experts to better allocate their resources and minimize risks before any attacks happen.²⁵

When it comes to dark web forensics, ethical considerations are absolutely essential, particularly in areas like privacy, surveillance, and cross-jurisdictional investigations. Professionals stress the need to follow legal and ethical standards when collecting evidence in anonymized networks. This means prioritizing user privacy during targeted investigations, avoiding any form of entrapment, and being clear about the techniques used. Numerous experts support international collaboration and the establishment of standardized forensic protocols to ensure that investigations are legally defensible and foster consistent practices across different nations.²⁶

²³ Akshat, & Chitra B. T. (2025): “*Digital forensics and cybercrime investigation: An extensive exploration into the digital frontier*”, *International Journal of Creative Research Thoughts (IJCRT)*, 13(6), 796–807. ISSN 2320-2882.

²⁴ Magán-Carrión, R., Abellán-Galera, A., Maciá-Fernández, G., & García-Teodoro, P. (2021): “*Unveiling the I2P web structure: A connectivity analysis*”, *Computer Networks*, 194, 108158. DOI: 10.1016/j.comnet.2021.108158

²⁵ Brinson, R., Wimmer, H., & Chen, L. (2022): “*Dark web forensics: An investigation of tracking dark web activity with digital forensics*”, In: *Interdisciplinary Research in Technology and Management (IRTM) Conference Proceedings*, IEEE. DOI: 10.1109/IRTM54583.2022.9791646

²⁶ Akshat, & Chitra B. T. (2025): “*Digital forensics and cybercrime investigation: An extensive exploration into the digital frontier*”, *International Journal of Creative Research Thoughts (IJCRT)*, 13(6), 796–807. ISSN 2320-2882.

CONCLUSION

The dark web is a multifaceted and ever-changing area that offers users a significant amount of anonymity. While this can protect privacy, it also complicates forensic investigations into criminal behavior. To effectively trace digital footprints in this realm, investigators need to employ specialized tools and methods, including advanced network forensics, blockchain analysis, and AI-driven strategies for data classification and correlation.

Digital forensic specialists face a variety of challenges, including encryption, data volatility, temporary services, and the complexities of international legal systems. This reality pushes them to keep adapting and improving their investigative methods. The use of technologies like Tor and I2P networks, along with analyzing cryptocurrency transactions, is key to identifying and tracking illegal activities. These tools also bring up some serious ethical and legal issues. Striking a balance between protecting privacy and collecting reliable evidence is super important for us. With the latest advancements in artificial intelligence (AI) and machine learning, investigators are now able to detect patterns in criminal behavior more quickly and accurately. By piecing together various digital data, they can form a more complete understanding of the activities happening in the dark web.

However, tackling cybercrime effectively calls for international teamwork, standardized forensic methods, and continuous professional development. Ultimately, the secret to successfully tackling criminal activities hidden in the depths of the Internet is to combine technical innovation with a strong sense of ethical responsibility and adherence to the law. This blend not only creates a safer online space but also builds trust in the field of digital forensics.

LITERATURE

- AlSabah, M., & Goldberg, I. (2016): "Performance and security improvements for Tor: A survey", *ACM Computing Surveys*, 49(2), Article 32. DOI: 10.1145/2946802
- Akshat, & Chitra B. T. (2025): "Digital forensics and cybercrime investigation: An extensive exploration into the digital frontier", *International Journal of Creative Research Thoughts (IJCRT)*, 13(6), 796–807. ISSN 2320-2882.
- Brinson, R., Wimmer, H., & Chen, L. (2022): "Dark web forensics: An investigation of tracking dark web activity with digital forensics", In: *Interdisciplinary Research in Technology and Management (IRTM) Conference Proceedings*, IEEE. DOI: 10.1109/IRTM54583.2022.9791646
- de-Marcos, L., Medina-Merodio, J. A., & Štapić, Z. (2025): "Methodologies for data collection and analysis of dark web forum content: A systematic literature review", *Electronics*, 14(21), 4191. DOI: 10.3390/electronics14214191
- Gupta, A., Maynard, S. B., & Ahmad, A. (2021): "The dark web phenomenon: A review and research agenda", *arXiv preprint*, arXiv:2107.04490. <https://arxiv.org/abs/2107.04490>.
- Kwiatek, P., Papakonstantinidis, S., & Baltezarević, R. (2021): "Digital Masters' Entrepreneurial Mindset: A Comparative Study in Emerging Markets", in: U S. Rezaei, J. Li, S. Ashourizadeh, V. Ramadani i S. Gërguri-Rashiti (Ur.): *The Emerald Handbook of Women and Entrepreneurship in Developing Economies* (str. 295-315), Emerald Publishing Ltd.
- Magán-Carrión, R., Abellán-Galera, A., Maciá-Fernández, G., & García-Teodoro, P. (2021): "Unveiling the I2P web structure: A connectivity analysis", *Computer Networks*, 194, 108158. DOI: 10.1016/j.comnet.2021.108158
- McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008): "Shining light in dark places: Understanding the Tor network", In: N. Borisov & I. Goldberg (Eds.): *Privacy Enhancing Technologies – 8th International Symposium, PETS 2008, Leuven, Belgium, July 23-25, 2008, Proceedings* (Vol. 5134, pp. 63-76), Springer. DOI: 10.1007/978-3-540-70630-4_5
- Ruiz Ródenas, J. M., Pastor-Galindo, J., & Gómez Mármol, F. (2024): "A general and modular framework for dark web analysis", *Cluster Computing*, 27, 4687–4703. DOI: 10.1007/s10586-023-04189-2
- Safieddine, F., & Baltezarević, R. (2016): "Advances in technologies evolving new dimensions in e-society", In: V. Baltezarević, R. Baltezarević, & B. Baltezarević (Eds.): *The Internet as a tool of modern business and communication* (pp. 43-75), Lap Lambert Academic Publishing, Saarbrücken - Germany.
- UN (2025): *Darknet investigations*, <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/darknet.html> (01.11.2025).

- Vaghela, H., Varshney, N., & Jain, R. (2025): “Leveraging AI and ML to innovate forensic frameworks for the identification of illicit operations and extraction of digital artifacts within deep web and dark web environments”, *Journal of Digital Security and Forensics*, 2(1), 20–35. DOI: 10.29121/DigiSecForensics.v2.i1.2025.43
- Yin, H., & He, Y. (2019, March 15–16): “I2P anonymous traffic detection and identification”, In *Proceedings of the 5th International Conference on Advanced Computing & Communication Systems (ICACCS 2019)*, Coimbatore, India (pp. 157–162), IEEE. DOI: 10.1109/ICACCS.2019.8728517

FORENZIKA MRAČNOG VEB I ISTRAGA NEZAKONITIH DIGITALNIH TRAGOVA

Sažetak: *Mračni veb je poput tajnog kutka interneta, skriven od uobičajenih pretraživača i dostupan samo preko specijalizovanih mreža poput Tora ili I2P-a. U ovom mračnom carstvu, privatnost i enkripcija služe dvostrukoj svrsi, olakšavajući i legitimnu komunikaciju koja daje prioritet privatnosti, dok s druge strane olakšavaju različite oblike nezakonitih aktivnosti, uključujući trgovinu drogom i oružjem, finansijske prevare, kršenje bezbednosti podataka i sajber eksploataciju. Mračni veb predstavlja jedinstven skup izazova zbog svoje složene prirode i anonimnosti, što otežava život digitalnim istražiteljima. Moraju da se kreću kroz šifrovane sisteme, nose se sa nepredvidivim podacima i rešavaju složene međunarodne zakone. Ovaj rad detaljnije razmatra forenziku mračnog veba, otkrivajući kako istražitelji mogu da identifikuju, izdvoje i sačuvaju digitalne dokaze u ovom tajnom prostoru. Ovo ističe važnost obaveštajnih podataka otvorenog koda, analize blokčejna, mašinskog učenja i mrežne forenzike kao osnovnih alata za otkrivanje kriminalnih aktivnosti i praćenje ilegalnih digitalnih tragova. Štaviše, studija se bavi etičkim i pravnim izazovima infiltracije, nadzora i prikupljanja dokaza u anonimnim mrežama, naglašavajući važnost održavanja proceduralnog integriteta i poštovanja prava na privatnost. Rad se završava preporukama strateških pristupa za unapređenje međunarodne saradnje, olakšavanje bolje razmene podataka i uspostavljanje jedinstvenih forenzičkih protokola za efikasnu borbu protiv sajber kriminala povezanog sa mračnim vebom.*

Ključne reči: *forenzika dark veba, sajber kriminal, digitalni tragovi, onlajn anonimnost*

Bojan Zimonjic*

<https://orcid.org/0009-0001-6374-6454>

Jovica Vasiljevic**

<https://orcid.org/0000-0003-0149-2935>

UDK: 656.73:004

DOI: 10.5937/MegRev2502193Z

Originalni naučni rad

Primljen 15.08.2025.

Odobren 19.10.2025.

ULOGA INFORMACIONIH TEHNOLOGIJA U UNAPREĐENJU BEZBEDNOSTI CIVILNOG VAZDUHOPLOVSTVA

Sažetak: Bezbednost civilnog vazduhoplovstva predstavlja jedan od najvažnijih aspekata savremenog globalnog saobraćaja. Povećanje broja letova, razvoj digitalne infrastrukture i rast sajber pretnji nameću potrebu za novim pristupima zaštiti putnika, osoblja i vazduhoplovnih sistema. U tom kontekstu, informacione tehnologije (IT) imaju ključnu ulogu u unapređenju svih segmenata bezbednosti – od fizičke i operativne, do komunikacione i sajber bezbednosti.

Cilj ovog rada jeste da se analizira značaj i primena informacionih tehnologija u sistemu bezbednosti civilnog vazduhoplovstva, uz posebnu analizu implementacije na primeru Aerodroma „Nikola Tesla“ Beograd. Primenom metoda analize, komparacije i studije slučaja, istraženo je kako savremeni IT sistemi doprinose prevenciji incidenata, bržoj komunikaciji, automatizaciji procesa i smanjenju rizika ljudske greške.

Rezultati pokazuju da integracija informacionih tehnologija značajno povećava efikasnost i pouzdanost sistema bezbednosti, ali istovremeno zahteva stalno tehnološko unapređenje i edukaciju kadra. Zaključuje se da informacione tehnologije nisu samo tehničko sredstvo, već strateški resurs koji obezbeđuje održiv razvoj i sigurnost savremenog civilnog vazduhoplovstva.

Ključne reči: bezbednost, civilno vazduhoplovstvo, informacione tehnologije, sajber bezbednost, Aerodrom „Nikola Tesla“

* Megatrend Univerzitet, Beograd, Srbija
E-mail: bojanzimonjic1999@gmail.com

* Megatrend Univerzitet, Beograd, Srbija
E-mail: jovica.vasiljevic@gmail.com

UVOD

Bezbednost civilnog vazduhoplovstva predstavlja jedan od najvažnijih segmenata savremenog društva i globalnog saobraćajnog sistema. U eri ubrzanog tehnološkog razvoja i globalne povezanosti, vazdušni saobraćaj suočava se sa sve većim izazovima u pogledu zaštite putnika, osoblja, infrastrukture i informacionih sistema. Kako se pretnje razvijaju – od klasičnih oblika ugrožavanja bezbednosti do sofisticiranih sajber napada – tradicionalne metode zaštite više nisu dovoljne. U tom kontekstu, informacione tehnologije (IT) postaju ključni faktor u unapređenju i očuvanju bezbednosti civilnog vazduhoplovstva.

Informacione tehnologije omogućavaju bržu razmenu informacija, automatizovano prepoznavanje rizika, efikasnije reagovanje u kriznim situacijama i smanjenje ljudske greške. Korišćenjem savremenih IT sistema u oblastima kontrole letenja, nadzora, komunikacije, detekcije pretnji i sajber bezbednosti, ostvaruje se viši nivo pouzdanosti i sigurnosti vazdušnog saobraćaja.

Predmet ovog rada jeste analiza uloge informacionih tehnologija u unapređenju bezbednosti civilnog vazduhoplovstva, sa posebnim osvrtom na konkretan primer implementacije u okviru Aerodroma „Nikola Tesla“ Beograd.

Cilj rada je da se istraži kako savremene informacione tehnologije doprinose povećanju efikasnosti, preciznosti i sigurnosti sistema civilnog vazduhoplovstva, kao i da se prikažu konkretne prednosti i izazovi njihove primene u praksi. Osnovna hipoteza od koje se pošlo u radu je *Primena savremenih informacionih tehnologija značajno doprinosi unapređenju bezbednosti civilnog vazduhoplovstva.*

INFORMACIONE TEHNOLOGIJE

U savremenom društvu informacione tehnologije (IT) predstavljaju jedan od ključnih faktora razvoja gotovo svih delatnosti, uključujući i oblast bezbednosti civilnog vazduhoplovstva. IT sistemi omogućavaju obradu, razmenu, skladištenje i zaštitu podataka u realnom vremenu, čime se povećava efikasnost, tačnost i sigurnost procesa u kojima učestvuju ljudi i mašine.¹

Razvoj informacionih tehnologija zasnovan je na povezivanju računarskih sistema, softverskih aplikacija i telekomunikacionih mreža koje omogućavaju brz i bezbedan prenos informacija. U kontekstu vazduhoplovstva, IT ima poseban značaj jer se koristi u sistemima za navigaciju, komunikaciju, kontrolu letenja, nadzor i bezbednost putnika.²

¹ Laudon, K. C., & Laudon, J. P. (2020): *Management Information Systems: Managing the Digital Firm*, Pearson.

² Kovačević, D. (2019): *Bezbednost civilnog vazduhoplovstva*, Fakultet bezbednosti, Beograd.

Pod pojmom informacione tehnologije podrazumeva se skup tehničkih, softverskih i organizacionih rešenja koja omogućavaju efikasno upravljanje informacijama. Njihova osnovna funkcija jeste transformacija podataka u korisne informacije koje se mogu analizirati i koristiti za donošenje odluka.³

U oblasti bezbednosti, IT doprinosi uspostavljanju automatizovanih sistema praćenja, detekcije i komunikacije, čime se značajno smanjuje mogućnost greške ljudskog faktora. Savremeni informacioni sistemi u aviosaobraćaju karakterišu se integrisanošću (povezanost različitih podsistema), interoperabilnošću (mogućnost razmene podataka između različitih organizacija), i otpornosti na sajber pretnje.⁴

Informacione tehnologije mogu se klasifikovati prema njihovoj primeni i funkciji u vazduhoplovstvu:

1. Operativne tehnologije – odnose se na sisteme koji podržavaju kontrolu letenja, navigaciju, upravljanje aerodromskim operacijama i logistiku.
2. Bezbednosne tehnologije – uključuju video-nadzor, biometrijske sisteme, detekciju eksploziva, kontrolu pristupa i praćenje prtljaga.
3. Komunikacione tehnologije – obuhvataju radio-veze, digitalne mreže i enkriptovane kanale za razmenu podataka između letelica, tornjeva i zemaljskih službi.
4. Sajber bezbednosne tehnologije – namenjene su zaštiti informacionih mreža, baza podataka i sistema upravljanja od hakerskih napada i neovlašćenog pristupa.⁵

Ova podela pokazuje da informacione tehnologije prožimaju svaki segment vazduhoplovnog sistema, čineći ga bržim, preciznijim i sigurnijim.

Razvoj IT sistema u civilnom vazduhoplovstvu počeo je već sredinom XX veka sa uvođenjem prvih radarskih i komunikacionih sistema za kontrolu letenja. Tokom narednih decenija, tehnologija je napredovala kroz digitalizaciju kontrole saobraćaja i automatizaciju aerodromskih procesa.

Danas, informacione tehnologije obuhvataju napredne softverske platforme za upravljanje saobraćajem (ATM – Air Traffic Management), baze podataka za evidenciju letova, sisteme za bezbednosno praćenje i AI alate za analizu rizika.⁶

Poseban značaj imaju tehnologije poput:

- ADS-B (Automatic Dependent Surveillance – Broadcast) sistema koji omogućava automatsko praćenje letelica;

³ Vukićević, M. (2020): *Informacione tehnologije i savremeni bezbednosni sistemi*, FTN Izdavaštvo, Novi Sad.

⁴ Turban, E., & Volonino, L. (2017): *Information Technology for Management*, Wiley.

⁵ ICAO Annex 17 – *Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Montreal, ICAO, 2022.

⁶ International Civil Aviation Organization (ICAO) (2021): *Aviation Security Manual (Doc 8973)*.

- TCAS (Traffic Collision Avoidance System) koji sprečava sudare u vazduhu;
- i ACARS (Aircraft Communications Addressing and Reporting System) koji omogućava razmenu tehničkih i bezbednosnih informacija između letelice i kontrolnog tornja.⁷

BEZBEDNOST CIVILNOG VAZDUHOPLOVSTVA

Bezbednost civilnog vazduhoplovstva predstavlja jednu od najvažnijih komponenti međunarodnog saobraćajnog sistema i osnovni preduslov njegovog funkcionisanja. Ona podrazumeva sve mere, aktivnosti i procedure koje se sprovode s ciljem zaštite putnika, osoblja, vazduhoplova i infrastrukture od nezakonitih radnji, tehničkih incidenata i drugih rizika koji mogu ugroziti sigurnost leta.⁸

U savremenom dobu, kada se godišnje preveze više od četiri milijarde putnika širom sveta, bezbednost je postala globalni prioritet koji zahteva stalno unapređenje, tehnološki napredak i međunarodnu saradnju. Bezbednost civilnog vazduhoplovstva ne može se posmatrati kao izolovana delatnost, već kao složeni sistem u kojem učestvuju državne institucije, aerodromi, aviokompanije, međunarodne organizacije i sami putnici.⁹

Prema definiciji Međunarodne organizacije civilnog vazduhoplovstva (ICAO), bezbednost civilnog vazduhoplovstva (aviation security) obuhvata skup mera i ljudskih i materijalnih resursa kojima se sprečavaju akti nezakonitog mešanja u civilno vazduhoplovstvo, kao što su otmice vazduhoplova, sabotaze, teroristički napadi i druge radnje koje mogu ugroziti živote i imovinu.¹⁰

Značaj bezbednosti civilnog vazduhoplovstva ogleda se u njenoj preventivnoj funkciji — cilj nije samo reagovanje na incident, već pre svega njegovo sprečavanje. Efikasan sistem bezbednosti doprinosi poverenju putnika, stabilnosti avio-industrije i međunarodnom ugovornom poverenju među državama.¹¹

Bezbednost u vazduhoplovstvu se danas posmatra kroz dve osnovne dimenzije:

- fizičku bezbednost, koja se odnosi na zaštitu aerodroma, letelica i osoblja od fizičkih pretnji, i

⁷ EASA (2023): *Cybersecurity in Aviation – Safety Information Bulletin*, European Union Aviation Safety Agency, Köln.

⁸ Glišović, M. (2016): "Otmica vazduhoplova kao bezbednosna pretnja civilnom vazduhoplovstvu", *Nauka, bezbednost, policija*, 21(2), 197-213.

⁹ Гордић, П. (2025): "Тероризам као претња цивилном ваздушном саобраћају – историјски и правни аспекти, *Баština*, 35(66).

¹⁰ ICAO Annex 17 – *Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Montreal, 2022.

¹¹ EASA (2023): *Cybersecurity in Aviation – Safety Information Bulletin*, European Union Aviation Safety Agency, Köln.

- sajber bezbednost, koja se odnosi na zaštitu informacionih sistema i komunikacione infrastrukture od digitalnih napada.¹²

Obe dimenzije su podjednako važne jer se savremeni vazduhoplovni sistem oslanja na visok stepen digitalizacije, što povećava rizike, ali i mogućnosti zaštite.

Koncept zaštite civilnog vazduhoplovstva razvijao se postepeno, prateći razvoj avio-industrije i globalne bezbednosne situacije. Prvi ozbiljni naponi u uspostavljanju međunarodnog sistema bezbednosti datiraju iz 1944. godine, kada je osnovana ICAO potpisivanjem Čikaške konvencije o međunarodnom civilnom vazduhoplovstvu.

Tokom šezdesetih i sedamdesetih godina prošlog veka, sa pojavom sve češćih otmica aviona, uspostavljene su prve međunarodne konvencije o sprečavanju nezakonitih radnji u vazduhoplovstvu, kao što su:

- *Tokijska konvencija* (1963) o krivičnim delima i nekim drugim radnjama izvršenim na vazduhoplovima,
- *Haška konvencija* (1970) o suzbijanju otmica vazduhoplova, i
- *Montrealska konvencija* (1971) o suzbijanju nezakonitih radnji usmerenih protiv bezbednosti civilnog vazduhoplovstva.¹³

U periodu nakon terorističkih napada 11. septembra 2001. godine, globalni sistem bezbednosti u aviosaobraćaju doživeo je radikalnu transformaciju. Uvedene su strože kontrole putnika, obavezna provera prtljaga, biometrijska identifikacija i digitalna razmena bezbednosnih podataka između država. Ovaj period označio je početak nove ere u kojoj bezbednost civilnog vazduhoplovstva postaje visoko tehnološki i koordinisan sistem zaštite.

Bezbednost civilnog vazduhoplovstva funkcioniše kroz više nivoa upravljanja i uključuje međusobno povezane subjekte:

- međunarodne organizacije (ICAO, EASA, EUROCONTROL),
- nacionalne institucije (Direktorati civilnog vazduhoplovstva, ministarstva i agencije),
- aerodrome i aviokompanije.

Na međunarodnom nivou, osnovni dokument koji definiše bezbednosne standarde jeste ICAO Annex 17 – Security, koji propisuje obavezne mere za zaštitu od nezakonitih radnji. U okviru Evropske unije, bezbednost je regulisana Uredbom (EZ) br. 300/2008, kojom se definišu zajednička pravila i minimalni standardi zaštite.¹⁴

¹² *Convention on International Civil Aviation*, Chicago Convention, 1944.

¹³ Marković, A. N., & Zimonjić, B. (2025): "Analiza međunarodnog pravnog okvira u civilnom vazduhoplovstvu: Ženevska konvencija, haški protokol i pariski sporazum", *Megatrend revija*, 141.

¹⁴ Direktor civilnog vazduhoplovstva Republike Srbije (2021): *Nacionalni program zaštite civilnog vazduhoplovstva od nezakonitih radnji*.

U Republici Srbiji, sistem bezbednosti civilnog vazduhoplovstva uređuje se Zakonom o vazdušnom saobraćaju i Pravilnikom o merama zaštite civilnog vazduhoplovstva od nezakonitih radnji, koji se sprovodi pod nadzorom Direktorata civilnog vazduhoplovstva Srbije. Na nacionalnom nivou postoji i Nacionalni program zaštite civilnog vazduhoplovstva, koji predstavlja strateški okvir koordinacije između državnih organa i aerodroma.

Savremeni sistemi bezbednosti suočavaju se sa kompleksnim izazovima koji prevazilaze tradicionalne oblike ugrožavanja. Pored fizičkih pretnji, poput terorizma i sabotaza, sve više u prvi plan dolaze sajber napadi usmereni na kontrolne sisteme, baze podataka i komunikacione mreže. Prema izveštaju EASA iz 2023. godine, broj pokušaja sajber upada u avio-industriju porastao je za više od 25% u odnosu na prethodnu godinu, što ukazuje na potrebu za stalnim jačanjem digitalne zaštite.

Još jedan izazov predstavlja automatizacija i upotreba veštačke inteligencije (AI) u kontroli i nadzoru vazdušnog saobraćaja. Iako ovi sistemi doprinose efikasnosti, oni otvaraju nova pitanja odgovornosti i bezbednosti u slučaju tehničkih grešaka ili zloupotrebe podataka.

Bezbednost civilnog vazduhoplovstva danas zahteva multidisciplinarni pristup, koji obuhvata tehničke, organizacione i ljudske faktore. Ključ uspeha leži u stalnom usklađivanju nacionalnih propisa sa međunarodnim standardima i u kontinuiranoj obuci kadra koji upravlja bezbednosnim sistemima.¹⁵

Bezbednost civilnog vazduhoplovstva više nije samo tehničko ili administrativno pitanje, već globalni sistem saradnje i poverenja. Ona se zasniva na kombinaciji međunarodnih standarda, nacionalnih propisa, tehnoloških inovacija i ljudskog faktora. Savremeni trendovi pokazuju da je budućnost bezbednosti u aviosaobraćaju u potpunosti povezana sa razvojem informacionih tehnologija, digitalizacijom procesa i globalnom razmenom podataka. Samo integrisanim pristupom, koji kombinuje prevenciju, edukaciju i tehnologiju, moguće je obezbediti visok i trajan nivo zaštite u civilnom vazduhoplovstvu.

INFORMACIONE TEHNOLOGIJE U VAZDUHOPLOVSTVU

Informacione tehnologije zauzimaju centralno mesto u savremenom vazduhoplovstvu i predstavljaju osnovu funkcionisanja globalnog sistema civilnog saobraćaja. Njihova primena prožima gotovo svaki segment vazduhoplovne delatnosti — od planiranja i kontrole letenja, preko održavanja letelica i upravljanja aerodromima, do zaštite podataka i bezbednosti putnika. Bez informacionih tehnologija današnji

¹⁵ Stanković, V. A., & Petrošević, V. R. (2012): "Kontrola i zaštita vazdušnog prostora Republike Srbije", *Vojnotehnički glasnik*, 60(4), 211-229.

avio-saobraćaj ne bi mogao da obezbedi ni minimalni nivo pouzdanosti i efikasnosti koji se podrazumeva u modernom svetu.¹⁶

Primena informacionih tehnologija u vazduhoplovstvu ima za cilj da poveže i automatizuje različite operativne i administrativne procese koji su nekada bili potpuno odvojeni. Savremeni informacioni sistemi omogućavaju brzo prikupljanje, obradu i distribuciju podataka između letelica, kontrolnih tornjeva, aerodromskih službi i međunarodnih organizacija. Time se obezbeđuje visok nivo koordinacije, tačnosti i predvidivosti, što direktno doprinosi bezbednosti letenja. Digitalne platforme danas povezuju kontrolore letenja, pilote, meteorološke službe, logističke timove i bezbednosne agencije u jedinstvenu mrežu kroz koju informacije putuju u realnom vremenu.¹⁷

Jedan od najvažnijih aspekata primene IT u vazduhoplovstvu jeste upravljanje vazдушnim saobraćajem (Air Traffic Management – ATM). Reč je o kompleksnom sistemu koji zahvaljujući naprednim softverskim rešenjima omogućava praćenje letelica u svakom trenutku, predviđanje gustine saobraćaja i automatsko prilagođavanje ruta radi smanjenja mogućnosti kolizije. U okviru ovih sistema koriste se satelitske tehnologije, radarski senzori i digitalne komunikacione mreže koje omogućavaju stalnu razmenu podataka između letelica i zemaljskih stanica. Time se smanjuje rizik od ljudske greške i povećava preciznost kontrole, naročito u uslovima velike frekvencije letova.¹⁸

Pored sistema za upravljanje letenjem, informacione tehnologije imaju ključnu ulogu i u organizaciji i funkcionisanju aerodroma. Integrisani sistemi za upravljanje aerodromskim operacijama (Airport Operations Management Systems) omogućavaju planiranje poletanja i sletanja, praćenje prtljaga, kontrolu putnika i koordinaciju između različitih službi — od bezbednosne i tehničke, do carinske i medicinske. Takvi sistemi funkcionišu kao digitalni mozak aerodroma, čineći sve procese transparentnijim i bržim. Korišćenjem RFID oznaka, biometrijske identifikacije i automatskih čitača dokumenata, omogućeno je praćenje svakog putnika i prtljaga od prijave do ulaska u avion, što značajno smanjuje mogućnost propusta i zloupotreba.¹⁹

Tehnološki napredak doveo je i do razvoja brojnih specijalizovanih informacionih sistema koji podržavaju sigurnost letenja. Sistemi kao što su ADS-B (Automatic Dependent Surveillance – Broadcast) omogućavaju automatsko praćenje letelica putem satelitskog signala, dok TCAS (Traffic Collision Avoidance System) upozorava

¹⁶ Laudon, K. C., & Laudon, J. P. (2020): *Management Information Systems: Managing the Digital Firm*, Pearson.

¹⁷ Eurocontrol (2021): *European ATM Master Plan – Digitalisation of Air Traffic Management*, Brussels.

¹⁸ ICAO (2022): *Annex 10 – Aeronautical Telecommunications*, International Civil Aviation Organization, Montreal.

¹⁹ EASA (2023): *Cybersecurity in Aviation – Safety Information Bulletin*, European Union Aviation Safety Agency, Köln.

pilote na potencijalne konflikte u vazduhu i predlaže bezbedne manevre.⁵ Ovi sistemi funkcionišu nezavisno od ljudske kontrole, čime se povećava brzina reakcije i smanjuje mogućnost fatalnih grešaka. Još jedan važan sistem je ACARS (Aircraft Communications Addressing and Reporting System), koji omogućava razmenu digitalnih poruka između pilota i kontrolora letenja u realnom vremenu. Ovakvi sistemi čine osnovu digitalne komunikacione infrastrukture savremenog vazduhoplovstva.

Sa razvojem informacionih tehnologija pojavio se i novi vid izazova — potreba za zaštitom digitalne infrastrukture. U vreme kada je većina podataka elektronska, a procesi u potpunosti automatizovani, sajber bezbednost postaje jednako važna kao i fizička zaštita aerodroma i putnika. Hakerski napadi na kontrolne sisteme, baze podataka ili aerodromske mreže mogu imati ozbiljne posledice po bezbednost letenja i nacionalnu sigurnost. Zbog toga su međunarodne institucije poput ICAO i EASA uspostavile posebne smernice i bezbednosne standarde koji propisuju obaveznu implementaciju zaštitnih softvera, firewall sistema i enkripcije komunikacije. Sajber bezbednost postaje deo šireg koncepta integrisane zaštite civilnog vazduhoplovstva.

Uvođenje veštačke inteligencije (AI) i analitike velikih podataka (Big Data) dodatno je unapredilo rad informacionih sistema u vazduhoplovstvu. AI se koristi za predviđanje tehničkih kvarova, planiranje kapaciteta i optimizaciju ruta, dok analitički sistemi omogućavaju identifikaciju anomalija i potencijalnih pretnji na osnovu velikog broja parametara. Na taj način, informacione tehnologije ne samo da podržavaju operativne procese, već aktivno učestvuju u unapređenju bezbednosti i strateškom planiranju budućeg razvoja aviosaobraćaja.²⁰

Poseban segment razvoja predstavlja koncept tzv. „pametnih aerodroma“ (Smart Airports), gde se IT koristi za potpunu digitalizaciju aerodromskih procesa. IoT (Internet of Things) senzori prate temperature, kretanje ljudi, potrošnju energije i stanje opreme, dok centralni softver analizira prikupljene podatke i automatski donosi odluke o optimalnom korišćenju resursa. Time se ne samo povećava bezbednost, već i smanjuju troškovi i emisija štetnih gasova, što doprinosi održivom razvoju transporta.

Uloga informacionih tehnologija u vazduhoplovstvu ne ogleda se samo u tehničkom smislu, već i u strateškom — one omogućavaju globalnu povezanost, standardizaciju procedura i povećano poverenje između država i institucija. Vazduhoplovni sistem današnjice je visoko digitalizovan i međusobno zavisn, pa svaka promena ili propust u informacionom sistemu može imati dalekosežne posledice. Zato se može reći da informacione tehnologije čine okosnicu bezbednog i efikasnog funkcionisanja civilnog vazduhoplovstva, dok njihova stalna modernizacija predstavlja uslov za dalji razvoj ove strateški važne oblasti.²¹

²⁰ Turban, E., & Volonino, L. (2017): *Information Technology for Management*, Wiley.

²¹ IATA (2023): *Smart Airports: The Digital Future of Aviation*, International Air Transport Association, Montreal.

STUDIJA SLUČAJA: AERODROM „NIKOLA TESLA“ BEOGRAD

Aerodrom „Nikola Tesla“ u Beogradu predstavlja najvažniji međunarodni aerodrom Republike Srbije i jedno od ključnih čvorišta vazdušnog saobraćaja u jugoistočnoj Evropi. Kao strateški infrastrukturni objekat od nacionalnog značaja, on ima dvostruku ulogu — ekonomsku i bezbednosnu. S jedne strane, omogućava nesmetano odvijanje putničkog i teretnog saobraćaja i doprinosi razvoju turizma i privrede, dok sa druge, ima presudnu funkciju u sistemu nacionalne bezbednosti i međunarodne povezanosti države.

Bezbednosni sistem ovog aerodroma organizovan je u skladu sa međunarodnim standardima koje propisuju Međunarodna organizacija civilnog vazduhoplovstva (ICAO) i Evropska agencija za bezbednost vazduhoplovstva (EASA), kao i sa domaćim zakonodavstvom. Njegova struktura zasniva se na kombinaciji informacionih tehnologija, fizičke zaštite i ljudskog nadzora, čime se obezbeđuje sveobuhvatna zaštita od nezakonitih radnji i tehničkih incidenata. Ova studija slučaja ima za cilj da prikaže načine na koje su informacione tehnologije integrisane u sistem bezbednosti Aerodroma „Nikola Tesla“ i da analizira njihov doprinos efikasnijem funkcionisanju i višem nivou zaštite.

Bezbednosni sistem Aerodroma „Nikola Tesla“ funkcioniše u okviru Nacionalnog programa zaštite civilnog vazduhoplovstva od nezakonitih radnji, koji je u potpunosti usklađen sa međunarodnim propisima. Organizacija sistema obuhvata više međusobno povezanih segmenata: kontrolu pristupa, video-nadzor, kontrolu prtljaga i tereta, sajber bezbednost, komunikacione i krizne informacione sisteme. Sektor za bezbednost i zaštitu aerodroma ima centralnu ulogu u koordinaciji svih aktivnosti i sarađuje sa Direktoratom civilnog vazduhoplovstva, Ministarstvom unutrašnjih poslova i Bezbednosno-informativnom agencijom. Takav model saradnje između civilnih i državnih institucija omogućava brzo reagovanje i efikasnu razmenu informacija u slučaju bezbednosnih incidenata.

Primena informacionih tehnologija na Aerodromu „Nikola Tesla“ posebno je vidljiva u sistemima kontrole pristupa, video-nadzora, kontrole prtljaga, kriznog upravljanja i sajber zaštite. Integrisani sistem elektronske i biometrijske kontrole pristupa primenjuje se u svim sigurnosnim zonama aerodroma, uključujući terminale, piste, tehničke zone i tovarišta. Svaki zaposleni poseduje personalizovanu identifikacionu karticu sa čipom, a u posebno osetljivim područjima koristi se biometrijska autentifikacija putem otiska prsta ili prepoznavanja lica. Svi podaci o pristupu automatski se čuvaju i analiziraju u centralnoj bazi, što omogućava identifikaciju neuobičajenih obrazaca ponašanja i potencijalnih bezbednosnih rizika.

Jedan od najvažnijih segmenata digitalne zaštite čini sistem video-nadzora i inteligentne analitike. Na prostoru aerodroma instalirano je više od šest stotina kamera visoke rezolucije koje pokrivaju sve ključne zone, od putničkih terminala do manipulativnih i tehničkih prostora. Savremeni softveri zasnovani na veštačkoj inteligenciji omogućavaju automatsko prepoznavanje sumnjivih aktivnosti, detekciju napuštenih predmeta i praćenje kretanja osoba u zabranjenim područjima. Video-sistem povezan je sa komandnim centrom, što omogućava brzu reakciju službi obezbeđenja i policije u realnom vremenu. Ovakva integracija tehnologije i ljudske kontrole doprinosi prevenciji incidenata i podiže nivo bezbednosti putnika i zaposlenih.²²

Podjednako važnu ulogu imaju i sistemi za kontrolu prtljaga i tereta. Sav prtljag prolazi kroz višeslojne rendgenske i CT skenere koji su povezani sa centralnim IT sistemom aerodroma. Korišćenjem RFID (Radio Frequency Identification) tehnologije svaki komad prtljaga dobija jedinstvenu elektronsku oznaku koja omogućava njegovo praćenje od trenutka prijave do isporuke na odredištu. Ova tehnologija smanjuje mogućnost gubitka prtljaga i povećava efikasnost inspekcijskih postupaka. Softverska rešenja dodatno analiziraju slike sa skenera i automatski upozoravaju osoblje na prisustvo sumnjivih predmeta, čime se značajno smanjuje mogućnost ljudske greške.

Komunikacioni i krizni informacioni sistemi čine još jedan važan sloj digitalne infrastrukture. Aerodrom koristi digitalne radio-veze i enkriptovane komunikacione kanale između službi bezbednosti, kontrole letenja, vatrogasnih jedinica i medicinskih ekipa. U okviru ovih sistema funkcioniše i Emergency Response System, koji omogućava koordinisanu reakciju svih relevantnih službi u slučaju vanrednih događaja, kao što su tehnički kvarovi, požari ili bezbednosni incidenti. Ovakav sistem ne samo da skraćuje vreme reakcije, već i omogućava preciznu raspodelu zadataka i efikasno upravljanje kriznim situacijama.

Zbog visokog stepena digitalizacije poslovanja, sajber bezbednost zauzima centralno mesto u okviru IT strategije aerodroma. Korišćenjem firewall zaštite, antivirusnih programa, sistema za detekciju upada (IDS/IPS) i enkripcije komunikacije, obezbeđuje se siguran prenos podataka između različitih jedinica i institucija. Redovni sajber testovi i obuke zaposlenih imaju za cilj podizanje svesti o digitalnim rizicima i jačanje otpornosti sistema na moguće napade. Uspostavljanjem takvih protokola, Aerodrom „Nikola Tesla“ usklađuje svoje mere sa najvišim međunarodnim standardima zaštite informacionih sistema u vazduhoplovstvu.

Analiza efikasnosti pokazuje da je primena informacionih tehnologija na Aerodromu „Nikola Tesla“ značajno unapredila funkcionisanje bezbednosnog sistema. Automatizacija procesa omogućila je brže reagovanje na potencijalne

²² Zimonjić, M. (2025): „Uticaj ljudskog faktora na razvoj i značaj avijacijske komunikacije u očuvanju bezbednosti letenja“, *Megatrend revija*, 173.

pretnje, smanjila mogućnost ljudske greške i poboljšala koordinaciju između različitih službi i državnih organa. Obrada podataka u realnom vremenu omogućava donošenje pravovremenih odluka i bolju analizu rizika. Ipak, identifikovani su i određeni izazovi, među kojima se posebno ističe potreba za stalnim tehnološkim unapređenjem i obukom kadra za rad sa kompleksnim informacionim sistemima.

Rezultati istraživanja

Digitalizacija bezbednosnih procesa

Podaci iz godišnjih izveštaja Aerodroma „Nikola Tesla“ pokazuju da je u poslednjih pet godina digitalizovano više od 80% bezbednosnih procedura, uključujući:

- kontrolu pristupa osoblja,
- praćenje prtljaga putem RFID sistema,
- video-nadzor u realnom vremenu,
- elektronsku verifikaciju dokumenata i ID kartica.

Ova digitalna transformacija dovela je do smanjenja vremena reakcije u kriznim situacijama za oko 40%, kao i do povećanja tačnosti detekcije pretnji (posebno pri skeniranju prtljaga).

Efekti upotrebe biometrijskih i nadzornih sistema

Rezultati interne procene bezbednosti pokazuju da su biometrijski sistemi pristupa smanjili broj pokušaja neovlašćenog ulaska u kontrolisane zone za 65% u odnosu na period pre njihove implementacije. Istovremeno, inteligentne kamere sa AI analizom doprinele su bržem prepoznavanju neuobičajenog ponašanja, što je omogućilo preventivno reagovanje u više situacija bez većih incidenata.

Iako su zabeleženi pokušaji sajber napada na informacioni sistem aerodroma, nijedan nije rezultirao kompromitacijom kritičnih podataka zahvaljujući uvođenju višeslojnih zaštitnih mehanizama (firewall, IDS/IPS, enkripcija podataka). Broj registrovanih pokušaja napada porastao je za oko 30% u 2023. godini, što potvrđuje rastući značaj sajber bezbednosti kao komponente ukupnog sistema zaštite.

Prema anketi sprovedenoj među 50 zaposlenih u sektoru bezbednosti i IT podrške, čak 88% ispitanika ocenilo je da informacione tehnologije „značajno unapređuju efikasnost i tačnost rada“, dok je 12% ispitanika navelo da sistemi zahtevaju dodatne obuke i tehničko održavanje. Najvećim prednostima IT sistema zaposleni smatraju:

- brzu dostupnost informacija (56%),
- smanjenje grešaka (28%),
- bolju komunikaciju između službi (16%).

Kao najveći izazovi navedeni su:

- složenost softverskih platformi,
- troškovi održavanja,
- i potreba za stalnim ažuriranjem i obukom korisnika.

Tabela 1: Tipovi informacionih tehnologija i njihove funkcije u bezbednosti civilnog vazduhoplovstva

Vrsta tehnologije	Osnovna funkcija	Efekat na bezbednost	Primenjeni primer na Aerodromu „Nikola Tesla“
CCTV kamere visoke rezolucije	Video-nadzor, praćenje pokreta i ponašanja	Pravovremeno uočavanje incidenata i neovlašćenog kretanja	Kamere sa AI analitikom u terminalima i oko pista
AI softver za analizu slike	Automatsko prepoznavanje lica, predmeta, napuštenog prtljaga	Smanjenje ljudske greške, brža reakcija	„SmartVision“ algoritmi za prepoznavanje anomalija
Biometrijski sistemi	Identifikacija osoblja putem otiska prsta ili lica	Sprečavanje neovlašćenog pristupa sigurnosnim zonama	Biometrijske čitačiće u zoni kontrole i hangarima
RFID tehnologija	Praćenje prtljaga i tereta u realnom vremenu	Smanjenje gubitaka, poboljšana kontrola logistike	RFID oznake integrisane u sistem za rukovanje prtljagom
CT i rendgenski skeneri	Analiza sadržaja prtljaga i otkrivanje zabranjenih predmeta	Povećana tačnost kontrole i efikasnost pregleda	Digitalno povezani skeneri sa centralnim serverom
Firewall i IDS/IPS sistemi	Detekcija i sprečavanje sajber napada	Zaštita informacionih mreža i baza podataka	Višeslojna mrežna zaštita i redovni bezbednosni testovi
Krizni informacioni sistem (Emergency Response System)	Automatsko obaveštavanje i koordinacija u vanrednim situacijama	Brže reagovanje i sinhronizacija službi	Digitalna platforma povezana sa MUP-om i BIA-om
Digitalne radio-komunikacije	Brza i bezbedna komunikacija između službi	Povećana koordinacija i smanjenje kašnjenja reakcije	Enkriptovani radio-kanali i bežične veze
Centralna baza podataka (Security Data Center)	Skladištenje i analiza podataka o pristupu, video-sadržajima i incidentima	Integracija informacija i efikasno donošenje odluka	Centralizovani serverski sistem sa šifrovanim pristupom

Izvor: Autori, na osnovu dostupne dokumentacije i literature (2025).

Tabela prikazuje najvažnije informacione tehnologije koje se koriste u savremenim sistemima bezbednosti civilnog vazduhoplovstva, sa posebnim osvrtom na njihovu primenu na Aerodromu „Nikola Tesla“ Beograd. Svaka tehnologija doprinosi određenom segmentu bezbednosti – od fizičke i tehničke, do sajber zaštite i kriznog upravljanja.

Kamera visoke rezolucije i AI analitika omogućavaju kontinuirani nadzor i detekciju sumnjivog ponašanja u realnom vremenu. Biometrijski sistemi i elektronske kartice obezbeđuju kontrolisan pristup osetljivim zonama, dok RFID i CT sistemi obezbeđuju praćenje i proveru prtljaga i tereta. S druge strane, IT infrastruktura – poput firewall zaštite i IDS/IPS sistema – ima ključnu ulogu u zaštiti od sajber napada i neovlašćenog pristupa bazama podataka.

Tabela jasno pokazuje da svaka od navedenih tehnologija ima specifičnu funkciju, ali da njihova integracija u jedinstveni bezbednosni sistem daje najbolji rezultat u zaštiti putnika, osoblja i infrastrukture.

Analizom prikupljenih podataka potvrđeno je da su informacione tehnologije imale značajan pozitivan uticaj na bezbednosni sistem Aerodroma „Nikola Tesla“. Integracija biometrije, pametnog video-nadzora, RFID tehnologije i kriznog informacionog sistema dovela je do smanjenja broja incidenata, bržeg reagovanja službi i većeg stepena pouzdanosti u zaštiti infrastrukture i putnika.

S druge strane, rezultati ukazuju na potrebu kontinuiranog unapređenja u oblasti sajber bezbednosti i edukacije zaposlenih. Visok stepen automatizacije ne može u potpunosti zameniti ljudski faktor, već zahteva skladnu saradnju čoveka i tehnologije, zasnovanu na znanju i disciplini.

ZAKLJUČAK

Bezbednost civilnog vazduhoplovstva danas predstavlja jedan od najkompleksnijih i najvažnijih aspekata globalnog saobraćaja. Savremeni vazduhoplovni sistemi ne mogu se posmatrati izolovano od informacionih tehnologija, jer upravo IT čini njihovu osnovu i povezuje sve operativne, tehničke i bezbednosne funkcije u jedinstvenu celinu. Digitalizacija procesa, automatizacija nadzora i razvoj naprednih sistema analitike omogućili su značajno unapređenje bezbednosti na svim nivoima – od kontrole pristupa i praćenja letova do zaštite komunikacionih i informacionih mreža.

Analiza sprovedena u ovom radu pokazala je da informacione tehnologije ne samo da povećavaju efikasnost i brzinu reagovanja u kriznim situacijama, već i smanjuju mogućnost ljudske greške, unapređuju preciznost donošenja odluka i omogućavaju pravovremenu detekciju i prevenciju bezbednosnih pretnji. Studija slučaja Aerodroma „Nikola Tesla“ Beograd potvrđuje da integracija biometrijskih sistema, inteligentnog video-nadzora, RFID tehnologije i naprednih sajber zaštita rezultira višim stepenom sigurnosti i boljom koordinacijom svih službi.

Međutim, rezultati istraživanja ukazuju i na to da bezbednosni sistem mora biti u stalnom procesu modernizacije. Pojava novih oblika sajber pretnji, ubrzani

razvoj veštačke inteligencije i rast kompleksnosti vazdušnog saobraćaja zahtevaju kontinuirano unapređenje softverskih i hardverskih komponenti, kao i neprestanu edukaciju stručnog kadra. Održavanje visokog nivoa bezbednosti moguće je jedino ako tehnološki razvoj prati odgovarajuća institucionalna podrška, međunarodna saradnja i primena propisa usklađenih sa ICAO i EASA standardima.

Uloga informacionih tehnologija u bezbednosti civilnog vazduhoplovstva više nije pomoćna, već strateška. One predstavljaju osnovni instrument očuvanja poverenja putnika, stabilnosti saobraćajnog sistema i međunarodne saradnje u oblasti avijacije. Integracijom IT rešenja u sve segmente bezbednosne infrastrukture stvara se preduslov za održiv razvoj i dugoročnu otpornost sistema na izazove savremenog doba.

Zaključno, može se reći da budućnost bezbednosti civilnog vazduhoplovstva zavisi od sposobnosti da se informacione tehnologije neprestano razvijaju, prilagođavaju i integrišu u sve procese — jer jedino kroz sinergiju čoveka, tehnologije i organizacije moguće je ostvariti cilj: sigurno, efikasno i pouzdano vazduhoplovstvo za 21. vek.

LITERATURA

1. *Convention on International Civil Aviation*, Chicago Convention, 1944.
2. Direktorat civilnog vazduhoplovstva Republike Srbije (2021): *Nacionalni program zaštite civilnog vazduhoplovstva od nezakonitih radnji*.
3. Eurocontrol (2021): *European ATM Master Plan – Digitalisation of Air Traffic Management*, Brussels.
4. EASA (2023): *Cybersecurity in Aviation – Safety Information Bulletin*, European Union Aviation Safety Agency, Köln.
5. Glišović, M. (2016): "Otmica vazduhoplova kao bezbednosna pretnja civilnom vazduhoplovstvu", *Nauka, bezbednost, policija*, 21(2), 197–213.
6. Гордић, П. (2025): "Тероризам као претња цивилном ваздушном саобраћају – историјски и правни аспекти", *Baština*, 35(66).
7. IATA (2023): *Smart Airports: The Digital Future of Aviation*, International Air Transport Association, Montreal.
8. ICAO (2021): *Aviation Security Manual (Doc 8973)*, International Civil Aviation Organization, Montreal.
9. ICAO (2022): *Annex 10 – Aeronautical Telecommunications*, International Civil Aviation Organization, Montreal.
10. ICAO (2022): *Annex 17 – Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, International Civil Aviation Organization, Montreal.

11. Kovačević, D. (2019): *Bezbednost civilnog vazduhoplovstva*, Fakultet bezbednosti, Beograd.
12. Laudon, K. C., & Laudon, J. P. (2020): *Management Information Systems: Managing the Digital Firm*, Pearson.
13. Marković, A. N., & Zimonjić, B. (2025): "Analiza međunarodnog pravnog okvira u civilnom vazduhoplovstvu: Ženevska konvencija, Haški protokol i Pariski sporazum", *Megatrend revija*, 141.
14. Stanković, V. A., & Petrošević, V. R. (2012): "Kontrola i zaštita vazdušnog prostora Republike Srbije", *Vojnotehnički glasnik*, 60(4), 211–229.
15. Turban, E., & Volonino, L. (2017): *Information Technology for Management*, Wiley.
16. Vukićević, M. (2020): *Informacione tehnologije i savremeni bezbednosni sistemi*, FTN Izdavaštvo, Novi Sad.
17. Zimonjić, M. (2025): "Uticaj ljudskog faktora na razvoj i značaj avijacijske komunikacije u očuvanju bezbednosti letenja", *Megatrend revija*, 173.

THE ROLE OF INFORMATION TECHNOLOGY IN ENHANCING THE SECURITY OF CIVIL AVIATION

Summary: *The security of civil aviation represents one of the most important aspects of modern global transportation. The increasing number of flights, the development of digital infrastructure, and the growing cyber threats create the need for new approaches to protecting passengers, personnel, and aviation systems. In this context, information technology (IT) plays a crucial role in improving all aspects of security – from physical and operational to communication and cybersecurity.*

This paper aims to analyze the significance and application of information technologies within the civil aviation security system, with a special focus on the implementation at Belgrade Nikola Tesla Airport. Through methods of analysis, comparison, and case study, the research examines how modern IT systems contribute to incident prevention, faster communication, process automation, and the reduction of human error risks.

The results show that the integration of information technologies significantly increases the efficiency and reliability of security systems, while at the same time requiring continuous technological advancement and staff training. It is concluded that information technologies are not merely a technical tool but a strategic resource that ensures the sustainable development and safety of modern civil aviation.

Keywords: *security, civil aviation, information technology, cybersecurity, Belgrade Nikola Tesla Airport*

Dejana Radović*

<https://orcid.org/0009-0007-0762-5352>

Dragan Nikolić**

<https://orcid.org/0009-0000-0054-6861>

UDC: 341.7:811.111

DOI: 10.5937/MegRev2502209R

Original scientific paper

Received 15.06.2025.

Approved 17.09.2025.

DIPLOMATIC ACTIVITIES AND THE INFLUENCE OF THE ENGLISH LANGUAGE ON LOCAL TERMINOLOGY IN SECURITY AND CORPORATE CONTEXTS

Abstract: *This paper delves into the significant impact of the English language on local terminology, especially within the realms of diplomacy, security, and corporate settings. By examining both theoretical frameworks and real-life examples, the study illustrates that English is not just a global communication tool but also a significant force in transforming the language used in diplomatic and institutional contexts. It merges institutional and linguistic perspectives, especially through the lens of New Institutional Theory, to analyze how language helps construct organizational legitimacy and identity in diplomatic settings. Additionally, it explores lexical borrowing, translation practices, and language policies in multilingual contexts, shedding light on how English terms related to diplomacy, such as protocol, negotiation, and bilateral agreement, as well as security and corporate concepts like firewall and risk management, are adopted, modified, or resisted at the local level. The results suggest that while the English language's influence helps create a more standardized and effective framework for diplomatic and institutional dialogues, it also raises important issues about clarity, fairness, and cultural significance. Ultimately, this research reveals the intricate relationship between the global influence of English and the local linguistic identities that shape diplomatic efforts, security issues, and corporate communication.*

Keywords: *diplomatic activities, englishization, institutional legitimacy, lexical borrowing*

* E-mail: littlemissmuffet08@gmail.com

** E-mail: nikolic.dragan.0314@gmail.com

1. INTRODUCTION

In the contemporary world of business and security, the English language has emerged as a crucial influence on local terminology, professional exchanges, and institutional communication. Organizations that work across borders, like multinational corporations, security agencies, and cyber security firms, often choose English as their primary means of communication and as a source of new terms. This trend impacts how local languages incorporate, modify, or resist English words, acronyms, discourse patterns, and expressions.

Research indicates that English plays a significant role in corporate settings. Take, for instance, a multinational company in Chile where only about 25% of employees were highly fluent in English as the corporate language. Meanwhile, 53% had a medium level of fluency, and 22% were at a low fluency level.¹ Looking at Norway, a study of 492 of the largest companies by revenue showed that 36.2% published their annual reports only in Norwegian, while 18.9% used English exclusively (with permission under the Norwegian Accounting Act). The remaining 44.9% utilized multiple languages, typically presenting Norwegian and English in parallel versions.² These statistics highlight that English often serves as a complementary language to the national tongue in official documents, rather than completely taking its place.

Diplomatic efforts today are increasingly reliant on clear and standardized language to ensure smooth communication and coordination among a variety of institutional and national actors. English, as the go-to language for international diplomacy, plays a key role in shaping the specialized vocabulary that diplomats, security personnel, and business stakeholders use to navigate the complexities of negotiations, treaties, and collaborative initiatives. The use of English terms related to diplomatic protocols, negotiation strategies, and both bilateral and multilateral agreements has significantly altered local terminology systems. This shift not only changes how these discussions take place but also impacts how legitimacy and authority are perceived within diplomatic institutions. This integration highlights the need to grasp the relationship between English's linguistic influence and the unique cultural and institutional contexts of diplomatic settings.

When it comes to security-related communication, especially in the fields of cybersecurity and risk management, the emphasis on English terminology is even more pronounced. A study involving Data Science and Cyber Security students at Al Istiqlāl University found that cadets need to have strong English

¹ Reiche, B. S. & Neeley, T. B. (2019): "Head, heart, or hands: how do employees respond to a radical global language change over time?", *Organization Science*, 30(6), 1252–1269. DOI: 10.1287/orsc.2019.1289

² Sanden, G. R. (2020): "Language policy and corporate law: A case study from Norway", *Nordic Journal of Linguistics*, 43(1), 59–91. DOI: 10.1017/S0332586519000222

communication skills, particularly in listening, speaking, and comprehension. This need underscores the global aspect of threat intelligence, technical training, and the standardization of terms.³ However, the studies highlight a few concerns: local participants might not have the necessary skills or could find it challenging to translate or adapt new English terms to fit their local contexts.

These influences extend beyond mere vocabulary. Language policy, identity, and institutional practices all contribute to the mix. When English terminology is adopted, it can reinforce power imbalances, like those between native and non-native speakers. This can lead to confusion or even a loss of culturally specific meanings, often resulting in a struggle between preserving our linguistic heritage and achieving international clarity. Furthermore, research into business English as a lingua franca (BELF) points out that it's not just about the words; the way we communicate, the genres we use, and our pragmatic expectations often shift under the influence of English (think about press releases, international reports, and corporate social responsibility disclosures).

This paper examines the ways in which English shapes local terminology in security and corporate environments. It will focus on how borrowed terms integrate into local usage, the influence of language policy and translation on these borrowings, and their effects on clarity, identity, and institutional legitimacy. It will also examine the tactics that local players use, including adopting, adapting, hybridizing, or resisting these terms. The aim is to offer a deeper understanding of how global English impacts these environments and the implications for local terminology systems.

2. EMPIRICAL AND THEORETICAL INSIGHTS

Since interest in organisational theories moved from sociology and linguistics, it has been acknowledged that language plays a crucial role in comprehending organisational symbols.⁴ Organisational language is central to New Institutional Theory (NIT), according to two sets of studies in the literature. The first focusses on how organisational language affects how institutions are formed and evolve.⁵

³ Masood, K. (2022): "English Competencies and Challenges for Data Science and Cyber Security Students at Al Istiqlal University", *The Creative Launcher*, 7(5), 48–68. DOI: 10.53032/tcl.2022.7.5.05

⁴ Putnam, L., & Fairhurst, G. L. (2001): "Discourse analysis in organizations"; In: F. M. Jablin & L. Putnam (Eds.): *Sage handbook of organizational communication* (pp. 78–136), Sage, London.

⁵ Cornelissen, J. P., Durand, R., Fiss, P. C., Lammers, J. C., & Vaara, E. (2015): "Putting communication front and center in institutional theory and analysis", *Academy of Management Review*, 40(1), 10–27.

This method, which emphasises the crucial significance of language and meaning, is known as “communicative institutionalism” or “rhetorical institutionalism.”⁶ The second set of research raises concerns about how organisational language contributes to the establishment of organisational legitimacy. According to this research, legitimacy is a perceptual process that is based on linguistic structure and involves the emergence of shared meaning through language.⁷ While “linguistic method” refers to any technique that looks at the relationship between institutions and language-based institutional variables, “grounded in language” also refers to approaches that use language to explain legitimacy. “Institutional strategies” are the use of standard language practices to gain legitimacy.⁸ The intended legitimacy cannot be attained if an organization’s language strategies do not align with the institutional environment or the opinions and views of the actors evaluating it. Because of this, organisations prioritise the demands of their institutional context when developing their language strategies.⁹

One of the most important strategic instruments in diplomacy is language. It affects not just the way we communicate but also the power balance and the legitimacy of the organizations engaged in international affairs. English has emerged as the primary language of diplomacy, making it easier for state actors, international organizations, and corporations to engage in discussions about security and foreign policy. The words used in diplomatic conversations, such as summit, consulate, diplomatic immunity, and conflict resolution, are significant in defining roles and ensuring that local practices meet global expectations. Therefore, the trend of Englishization in diplomacy is key to understanding how local terminology shifts in response to global pressures and institutional requirements.

With the help of globalisation, English has changed from being just one foreign language among many to becoming a common language used for both work and play.¹⁰ This Englishization is displacing other languages used in non-Anglophone contexts and is particularly prevalent in the business and academic sectors. Finland serves as an example, where business managers, for instance, lead mobile lives and do their work in English, communicating with clients and coworkers by email and text commenting. The country also boasts a high level of English proficiency.¹¹

⁶ Green, S. E. (2004): “A rhetorical theory of diffusion”, *Academy of Management Review*, 29(4), 653–669.

⁷ Suddaby, R., Bitektine, A. & Haack, P. (2017): “Legitimacy”, *Academy of Management Annals*, 11(1), 451–478.

⁸ Lawrence, T. B. (1999): “Institutional strategy”, *Journal of Management*, 25(2), 161–188.

⁹ Green, S. E. (2004): “A rhetorical theory of diffusion”, *Academy of Management Review*, 29(4), 653–669.

¹⁰ Graddol, D. (1999): “The decline of the native speaker”, *AILA Review*, 13, 57–68.

¹¹ Leppänen, S., Pitkänen-Huhta, A., Nikula, T., Kytölä, S., Törmäkangas, T., Nissinen, K., Kääntä, L., Räisänen, T., Laitinen, M., Pahta, P., Koskela, H., Lähdesmäki, S. and Jousmäki, H.

English has become the work language of a new generation of employees who take charge of their own message exchange with foreign partners after globalisation and the drastic advancements in communication technologies replaced secretaries with foreign language proficiency handling format-bound business correspondence. English is now at the core of linguistic forms of employment and work processes due to its evolution as a global language. The language of mobile, international knowledge work is now English.¹² English is frequently chosen by management as the corporate language, and it is enforced through formal rules or more casual suggestions.¹³ In either scenario, the corporate language is at the top of the corporate language hierarchy, which could lead to a rise in status disparities and competition between individuals who are proficient in the language and those who are not.¹⁴

It is said that an increasing number of businesses have made English their official or common corporate language since it seems to be the simplest way to address the communication problems brought on by linguistic differences. But the problems with language or languages are sensitive and nuanced. Even if English is the official/common language of the organisation, research have shown that personnel from various linguistic and cultural backgrounds have trouble communicating with one another.¹⁵

Not all linguistic problems in international commerce are resolved by making English the standard or official corporate language. Previous research has shown that company-wide language rules can have unfavourable side effects. Most importantly, there may be problems with status gain and loss. The language policy may be resented by non-native speakers of the company's dominant language who feel they have lost their status and competitive edge because they worry that they won't be able to express themselves as clearly and sophisticatedly as they can in their native tongue. However, because the status-gain was undeserved, the Native

(2011): "National survey on the English language in Finland: Uses, meanings and attitudes", *Studies of Variation, Contacts and Change in English*, Vol. 5, <http://www.helsinki.fi/varieng/journal/volumes/05/>.

¹² Duchêne, A. and Heller, M. (2012): "Language policy and the workplace", in: Spolsky, B. (Ed.): *The Cambridge Handbook of Language Policy*, Cambridge University Press, Cambridge, pp.323–335.

¹³ Sanden, G. & Lønsmann, D. (2018). Discretionary power on the front line: a bottom-up perspective on corporate language management', *European Journal of International Management*, 12(1/2), 111–137.

¹⁴ Lønsmann, D. (2015). 'Language ideologies in a Danish company with English as a corporate language: 'it has to be English'', *Journal of Multilingual and Multicultural Development*, 36(4), 339–356.

¹⁵ Neeley, T. B. (2013): "Language matters: Status loss and achieved status distinctions in global organizations", *Organization Science*, 24(2), 476–497.

English speakers of the US subsidiary of a Japanese corporation that had made English their official corporate language felt uneasy.¹⁶

When it comes to institutional communication, especially through digital or tech-driven channels, the usual boundaries of concepts and terms can get a bit fuzzy. One study highlights this by stating, a discourse which takes place in virtual space ... raises the question of whether traditional conceptual categories remain appropriate when mediated by digital interfaces.¹⁷

Words from English are now utilised in many other languages worldwide. It is hardly surprising that English terminology being incorporated into other languages given that English has become a universal language. Simply put, a loan word is a word that has been borrowed and used in another language. Other names for it are borrowing and, occasionally, calque. These borrowed terms are also referred to as anglicisms, which only indicates that they have English roots.

For a variety of reasons, English words can be borrowed into other languages. This may be done to keep up with current trends or to give a language a more global feel, but other times it may be done because the language lacks a natural equivalent for something. Any language needs loan words because they frequently supply desirable or practical concepts that might not be present in the native tongue. Numerous languages have borrowed terms from English for a variety of purposes, ranging from literal translation to more imaginative uses, and they frequently offer fascinating insights into a language's past and culture.¹⁸

A common occurrence that represents linguistic and cultural exchanges is lexical borrowing, the process by which one language absorbs words and phrases from another. The vocabulary and usage patterns of the borrowed language are greatly impacted by this process, creating linguistic landscapes that are both complex and enriching.¹⁹ Lexical borrowing is important because it represents historical, social, and cultural interactions and shows how dynamic languages in touch are.²⁰ Its value goes beyond simple vocabulary growth.

Diplomatic terminology is especially susceptible to borrowing from other languages, largely because diplomatic work is inherently international and multicultural. When English terms are borrowed, they not only help make communication

¹⁶ Neeley, T. B. & Dumas, T.L. (2016): "Unearned status gain: Evidence from a global language mandate", *Academy of Management Journal* 59(1), 14–43.

¹⁷ Baltezarević, R. & Baltezarević, B. (2018): "The Impact of Video Games on the Formation of Esports", *Facta Universitatis, Series: Physical Education and Sport*, 16(1), 137–147. DOI: 10.22190/FUPES170614012B

¹⁸ Readle-app (2024): *Loan Words: English Words Used in Other Languages*. <https://readle-app.com/en/blog/loan-words-english-words-used-in-other-languages/>.

¹⁹ Hoffer, B. L. (2005): "Language borrowing and the indices of adaptability and receptivity", *Intercultural Communication Studies*, 14(4), 53–68.

²⁰ Winford, D. (2003): *An introduction to contact linguistics*, Blackwell Publishing.

clearer across various languages but also act as symbols of legitimacy and professionalism in diplomatic circles. For instance, terms like “memorandum of understanding,” “diplomatic corps,” and “track two diplomacy” are frequently adopted or modified, demonstrating how English has permeated diplomatic language. This trend sheds light on the wider cultural and political effects of borrowing language, where the prestige of English terms can sometimes eclipse local linguistic traditions, yet also foster better cooperation in international contexts.

In multilingual institutions, using English security or corporate jargon can really widen the gap in understanding and access. Communication in a virtual environment includes key issues of equality in access in more complex, multicultural societies.²¹ This same issue pops up in corporate or security settings, where non-native speakers or those with limited English skills might find themselves sidelined or misunderstood due to the use of specialized terms.

In many corporate and security settings where English isn't the primary language, it serves not just as a tool for global communication but also as a source of new vocabulary. Terms are borrowed, adapted, or mixed, which changes the local terminology landscape. For example, in the realm of information security, glossaries often include English technical terms like “firewall,” “access control,” “incident management,” and “threat modeling.” These terms might appear as direct loanwords (unchanged), be translated while keeping the English form for prestige or clarity, or even be calqued. This phenomenon is evident in Turkish, Spanish, Croatian, etc. translations of glossaries.²²

English serves as a crucial bridge in establishing institutional legitimacy and standardization efforts. For instance, the Global Interagency Security Forum (GISF) has put together a glossary featuring over 230 terms related to security-risk management in English, which have also been translated into French, Spanish, and Arabic. This effort is all about fostering a common understanding and precision among different language groups.²³ In this context, English acts as the main standard, while local terms evolve through translation, equivalence, or borrowing. This approach helps local actors connect with global norms while maintaining clarity.

Still, embracing English terms can stir up some challenges around clarity, identity, and power dynamics. Often, local players are hesitant to adopt these terms entirely, as they might not mesh well with local beliefs or cultural contexts. Take peacebuilding and security sector work, for example; civil society organizations

²¹ Baltezarević, I. & Baltezarević, R. (2020): “Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku”, *Megatrend revija*, 17(4), 27–40. DOI: 10.5937/MegRev2004027B

²² Kosutic, D. (2025): *Glossary of information security and business continuity terms*, <https://advisera.com/27001academy/knowledgebase/glossary/>.

²³ Global Interagency Security Forum (GISF) (2024): *GISF's interactive glossary is released in four languages!*, <https://gisf.ngo/gisf-glossary-released-in-four-languages/>.

frequently mention that “security forces and civil society are not speaking the same language.” This means that the same English or technical terms can be interpreted differently or carry various meanings across different groups. Efforts to translate, define, or differentiate these terms are crucial in tackling miscommunication and reinforcing institutional legitimacy or local identity.²⁴

The evolution and acceptance of diplomatic terms are significantly influenced by language regulations that require the use of English, much like in the corporate and security arenas. Diplomatic missions and international organizations typically develop language guidelines that favor English for official communications, documents, and protocols. These policies play a crucial role in not just standardizing communication but also shaping how local diplomats manage their linguistic identities and the credibility of their institutions. Consequently, the struggle between embracing English terminology and maintaining culturally meaningful local terms becomes particularly evident in diplomatic contexts, where language choices mirror larger issues of sovereignty, representation, and global integration.

Translation and policy mechanisms play a crucial role in how terms derived from English are incorporated into other languages. Language policies, whether they come from corporations or governments, that require English to be used (or allow it as the default for certain documents) or that necessitate bilingual glossaries have a strong impact on which terms get borrowed and how they’re used. The recent “Translation and Security” symposium²⁵ stressed the need for national security translation centers, the development of standards for security-related translations, and the provision of cultural and ethical training for translators in security agencies. This is all aimed at standardizing terminology and reducing the chances of misinterpretation or the confusion that comes from overlapping terms.

3. CONCLUSION

This paper emphasizes how deeply English influences local terminology, especially in the realms of diplomacy, corporate affairs, and security. In diplomatic communication, English plays a crucial role in ensuring consistency, clarity, and

²⁴ Schirch, L. & Mancini-Griffoli, D. (2016): “Local Ownership in Security Report. Alliance for Peacebuilding / GPPAC”, *Translating Language and Terminology*, <https://gppac.net/files/2019-01/Local%20Ownership%20in%20Security%20Report.%2015%20March%202016.pdf>.

²⁵ ICESCO (2025): *Translation and Security Symposium Calls for Developing Technological and Linguistic Mechanisms, Fostering Complementarity between Security Agencies and Translators*, <https://icesco.org/en/2025/07/07/translation-and-security-symposium-calls-for-developing-technological-and-linguistic-mechanisms-fostering-complementarity-between-security-agencies-and-translators/>.

institutional credibility among various international players. The patterns we see in diplomatic language practices reveal a larger negotiation between global language norms and local cultural identities, highlighting the intricate process of adopting terminology in sensitive and politically charged environments.

Furthermore, this analysis shows just how important the English language is in shaping local terminology within corporate and security contexts. English serves not just as a common language that bridges global communication, but it also brings a wealth of new words that impact the language landscape in places where English isn't the primary language. This trend of Englishization, or anglicization, stems directly from globalization and technological progress, which have positioned English at the heart of international business, security, and knowledge sharing. This leads to English words often creeping into official documents, technical glossaries, and our daily interactions, changing local language practices in diverse and significant ways.

The journey of adopting English terminology is closely linked to the methods organizations employ to build trust and maintain consistency. In the world of multinational corporations and security agencies, language policies often elevate English to the status of the main corporate or operational language, highlighting its vital role in fostering connections across different countries. Adopting new language practices can be quite a challenge. Local actors often find themselves in a delicate dance between welcoming global English terms and protecting their own linguistic and cultural identities. This delicate balancing act can lead to different outcomes, such as acceptance, adaptation, or even resistance. These tensions expose the intricate social and power dynamics involved, demonstrating how language proficiency can significantly shape one's status, sense of belonging, and the fairness they find in institutions.

Incorporating English terms into local languages really hinges on effective translation and policy frameworks. Bilingual glossaries, translation standards, and cultural training for translators are all key elements that help bridge understanding and foster clearer communication. Still, despite these efforts, there's always a risk of ambiguity and misinterpretation, particularly when technical terms have varying meanings or when institutional objectives clash with local linguistic contexts. This really brings to light the need to consider the influence of English in a thoughtful and adaptable way. We should allow local terms to evolve while ensuring they remain clear and culturally meaningful.

In conclusion, this research emphasizes that English has a diverse and constantly evolving role in the realms of business and security. While it's essential for global communication and gaining institutional credibility, it also presents various challenges concerning identity, power, and equitable communication. To navigate

these challenges successfully, we need a thoughtful approach that embraces the advantages of English as a global language while also valuing and integrating local linguistic customs. This way, we can improve international teamwork and ensure that communication within organizations is inclusive and mindful of cultural nuances.

LITERATURE

- Baltezarević, I. & Baltezarević, R. (2020): “Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku”, *Megatrend revija*, 17(4), 27–40. DOI: 10.5937/MegRev2004027B
- Baltezarević, R. & Baltezarević, B. (2018): “The Impact of Video Games on the Formation of Esports”, *Facta Universitatis, Series: Physical Education and Sport*, 16(1), 137–147. DOI: 10.22190/FUPES170614012B
- Cornelissen, J. P., Durand, R., Fiss, P. C., Lammers, J. C., & Vaara, E. (2015): “Putting communication front and center in institutional theory and analysis”, *Academy of Management Review*, 40(1), 10–27.
- Global Interagency Security Forum (GISF) (2024): *GISF’s interactive glossary is released in four languages!*, <https://gisf.ngo/gisf-glossary-released-in-four-languages/>.
- Graddol, D. (1999): “The decline of the native speaker”, *AILA Review*, 13, 57–68.
- Green, S. E. (2004): “A rhetorical theory of diffusion”, *Academy of Management Review*, 29(4), 653–669.
- Hoffer, B. L. (2005): “Language borrowing and the indices of adaptability and receptivity”, *Intercultural Communication Studies*, 14(4), 53–68.
- ICESCO (2025): *Translation and Security Symposium Calls for Developing Technological and Linguistic Mechanisms, Fostering Complementarity between Security Agencies and Translators*, <https://icesco.org/en/2025/07/07/translation-and-security-symposium-calls-for-developing-technological-and-linguistic-mechanisms-fostering-complementarity-between-security-agencies-and-translators/>.
- Kosutic, D. (2025): *Glossary of information security and business continuity terms*, <https://advisera.com/27001academy/knowledgebase/glossary/>.
- Lawrence, T. B. (1999): “Institutional strategy”, *Journal of Management*, 25(2), 161–188.
- Leppänen, S., Pitkänen-Huhta, A., Nikula, T., Kytölä, S., Törmäkangas, T., Nissinen, K., Kääntä, L., Räisänen, T., Laitinen, M., Pahta, P., Koskela, H., Lähdesmäki, S. and Jousmäki, H. (2011): “National survey on the English language in Finland: Uses, meanings and attitudes”, *Studies of Variation, Contacts and Change in English*, Vol. 5. <http://www.helsinki.fi/varieng/journal/volumes/05/>.

- Lønsmann, D. (2015): "Language ideologies in a Danish company with English as a corporate language: 'it has to be English'", *Journal of Multilingual and Multicultural Development*, 36(4), 339–356.
- Masood, K. (2022): "English Competencies and Challenges for Data Science and Cyber Security Students at Al Istiqlal University", *The Creative Launcher*, 7(5), 48–68. DOI: 10.53032/tcl.2022.7.5.05
- Neeley, T. B. (2013): "Language matters: Status loss and achieved status distinctions in global organizations", *Organization Science* 24(2), 476–497.
- Neeley, T. B. & Dumas, T.L. (2016): "Unearned status gain: Evidence from a global language mandate", *Academy of Management Journal* 59(1), 14–43.
- Putnam, L., & Fairhurst, G. L. (2001): "Discourse analysis in organizations", In: F. M. Jablin & L. Putnam (Eds.): *Sage handbook of organizational communication* (pp. 78–136), Sage, London.
- Reiche, B. S. & Neeley, T. B. (2019): "Head, heart, or hands: How do employees respond to a radical global language change over time?", *Organization Science*, 30(6), 1252–1269. DOI: 10.1287/orsc.2019.1289
- Readle-app (2024): *Loan Words: English Words Used in Other Languages*, <https://readle-app.com/en/blog/loan-words-english-words-used-in-other-languages/>.
- Sanden, G. & Lønsmann, D. (2018): "Discretionary power on the front line: A bottom-up perspective on corporate language management", *European Journal of International Management*, 12(1/2), 111–137.
- Sanden, G. R. (2020): Language policy and corporate law: A case study from Norway, *Nordic Journal of Linguistics*, 43(1), 59–91. DOI: 10.1017/S0332586519000222
- Schirch, L. & Mancini-Griffoli, D. (2016): "Local Ownership in Security Report. Alliance for Peacebuilding / GPPAC", *Translating Language and Terminology*, <https://gppac.net/files/201901/Local%20Ownership%20in%20Security%20Report.%2015%20March%202016.pdf>.
- Suddaby, R., Bitektine, A. & Haack, P. (2017): "Legitimacy", *Academy of Management Annals*, 11(1), 451–478.
- Winford, D. (2003): *An introduction to contact linguistics*, Blackwell Publishing.

DIPLOMATSKE AKTIVNOSTI I UTICAJ ENGLESKOG JEZIKA NA LOKALNU TERMINOLOGIJU U BEZBEDNOSNOM I KORPORATIVNOM KONTEKSTU

Sažetak: Ovaj rad se bavi značajnim uticajem engleskog jezika na lokalnu terminologiju, posebno u oblastima diplomatije, bezbednosti i korporativnog okruženja. Ispitivanjem teorijskih okvira i primera iz stvarnog života, studija ilustruje da engleski jezik nije samo globalno sredstvo komunikacije, već i značajna snaga u transformaciji jezika koji se koristi u diplomatskim i institucionalnim kontekstima. Spaja institucionalne i lingvističke perspektive, posebno kroz prizmu Nove institucionalne teorije, kako bi se analiziralo kako jezik pomaže u izgradnji organizacionog legitimiteta i identiteta u diplomatskim okruženjima. Pored toga, istražuje leksičko pozajmljivanje, prevodilačke prakse i jezičke politike u višejezičnim kontekstima, bacajući svetlo na to kako se engleski termini vezani za diplomatiju, kao što su protokol, pregovori i bilateralni sporazum, kao i bezbednosni i korporativni koncepti poput zaštitnog zida (firewall) i upravljanja rizikom (risk management), usvajaju, modifikuju ili odbijaju na lokalnom nivou. Rezultati sugerišu da, iako uticaj engleskog jezika pomaže u stvaranju standardizovanijeg i efikasnijeg okvira za diplomatske i institucionalne dijaloge, on takođe pokreće važna pitanja o jasnoći, pravičnosti i kulturnom značaju. Na kraju krajeva, ovo istraživanje otkriva složen odnos između globalnog uticaja engleskog jezika i lokalnih jezičkih identiteta koji oblikuju diplomatske napore, bezbednosna pitanja i korporativnu komunikaciju.

Ključne reči: diplomatske aktivnosti, anglicizacija, institucionalna legitimnost, leksičko pozajmljivanje

Mirjana Ristić*
<https://orcid.org/0009-0001-3877-0153>

UDC: 343.983:004.8

Danilo Izgarević**
<https://orcid.org/0009-0000-0785-3055>

DOI: 10.5937/MegRev2502221R

Marko Stanojević***
<https://orcid.org/0009-0007-7241-5503>

Original scientific paper

Received 13.08.2025.

Approved 19.10.2025.

DIGITAL FORENSICS AND INFORMATION SECURITY IN THE ERA OF ARTIFICIAL INTELLIGENCE – EXPLORING NEW APPROACHES AND ETHICAL IMPLICATIONS

Abstract: *As our digital lives get more complex, the traces we leave behind have turned into a vast landscape of evidence, and potential threats. Digital forensics now faces challenges not just from the overwhelming amount of data but also from the clever tactics employed by cybercriminals. Traditional methods are struggling to keep up, which is where artificial intelligence (AI) and machine learning (ML) come into play. They provide automated triage, pattern recognition, anomaly detection, and multimedia analysis, all of which significantly enhance the speed, accuracy, and depth of investigations. With AI-enhanced tools, investigators can uncover hidden connections, identify fraudulent activities, and validate digital evidence across various networks, devices, and cloud platforms. While AI brings a lot of exciting possibilities, it also opens up a can of ethical and legal worms. We're talking about issues like algorithmic bias, privacy concerns, the need for explainability, and who's really accountable when it comes to decisions made in forensic contexts. In this review, we bring together the latest findings on AI in digital forensics, underlining its revolutionary possibilities and the critical need for ethical and responsible application.*

Keywords: *artificial intelligence (ai), information security, digital forensics, cybercrime, ethical implications*

* E-mail: ristic85@yahoo.com

** E-mail: daniloizgarevic@gmail.com

*** E-mail: stanojevic.marko799@gmail.com

INTRODUCTION

The landscape of digital forensics has changed dramatically in recent years, fueled by the rapid growth of digital data, increasingly complex cyber threats, and the swift evolution of artificial intelligence (AI) technologies. Traditional forensic approaches, which often depend on manual analysis and rule-based methods, can be inadequate for tackling the scale, complexity, and speed of modern investigations.¹ In contrast, artificial intelligence (AI) and machine learning (ML) provide exciting opportunities for automating triage, detecting anomalies, and correlating various digital artifacts, thereby enhancing both the efficiency and effectiveness of forensic processes.²

AI has opened up a world of innovative strategies in digital forensics. For instance, automated triage and prioritization help forensic analysts sift through massive amounts of evidence quickly, pinpointing crucial items for investigation while easing the burden on human resources.³ Techniques like supervised learning, clustering, and anomaly detection have shown great success in uncovering suspicious patterns that might slip under the radar.⁴ The fields of multimedia and image forensics have also seen advancements, with deep learning models, particularly convolutional neural networks (CNNs), being used to spot altered images, videos, and audio files.⁵ Moreover, AI boosts network and log analysis, making it possible to detect cyber intrusions, ransomware attacks, and insider threats in real-time.⁶ It plays a crucial role in gathering and organizing data from the dark web and social media through natural language processing.⁷

¹ Ragho, S. R., & Chaudhari, N. (2025): "Artificial intelligence in digital forensics: A review of cyber-attack detection models and frameworks", *Journal of Information Systems Engineering and Management*, 10(57s), 740–748. DOI: 10.5525/jise.2025.1057s

² Ramchandra, M., Pravin, H., & Pravin, S. (2024): "Digital forensics in the age of AI and ML: Evidence handling, validation and reporting", *Open Access Journal of Data Science and Artificial Intelligence*, 2(1), 1-5. DOI: 10.23880/oajda-16000132

³ Ibid

⁴ Nayerifard, T., Amintoosi, H., Ghaemi Bafghi, A., & Dehghantanha, A. (2023): "Machine learning in digital forensics: A systematic literature review [Preprint]", *arXiv*. DOI: 10.48550/arXiv.2306.04965

⁵ Billah, M. (2025): "Explainable AI for digital forensics: Ensuring transparency in legal evidence analysis", *Journal of Forensic Science & Research*, 9(2), 109–116. DOI: 10.29328/journal.jfsr.1001089

⁶ Ragho, S. R., & Chaudhari, N. (2025): "Artificial intelligence in digital forensics: A review of cyber-attack detection models and frameworks", *Journal of Information Systems Engineering and Management*, 10(57s), 740–748. DOI: 10.5525/jise.2025.1057s

⁷ Khindre, M., & Monga, D. (2023): "Role of artificial intelligence (AI) in digital forensic", *International Journal of Law, Policy and Social Review*, 5(4), 121–123. DOI: 10.5281/zenodo.1701685

However, despite all these advancements in technology, using AI in digital forensics presents a variety of ethical, legal, and procedural challenges. One of the biggest worries is algorithmic bias; if AI systems are trained on data that's biased or not representative, they might produce results that are skewed, which could undermine the fairness and reliability of forensic investigations.⁸ Privacy concerns are a big deal, especially since AI systems can handle massive amounts of personal information. This leads to concerns about surveillance and unauthorized access.⁹ Additionally, the intricate nature of AI models, especially deep learning systems, can make them hard to explain, which poses challenges for human decision-makers and courts trying to grasp how certain conclusions were drawn.¹⁰ Lastly, accountability and governance are critical issues; figuring out who is responsible for errors or misuse of AI involves various stakeholders, including software developers, forensic analysts, and organizations, underscoring the need for clear regulatory guidelines.¹¹

In this review, we're diving into the intriguing blend of digital forensics and AI. We'll explore the newest technical strategies and tackle the ethical and legal issues that arise. By weaving together recent research and pinpointing major hurdles, the paper aims to shed light on how we can responsibly and effectively weave AI into digital forensic investigations, ensuring we strike a balance between technological progress and the core values of fairness, transparency, and accountability.

LITERATURE REVIEW

The extensive use of digital technology in daily life has made people more vulnerable to online threats,¹² underscoring the need for cutting-edge AI-driven solutions to safeguard individuals and businesses. Interpol defines digital forensics as

⁸ Khalid, A. A., Syed, W. S., & Sayed, I. S. (2024): "Ethical challenges in forensic imaging: A systematic review of key issues, emerging artificial intelligence (AI) implications and future directions", *International Journal of Allied Health Sciences*, 8(5), <https://journals.iiu.edu.my/ijahs/index.php/IJAHS/article/view/995>.

⁹ Billah, M. (2025): "Explainable AI for digital forensics: Ensuring transparency in legal evidence analysis", *Journal of Forensic Science & Research*, 9(2), 109–116. DOI: 10.29328/journal.jfsr.1001089

¹⁰ Nayerifard, T., Amintoosi, H., Ghaemi Bafghi, A., & Dehghantanha, A. (2023): "Machine learning in digital forensics: A systematic literature review [Preprint]", *arXiv*. DOI: 10.48550/arXiv.2306.04965

¹¹ Khindre, M., & Monga, D. (2023): "Role of artificial intelligence (AI) in digital forensic", *International Journal of Law, Policy and Social Review*, 5(4), 121–123. DOI: 10.5281/zenodo.1701685

¹² Baltezarevic, R., & Baltezarevic, I. (2021): "The dangers and threats that digital users face in cyberspace", *IPSI Transactions on Internet Research*, 17(1), 47–53.

a specialised area of forensic science with an emphasis on electronic data. The task of extracting, identifying, storing, analysing, and reporting digital data that may be pertinent to an inquiry falls to digital forensic scientists, and the recent growth of digital data has made it increasingly difficult to finish these investigations. AI in digital forensics, according to many forensic specialists, has the potential to completely transform the field and improve the efficacy and efficiency of digital forensic investigations.¹³

The growing integration of advanced technologies into everyday life is rapidly reshaping the e-society, even as it opens new vulnerabilities and shifts how we understand digital interaction and security.¹⁴ In order to gather digital evidence and investigate cybercrimes, digital forensics has become essential. However, conventional forensic techniques face serious difficulties due to the exponential increase in digital data volume as well as its growing complexity and diversity. With extensive data analysis, pattern recognition, and process automation capabilities that far surpass human capabilities, artificial intelligence (AI) has emerged as a potent and revolutionary tool to address these difficulties.¹⁵ Because AI technology can analyse network data and spot suspicious patterns that enable investigators to monitor and trace cybercriminals, it can assist investigators quickly become aware of common cybercrimes including hacking, malware attacks, and online fraud.¹⁶

It is impossible to exaggerate the significance of AI in digital forensics. Cybercriminals use ever-more-advanced methods to hide their actions. Investigators can use AI to find hidden patterns, identify abnormalities, and draw connections that might otherwise go unreported. Additionally, AI's capacity to automate a large portion of the forensic process frees up human specialists to concentrate on more difficult analytical tasks, improving the overall efficacy and efficiency of investigations.¹⁷ Researchers are looking into how AI may improve digital forensic procedures. Ganesh highlights how machine learning may speed up the examination of evidence, find anomalies in databases, and automate repetitive jobs, increasing the

¹³ Gaona, J. (2024): *The Role of AI in Forensics*, <https://marymount.edu/blog/the-role-of-ai-in-forensics/>.

¹⁴ Safieddine, F., & Baltezarević, R. (2016): "Advances in technologies evolving new dimensions in e-society", In: *The Internet as a tool of modern business and communication* (pp. 43–75), Lap Lambert Academic Publishing, Saarbrücken - Germany.

¹⁵ Li, G., Wang, J., & Wang, X. (2023): "Construction and path of urban public safety governance and crisis management optimization model integrating artificial intelligence technology", *Sustainability*, 15(9), Article 7487. DOI: 10.3390/su15097487

¹⁶ Gaona, J. (2024): *The Role of AI in Forensics*, <https://marymount.edu/blog/the-role-of-ai-in-forensics/>.

¹⁷ Dehghantanha, A., & Franke, K. (2019): "Privacy-preserving investigative machine learning in digital forensic", *Digital Investigation*, 29, 104–114.

effectiveness and scalability of investigative procedures. The use of AI in conjunction with forensic technologies is becoming increasingly common as its predictive analysis and pattern recognition capabilities improve.¹⁸

By improving efficiency, accuracy, and overall investigative outcomes, artificial intelligence is revolutionising the analysis of forensic evidence in criminal investigations.¹⁹ The transition from traditional digital forensics to intelligent forensics emphasises the necessity of systems for gathering, storing, and automatically analysing, comprehending, and connecting evidence. Irons and Lallie recommend intelligent forensics, which uses AI technologies to automate and use expert knowledge to make forensic choices. This makes it simpler to identify intricate danger patterns and reduces the number of errors analysts make in hectic settings.²⁰

DNA analysis, pattern recognition, crime scene reconstruction, and digital forensics are among the forensic uses of AI.²¹ AI technologies can increase the accuracy of object identification and facial recognition while cutting processing time for critical forensic tasks by up to 93%.²² The examination of large data sets is one of the most beneficial uses of AI in digital forensics. AI tools allow investigators to swiftly uncover crucial evidence in investigations involving numerous desktop computers, laptops, and mobile devices that hold terabytes of text, audio, and video data, greatly cutting down on the amount of time needed to resolve cases. In financial crime investigations, AI helps investigators uncover fraudulent activities, such as money laundering, by analyzing massive volumes of transactional data. Faster and more accurate criminal detection is made possible by the capacity to identify complicated and suspicious activities, which is a crucial advantage over manual analysis. In the meantime, detectives may see links between people and their travels across many platforms with the aid of AI-powered crime-mapping tools. In operations to dismantle organised crime networks, where comprehending

¹⁸ Anghel, C. (2019): "Digital forensics: A literature review", *The Annals of "Dunarea de Jos" University of Galati, Fascicle III: Electrotechnics, Electronics, Automatic Control, Informatics*, 42, 23–27.

¹⁹ Das, S. S., Patnaik, S., Pattnayak, P., & Mohanty, A. (2023): "An advancement in forensic and criminal investigation through artificial intelligence", In: *2023 OITS International Conference on Information Technology (OCIT)* (pp. 920–926), IEEE. DOI: 10.1109/OCIT58482.2023.10448291

²⁰ Lovanshi, M., & Bansal, P. (2019): "Comparative study of digital forensic tools", In: R. (Ed.): *Data, engineering and applications* (Vol. 2, pp. 195–204), Springer.

²¹ El-Din, E. (2022): "Artificial intelligence in forensic science: Invasion or revolution?", *Egyptian Society of Clinical Toxicology Journal*. DOI: 10.21608/esctj.2022.158178.1012

²² RizwanBasha, A., & Annamalai, R. (2024): "Transforming crime scene investigations through the integration of artificial intelligence in digital forensics", In: *2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS)* (pp. 1–6), IEEE. DOI: 10.1109/IICCCS60115.2024.10594829

and mapping interconnections and connections between suspects is crucial to developing a thorough case, this analytical aptitude is extremely helpful.²³

One of the main ways AI aids in digital forensics is through automation. AI technology makes it possible to quickly prioritise data, sort hazards, and provide a comprehensive schedule. However, because forensic science places a strong focus on establishing evidence and getting it accepted in court, it can be challenging to understand these models.²⁴ Additionally, forensic sciences should employ explainable AI (XAI) techniques to guarantee the transparency of model results and reports.²⁵ Cutting-edge digital forensics solutions go beyond traditional data recovery, combining AI to examine evidence from mobile devices, PCs, and cloud-based sources. With the help of this creative method, investigators may easily create thorough reports and exhibits that are ready for the trial while sorting through enormous volumes of digital data to find pertinent details and digital artefacts. AI-enhanced technologies prioritise the identification and analysis of verifiable, probative evidence while offering specialised skills to help investigators find and record altered content. AI solutions enable agencies to confidently analyse and create presentations that are fit for court by confirming the legitimacy of audio, video, and image assets. With agencies accepting more media files from the public via digital tip lines and having to differentiate between authentic evidence and altered content, this technology is extremely important.²⁶

Ethical and legal issues must also be addressed by AI and ML in forensic reporting. The application of AI should guarantee that the assessments are objective and considerate of privacy. This is made possible by explainable AI, which addresses possible ethical concerns by making the decision-making process visible. For AI-driven forensic reports to be accepted and legitimate in court, they must comply with legal requirements.²⁷ Improving security and safeguarding data privacy are crucial aspects of a digital forensic investigation. Strong data protection

²³ Amick, T. (2025): *How AI Is Revolutionizing Digital Forensics*, <https://www.policechiefmagazine.org/ai-is-revolutionizing-digital-forensics-magnet/>.

²⁴ Costantini, S., De Gasperis, G., & Olivieri, R. (2019): "Digital forensics and investigations meet artificial intelligence", *Annals of Mathematics and Artificial Intelligence*, 86, 193–229. DOI: 10.1007/s10472-019-09644-2

²⁵ Mitchell, F. (2010): "The use of artificial intelligence in digital forensics: An introduction", *Digital Evidence and Electronic Signature Law Review*, 7, 35–39. DOI: 10.14296/deeslr.v7i0.2242

²⁶ Amick, T. (2025): *How AI Is Revolutionizing Digital Forensics*, <https://www.policechiefmagazine.org/ai-is-revolutionizing-digital-forensics-magnet/>.

²⁷ Thorat, O., Parekh, N., & Mangrulkar, R. S. (2021): "TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification", *International Journal of Information Management Data Insights*, 1(2), 100048.

procedures and ethical standards must be in place since digital investigations include the extraction and analysis of vast volumes of digital data.²⁸

However, AI has the potential to completely change the field of digital forensics by revolutionising the handling and analysis of digital evidence. The more effective data processing of AI eventually increases the cyber detection and investigation process in an effort to keep up with huge volumes of data to investigate and remediate. However, forensic specialists need to be cautious of the difficulties associated with using AI. There is no indication that AI will go away, and the area of digital forensics needs to be prepared for any new ramifications that AI may bring. The government is currently beginning to incorporate AI.²⁹ Implementing AI in law enforcement helps create a better and more secure society by reducing case backlogs and speeding up the administration of justice. In terms of company security, it minimises the financial and reputational harm brought on by outages and data breaches by reducing the time required to investigate and mitigate cyber incidents.³⁰

CONCLUSION

The way we conduct cyber investigations is undergoing a major transformation with the integration of artificial intelligence into digital forensics. With tools like machine learning, deep learning, and natural language processing, AI boosts the efficiency, accuracy, and scalability of forensic work. It automates the triage of evidence, identifies anomalies, and uncovers hidden patterns that might elude human analysts. Furthermore, AI enables a more advanced analysis of multimedia, network data, and financial transactions, allowing investigators to tackle sophisticated cybercrime more effectively.

At the same time, embracing AI in digital forensics brings along a host of ethical, legal, and procedural hurdles. We need to tackle issues like algorithmic bias, privacy, explainability, and accountability head-on to make sure that AI-driven forensic analyses are not only transparent and fair but also legally sound. The field needs to navigate the exciting possibilities that AI offers while staying true to the core principles of justice and ethical practice.

²⁸ Gaona, J. (2024): *The Role of AI in Forensics*, <https://marymount.edu/blog/the-role-of-ai-in-forensics/>.

²⁹ Cortado, J. (2024): *How AI Quakes the Digital Forensics Landscape*, <https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summaries/how-ai-quakes-the-digital-forensics-landscape/>.

³⁰ Gubanov, Y. (2025): *Revolutionizing Investigations: The Impact of AI in Digital Forensics*, <https://www.cyberdefensemagazine.com/revolutionizing-investigations-the-impact-of-ai-in-digital-forensics/>.

In closing, while artificial intelligence brings a wealth of exciting opportunities to enhance digital forensic capabilities, its responsible and effective use requires a commitment to ongoing research, clear regulations, and continuous education for those in the forensic field. By keeping these important factors in mind, AI can transform into a powerful tool for improving digital security, supporting law enforcement, and safeguarding the interests of both individuals and organizations in our ever-evolving digital world.

LITERATURE

- Amick, T. (2025): How AI Is Revolutionizing Digital Forensics. <https://www.policechiefmagazine.org/ai-is-revolutionizing-digital-forensics-magnet/>.
- Anghel, C. (2019): "Digital forensics: A literature review", *The Annals of "Dunarea de Jos" University of Galati, Fascicle III: Electrotechnics, Electronics, Automatic Control, Informatics*, 42, 23–27.
- Baltezarevic, R., & Baltezarevic, I. (2021): "The dangers and threats that digital users face in cyberspace", *IPSI Transactions on Internet Research*, 17(1), 47–53.
- Baltezarević, B., Baltezarević, R., & Baltezarević, V. (2018). Aktivnosti starijih osoba na onlajn društvenim mrežama. *Megatrend revija*, 15(3), 157–172.
- Billah, M. (2025): "Explainable AI for digital forensics: Ensuring transparency in legal evidence analysis", *Journal of Forensic Science & Research*, 9(2), 109–116. DOI: 10.29328/journal.jfsr.1001089
- Cortado, J. (2024): *How AI Quakes the Digital Forensics Landscape*, <https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summaries/how-ai-quakes-the-digital-forensics-landscape/>.
- Costantini, S., De Gasperis, G., & Olivieri, R. (2019): "Digital forensics and investigations meet artificial intelligence", *Annals of Mathematics and Artificial Intelligence*, 86, 193–229. DOI: 10.1007/s10472-019-09644-2
- Das, S. S., Patnaik, S., Pattanayak, P., & Mohanty, A. (2023): "An advancement in forensic and criminal investigation through artificial intelligence", In: *2023 OITS International Conference on Information Technology (OCIT)* (pp. 920–926), IEEE. DOI: 10.1109/OCIT58482.2023.10448291
- Dehghantanha, A., & Franke, K. (2019): "Privacy-preserving investigative machine learning in digital forensics", *Digital Investigation*, 29, 104–114.
- El-Din, E. (2022): "Artificial intelligence in forensic science: Invasion or revolution?", *Egyptian Society of Clinical Toxicology Journal*. DOI: 10.21608/esctj.2022.158178.1012
- Gaona, J. (2024): *The Role of AI in Forensics*, <https://marymount.edu/blog/the-role-of-ai-in-forensics/>.

- Gubanov, Y. (2025): *Revolutionizing Investigations: The Impact of AI in Digital Forensics*, <https://www.cyberdefensemagazine.com/revolutionizing-investigations-the-impact-of-ai-in-digital-forensics/>.
- Khalid, A. A., Syed, W. S., & Sayed, I. S. (2024): "Ethical challenges in forensic imaging: A systematic review of key issues, emerging artificial intelligence (AI) implications and future directions", *International Journal of Allied Health Sciences*, 8(5), <https://journals.iium.edu.my/ijahs/index.php/IJAHS/article/view/995>.
- Khindre, M., & Monga, D. (2023): "Role of artificial intelligence (AI) in digital forensic", *International Journal of Law, Policy and Social Review*, 5(4), 121–123. DOI: 10.5281/zenodo.1701685
- Li, G., Wang, J., & Wang, X. (2023): "Construction and path of urban public safety governance and crisis management optimization model integrating artificial intelligence technology", *Sustainability*, 15(9), Article 7487. DOI: 10.3390/su15097487
- Lovanshi, M., & Bansal, P. (2019): "Comparative study of digital forensic tools", In: R. (Ed.), *Data, engineering and applications* (Vol. 2, pp. 195–204), Springer.
- Mitchell, F. (2010): "The use of artificial intelligence in digital forensics: An introduction", *Digital Evidence and Electronic Signature Law Review*, 7, 35–39. DOI: 10.14296/deeslr.v7i0.2242
- Nayerifard, T., Amintoosi, H., Ghaemi Bafghi, A., & Dehghantanha, A. (2023): "Machine learning in digital forensics: A systematic literature review [Preprint]", *arXiv*. DOI: 10.48550/arXiv.2306.04965
- Ragho, S. R., & Chaudhari, N. (2025): "Artificial intelligence in digital forensics: A review of cyber-attack detection models and frameworks", *Journal of Information Systems Engineering and Management*, 10(57s), 740–748. DOI: 10.5525/jise.2025.1057s
- Ramchandra, M., Pravin, H., & Pravin, S. (2024): "Digital forensics in the age of AI and ML: Evidence handling, validation and reporting", *Open Access Journal of Data Science and Artificial Intelligence*, 2(1), 1-5. DOI: 10.23880/oajda-16000132
- RizwanBasha, A., & Annamalai, R. (2024): "Transforming crime scene investigations through the integration of artificial intelligence in digital forensics", In: *2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS)* (pp. 1–6), IEEE. DOI: 10.1109/IICCCS60115.2024.10594829
- Safieddine, F., & Baltezarević, R. (2016): "Advances in technologies evolving new dimensions in e-society", In: *The Internet as a tool of modern business and communication* (pp. 43–75), Lap Lambert Academic Publishing, Saarbrücken - Germany..
- Thorat, O., Parekh, N., & Mangrulkar, R. S. (2021): "TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification", *International Journal of Information Management Data Insights*, 1(2), 100048.

DIGITALNA FORENZIKA U ERI VEŠTAČKE INTELEGENCIJE - ISTRAŽIVANJE NOVIH PRISTUPA I ETIČKIH IMPLIKACIJA

Sažetak: *Kako naši digitalni životi postaju složeniji, tragovi koje ostavljamo za sobom pretvorili su se u ogroman pejzaž dokaza i potencijalnih pretnji. Digitalna forenzika se sada suočava sa izazovima ne samo zbog ogromne količine podataka, već i zbog pametnih taktika koje koriste sajber kriminalci. Tradicionalne metode teško uspevaju da održe korak, i tu na scenu stupaju veštačka inteligencija (AI) i mašinsko učenje (ML). Oni pružaju automatizovanu selekciju podataka, prepoznavanje obrazaca, otkrivanje anomalija i multimedijalnu analizu, što značajno poboljšava brzinu, tačnost i dubinu istraga. Uz AI unapređene alate, istražitelji mogu otkriti skrivene veze, identifikovati prevarne aktivnosti i validirati digitalne dokaze na različitim mrežama, uređajima i platformama u oblaku. Iako AI donosi mnogo uzbudljivih mogućnosti, ona takođe otvara i pitanja etike i prava. Govorimo o pitanjima poput algoritamske pristrasnosti, zabrinutosti za privatnost, potrebe za objašnjivošću i ko je zaista odgovoran kada su u pitanju odluke donete u forenzičkim kontekstima. U ovom pregledu objedinjujemo najnovija saznanja o AI u digitalnoj forenzici, ističući njene revolucionarne mogućnosti i kritičnu potrebu za etičkom i odgovornom primenom.*

Ključne reči: *veštačka inteligencija (ai), digitalna forenzika, sajber kriminal, etičke implikacije*

SIGURNOST ADS-B AVIO SISTEMA: ANALIZA LJUDSKIH FAKTORA

Apstrakt: *Automatic Dependent Surveillance – Broadcast (ADS-B) je jedan od značajnih sistema, koji omogućava ostvarivanje sigurnijeg/bezbednijeg i efikasnijeg sistema vazdušnog prostora. Pored brojnih prednosti, kao što su jednostavna implementacija, jeftin hardver i velika tačnost pozicioniranja, ovaj bežični komunikacioni protokol ima i nekoliko veoma važnih nedostataka, a to su zavisnost od sistema satelitske navigacije (koji može biti fizički oštećen, korumpiran ili izložen interferencijama) i veoma jednostavan protokol, a koji ne obezbeđuje autentifikaciju i enkripciju. Tako, osim što su realne, pretnje po sajber bezbednost ADS-B sistema su i u konstantnom porastu. Pri svemu tome, veoma važan aspekt korišćenja ADS-B jeste ljudski faktor, a koji se u avijaciji najčešće odnosi na aspekte ljudske greške u avio-nesrećama i kvarovima avio sistema. Kako ADS-B obezbeđuje podatke iz kojih se mogu izvesti brojne napredne aplikacije, tako implementacija nove ADS-B opreme i procedura proširuje spektar pitanja u vezi sa ljudskim faktorom, kao što je razumevanje upotrebe automatizovanih on-board sistema, a koji postaju sve kompleksniji. Zbog toga je od velikog značaja analiza sigurnosti ADS-B sistema, tj. razmatranje potencijalnih opasnosti i analiziranje istih, primenom određenih metodoloških pristupa, kao što je Preliminary Hazard Analysis (PHA), tj. Preliminarna Analiza Opasnosti/Stabla Grešaka. Ovakav pristup bazira se na analizi opasnosti koje se identifikuju u preliminarnoj listi opasnosti i identifikaciji prethodno neprepoznatih opasnosti u ranoj fazi razvoja sistema, u cilju davanju preporuka za sprečavanje/ublažavanje identifikovanih opasnosti.*

Ključne reči: *ADS-B, civilna avijacija, ljudski faktor, preliminarna analiza opasnosti, sigurnost, bezbednost*

* Fakultet za civilno vazduhoplovstvo, Megatrend Univerzitet, Beograd, Srbija
E-mail: dejankozovic@gmail.com

** Fakultet za civilno vazduhoplovstvo, Megatrend Univerzitet, Beograd, Srbija
E-mail: ddjurdjevic@megatrend.edu.rs

1. UVOD

U težnji za postizanjem sve većih zahteva u vezi sa kapacitetom vazdušnog prostora, smanjenjem operativnih troškova, zagušenjem u avio-saobraćaju, ekološkim zahtevima, itd., uz istovremeni porast sigurnosti i bezbednosti, Federalna uprava za vazduhoplovstvo (FAA) i Evropska organizacija za bezbednost vazdušne plovidbe (EUROCONTROL) uvele su (NextGen)¹ i SESAR² programe, u cilju modernizacije *Air Traffic Management*-a (ATM)-a i poboljšanja slanja/prijema digitalnih informacija. Njihov integralni deo je razvoj *Automatic Dependent Surveillance – Broadcast* (ADS-B), kao i potpuna integracija ovog navigacionog sistema u svrhu smanjenja zavisnosti avio-sistema od skupe i zastarele radarske opreme. Tako, ADS-B-u je dodeljen poseban ASTERIX (All Purpose Structured EUROCONTROL Surveillance Information Exchange) protocol kategorije 21, za razmenu informacija u vazduhoplovstvu.

Transformišući sve segmente avijacije, ADS-B je danas preferirani metod nadzora, koji nudi brojne benefite i Kontrolu vazdušnog saobraćaja (ATC) i pilotima, kao što je značajan porast *situational awareness* letačke posade i efikasniju operativnost kontrolora letenja. Pored toga, u odnosu na tradicionalne radarske sisteme, ADS-B smanjuje troškove postavljanja i održavanja sistema, značajno povećavajući pokrivenost područja³.

Međutim, ADS-B sistem ima i određene slabosti – nedostatak integriteta i autentičnosti u emitovanim tekstualnim porukama, povećavaju ranjivost ovog sistema na različite vrste sajber-fizičkih napada. Iako se smatra da primena ADS-B ne dovodi do porasta bezbednosnog rizika po avio-sisteme, u kontekstu unapređenja komunikacije korišćenjem vazduhoplovnih mreža, uvođenjem COTS (*Commercial-Off-The-Shelf*) komponenata, kao i široka upotreba IoT uređaja⁴ (internet stvari), predstavljaju rizik po sajber bezbednost jer mogu dovesti do ugrožavanja integriteta/dostupnosti podataka. Sajber bezbednosne pretnje nisu samo pretpostavka, već su neke i realizovane. U radovima autora Kožovića⁵ i Đurđevića⁶, dat je pregled objavljenih sajber incidenata i potencijalnih ranjivosti avio sistema, kao i predočene slabosti različitih avio sistema (npr. *Global positioning system*, GPS, odnosno *Global Navigation Satellite System*, GNSS, *Instrument Landing System*,

¹ NextGen - *Next Generation Air Transportation System*.

² SESAR - *Single European Sky Air Traffic Management Research*.

³ FAA (2025): *Automatic dependent surveillance – broadcast (ADS-B)*.

⁴ Stevanović, D. M., Đurđević, D. (2016): "internet stvari, lična i materijalna bezbednost", *Bezbednost*, 3/2016, 113-128.

⁵ Kožović, D. (2023): *Multidisciplinarni aspekti sajber bezbednosti avio sistema ADS-B*, doktorska disertacija, Fakultet za civilno vazduhoplovstvo, Megatrend univerzitet, Beograd.

⁶ Kožović, D., Đurđević, D. (2019): "Sajber bezbednost u avijaciji", *Megatrend revija*, 16(2)/2019, 39-56.

ILS⁷ i *Traffic Alert and Collision Avoidance System*, TCAS), a koji mogu biti ugroženi lažiranjem, tj. spufingom podataka⁸, veoma opasnim oblikom sajber napada čiji je cilj produkcija lažnih informacija/poruka (pogrešna pozicija/vremensko određenje).

S druge strane, kako ADS-B oprema može imati različite interfejsse s pilotima (od jednostavnog, do upravljačkog interfejsa naprednih karakteristika), veoma važan aspekt implementacije ADS-B jeste ljudski faktor, tj. odnos između ADS-B sistema i korisnika (pilota ili kontrolora letenja), kao i uloga koju ljudski faktor ima u odbrani od sajber napada.

Svakako, upotreba automatizovanih sistema, kao što je ADS-B, i generalno, veštačke inteligencije (AI), tj. povećanje automatizacije i razmene podataka, uključujući sajber-fizičke sisteme, IoT i računarstvo u oblaku, otvaraju širok spektar pitanja/barijera, a koja su u vezi sa tehnologijom (komunikacija i prikupljanje podataka, sajber-fizička bezbednost, donošenje odluka pomoću adaptivnih/nedeterminističkih sistema, integracija ljudi i mašina, itd), sertifikacijom i regulacijom (pristup vazдушnom prostoru za bespilotne letelice, proces sertifikacije, ekvivalentan nivo bezbednosti, poverenje u adaptivne/nedeterminističke IA sisteme, itd.), kao i s pravnim i društvenim pitanjima. Svaka od barijera se preklapa sa jednom ili više drugih, a njihovo prevazilaženje ne može biti izolovano, već je uslovljeno i podržano uspešnim rešavanjem svake od identifikovanih pojedinačnih barijera. Na primer, primena naprednih tehnologija u civilnom vazduhoplovstvu uslovljena je adekvatno završenim procesom sertifikacije; slično tome, napredne tehnologije mogu biti sertifikovane, samo ukoliko postoje robusni procesi verifikacije, a koji podržavaju razvoj tehnologije i sertifikaciju.

2. ADS-B TEHNOLOGIJA – KRATKI PREGLED

Jedan od gigantskih koraka u modernizaciji i poboljšanju kvaliteta bazduhoplovnih operacija predstavljalo je uvođenje *Automatic Dependent Surveillance-Broadcast* (ADS-B) – multiparametarskog sistema za nadzor, uvedenog od strane FAA i EASA (*European Union Aviation Safety Agency*). To je zavisano i kooperativan sistem za nadzor kod koga ADS-B transponder⁹ instaliran u avionu korišćenjem

⁷ Sathaye, H., Schepers, D., Ranganathan, A., Noubir, G. (2019): "Wireless attacks on aircraft instrument landing systems", in: 28th *USENIX Security Symposium*, August 14–16, 2019, Santa Clara, CA, USA, 1-16.

⁸ Pierpaoli, P., Egerstedt, M., Rahmani, A. (2015): "Altering UAV flight path by threatening Collision", in: *Digital Avionics Systems Conference (DASC)*, 2015 *IEEE/AIAA 34th* (2015), IEEE, 4A4-1-4A4-10.

⁹ Transponder (XPDR, XPNDR, TPDR или TP) je prijemnik/predajnik u avionu koji generiše odgovor/signal, nakon određenog upita; upit i odgovor su na različitim frekvencijama (dodekuje ih Međunarodna organizacija civilnog vazduhoplovstva, ICAO). Avio transponderi

SatNav (*Satellite Navigation*) tehnologije (GPS/GNSS), periodično razmenjuje (prenosi i prima) važne informacije s ATC i drugim avionima u neposrednoj okolini. Dakle, suština funkcionisanja ADS-B sistema sadržana je njegovom akronimu: *Automatic* – periodično prenosi informacije bez ikakve kontrole, tj. učešća pilota/operatera, *Dependent* – prenosi informacije koje se odnose na poziciju i vektor brzine dobijene od GPS/FMS (*Flight Management System*) i navigacione avionike, *Surveillance* – obezbeđuje metod za određivanje trodimenzionalne pozicije i identifikaciju aviona, ili drugih prevoznih sredstava i *Broadcast* - prenosi informacije (identitet, položaj, brzina, itd.) koje su dostupne svima, a koji imaju odgovarajuću opremu za prijem.

ADS-B ima dve različite funkcije: ADS-B Out i ADS-B In. ADS-B Out omogućava emitovanje informacija o avionu, kao što su identifikacija aviona i pozicija u realnom vremenu, visina i brzina, tj. ADS-B Out automatski prenosi parametre leta iz aviona do ATC na Zemlji, kao i do drugih aviona u neposrednoj okolini. ADS-B In omogućava prijem informacija o saobraćaju i meteorološkim uslovima od drugih aviona u neposrednoj okolini, značajno poboljšavajući svest pilota o situaciji, obezbeđujući pristup skoro identičnim podacima kojima raspolaže ATC. ADS-B Out je zahtevani globalni standard od 2022. godine (finalna odluka FAA i EASA kojom je ADS-B obavezni standard u Americi, Australiji i Evropi), dok je ADS-B In opcionalna usluga. Svaki avion može imati i "Out" i "In" mogućnosti, u zavisnosti od vrste transpondera koji je instaliran u avionu. Iako se smatra da istovremena primena ADS-B In s drugim sistemima¹⁰ omogućava povećanje bezbednosti, efikasnosti i kapaciteta vazdušnog prostora, bolje upravljanje, kao i kontrolu nekih operacija u uslovima velike gustine vazdušnog saobraćaja (npr. integracije ADS-B In i *Trajectory-Based Operations*), ADS-B ostaje opcionalna usluga, primarno usled visokih troškova implementacije, specifičnih standarda opreme, kao i zahteva za kokpit.

Pored zavisnosti od navigacionog sistema (GPS je najšire korišćeni), ADS-B značajno zavisi i od vrste komunikacionih sistema. Koriste se tri vrste *data* linikova, tj. protokola: 1090-ES, UAT i VDL-M4, u zavisnosti od vrste vazduhoplova, a najčešće se koristi 1090-ES; ADS-B Out šalje poruke svake sekunde brzinom 1 Mbit/s preko 1090-ES ili UAT¹¹.

Svaka ADS-B poruka sadrži preambulu¹² (8 μ s) i 56-bitni (kratki) ili 112-bitni (prošireni) blok podataka, koji se prenose automatski (bez ispitivanja od strane

moгу biti različitog režima rada: *Mode A* (šalje identifikacioni kod), *Mode C* (omogućava kontroloru automatsko očitavanje visine i nivoa leta) i *Mode S* (uključuje *Mode A* i *Mode C* i daje automatsku identifikaciju i podatke o visini vazduhoplova, kao i statusu leta.

¹⁰ McLean D. (2003): "Operational Requirements for Fully Automatic Flight", *Aircr. Eng. Aerosp. Technol.*, 75(6)/2003, 570–574.

¹¹ Pavić A., Lalić B., Đurđević M. (2014): Osnove ADS-B tehnologije i osmatranje područja Republike Srbije bez radarske pokrivenosti", *Zbornik radova Infoteh-Jahorina*, 13, 419–424.

¹² Preambula je inicijalni impuls (signal), koji se u mrežnim komunikacijama, koristi za sinhronizaciju vremena prenosa između dva ili više Sistema.

zemaljskih stanica) SSR transponderom (povezanim s različitim izvorom podataka). ADS-B poruke nisu enkriptovane (šifrovane): poslednja 24 bita uključuju proveru pariteta koja detektuje i ispravlja greške u prenosu poruka. Tako, zbog nedostatka enkripcije, kao i autentifikacije, ADS-B može biti meta različitih vrsta sajber napada, kao što su ometanje i uskraćivanje usluga, prisluškivanje, ubacivanje/reprodukovanje poruke, manipulacija porukama i lažiranje. Poslednje pomenuti, veoma je opasan¹³ – u napadu lažiranjem poruke (spufing napad) predajnik emituje lažne signale, tj. signale koji se razlikuju od autentičnih satelitskih signala, tako da vazduhoplov preko ADS-B šalje pogrešne informacije o svom položaju. Iako se smatra najteže izvodljivim, spufing ADS-B sistema (kao i GPS) postaje sve realnije, usled veoma brzog napretka jeftinih SDR (*Software Defined Radio*) platformi. S druge strane, porast upotrebe bezpilotnih letilica (*Unmanned Aerial Systems*, UAS/dronova) i GPS-a za njihovu navigaciju, otvara prostor za eventualnu primenu za izvođenje spufing napada iz vazduha u cilju otmice/distrikcije bezbednosti nadzora vazdušnog saobraćaja.

Iako avio sistem može biti izložen različitim vrstama sajber napada⁵, a potencijalno i spufingu, primenom različitih protiv-mera za sajber bezbednosnu zaštitu, kao što su metode koje se baziraju na algoritmima mašinskog učenja (npr. model dubokog učenja, tj. veštačka inteligencija¹⁴), ovi napadi mogu se značajno ublažiti. S druge strane, piloti, kao poslednja linija odbrane, osposobljeni su da detektuju i rešavaju različite operativne probleme. Ipak, zbog mogućih suptilnijih/naprednijih oblika sajber napada na sektor avijacije, različite organizacije, kao što su Međunarodna organizacija civilnog vazduhoplovstva (ICAO), Radio-tehnička komisija za aeronautiku (RTCA) i Evropska organizacija za opremu civilnog vazduhoplovstva (EUROCAE), proaktivno se bave povećanjem robusnosti GPS/GNSS/ADS-B sistema na različite vrste sajber napada¹⁵. Na primer, aktuelni pravac u okviru RTCA i EUROCAE za povećanje bezbednosne sigurnosti GNSS-a na rizik od spufinga, jeste uvođenje novih zahteva za sertifikovanu avio opremu, tj. za otkrivanje lažnih GNSS signala, u cilju korišćenja alternativne navigacione opreme, bez značajnog smanjenja bezbednosti/sigurnosti.

¹³ Kožović, D., Đurđević, D. (2021): "Spufing u civilnoj avijaciji: Bezbednost i sigurnost GPS/GNSS i ADS-B sistema", *Megatrend revija*, 18(3)/2021, 281-306.

¹⁴ Ying X., Mazer J., Bernieri G., Conti M., Buschell L., Poovendran R. (2019): "Detecting ADS-B spoofing attacks using deep neural networks", in *Proceeding of the IEEE Conference on Communications and Network Security (CNS2019)*, Washington D.C., USA, 9 p.

¹⁵ Hegarty C., Shallberg K., Walter T., Alexander K. (2018): "Spoofing detection for airborne GNSS equipment", in *Proceedings of 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, Miami, Florida, USA, 1350–1368.

3. IMPEMENTACIJA ADS-B: LJUDSKI FAKTOR

Uvođenje ADS-B aplikacija u vazduhoplovne operacije, obuhvata mnogobrojne aspekte, a jedan od veoma značajnih jeste aspekt integracije ljudi i mašina, tj. interakcije ljudi s automatizovanim *on-board* sistemima. Ovi sistemi postaju sve napredniji, kao i kompleksniji; viši nivoi automatizacije/autonomije zahtevaju dodatne softvere, procesore i senzore, a dodatne komunikacije, bežično povezivanje i opcije za zabavu putnika tokom leta doprinose složenosti ovih sistema. Zbog svega toga, od veoma velikog značaja je analiza i rešavanje bezbednosnih/sigurnosnih pitanja¹⁶.

Generalno, analiza ljudskog faktora odnosi se na razumevanje ljudskog ponašanja i ljudskih performansi. Primenjena na operacije u vazduhoplovstvu, ova analiza razmatra ljudske faktore u cilju optimizacije integracije ljudi i sistema, koje oni koriste ili u kojima rade, Ova optimizacija podrazumeva povećanje bezbednosti i performansi, tj. smanjenje pojava i uticaja ljudske greške u avio-sistemima i poboljšanje ljudskih performansi.

Dakle, veoma značajan aspekt korišćenja ADSB tehnologije jeste način na koji različiti korisnici (piloti, kontrolori i dispečari) mogu efikasno koristiti ADS-B podatke/informacije u okviru svojih relevantnih odgovornosti. Pored prihvatanja i korišćenja ADS-B tehnologije od strane pilota i kontrolora, to podrazumeva i izgradnju radne etike, tj. saradnje između pilota, kontrolora i sertifikovanih organa, kao i način delegiranja njihove uloge i odgovornosti u cilju bezbednog operativnog rada.

ADSB je veoma kompleksan sistem, koji obuhvata dva specifična podsistema, a koji su integrisani u kompletan ADS-B sistem: ADS-B In i ADS-B Out. Kompletan ADS-B sistem zavisi od drugih sistema, kao što su navigacioni i komunikacioni sistemi, sistemi operater/korisnik, itd. Dakle, mogu se identifikovati različite vrste/kategorije ranjivosti ovog sistema, između ostalih i opasnosti koje su prouzrokovane greškom pilota i kontrolora, kao i neadekvatnom komunikacijom između pilota i kontrolora. Pri tome, postoje brojne polazne tačke za ispitivanje uticaja ljudskog faktora, a jedna od njih je *Preliminary Hazard Analysis* (PHA)¹⁷, bazirana na *Fault Tree Analysis* (FTA)¹⁸.

Preliminary Hazard Analysis, jeste metodološki pristup analize sigurnosti, tj. alat koji se koristi za identifikaciju opasnosti, međusobno uslovljenih faktora

¹⁶ Kraemer A.D., Villani E., Arjoni D.H., (2019): "Aircraft FDI and human factors analysis of a take-off maneuver using SIVOR flight simulator", *IFAC-PaperOnLine*, 51(34)/2019, 184–189.

¹⁷ Olaganathan R. (2018): "Safety analysis of automatic dependent surveillance – broadcast (ADS-B) system", *Int. J. Aerosp. Eng.*, 5(2)/2018, 9–18.

¹⁸ Ericson, C. A. (2015): *Hazard analysis techniques for system safety*, (2nd Ed.), Wiley Inter Science, New York, NY.

i opasnih efekata, utvrđivanje nivoa rizika, kao i mera za ublažavanje. PHA procenjuje dizajn sistema na preliminarnom nivou bez sveobuhvatnih informacija, i predstavlja preliminarnu analizu opasnosti projektovanja, čiji je osnovni cilj analiziranje opasnosti koje su identifikovane u preliminarnoj listi opasnosti, kao i utvrđivanje prethodno neprepoznate opasnosti u ranoj fazi razvoja sistema. Ova metoda identifikuje uzročne faktore opasnosti, posledice i relativni rizik na početno koncipirani projekat. PHA se može primeniti za analizu svih vrsta sistema, operacija i funkcija, kako na podsistemu i sistemu, tako i na integrisanom skupu sistema.

Tako, na osnovu preliminarne liste opasnosti, može se sprovesti analiza različitih opasnosti, njihovih uzroka, efekata, nivoa uticaja opasnosti na avio-sistem i preventivnih mera. Suštine ove analize primenjene na konkretnu situaciju, a to je opasnost od gubitka razdvajanja uzrokovane ljudskim faktorom, tj. greškom pilota (u avionu, tj. vazduhu), kontrolora (ATC sistem) ili pogrešnom komunikacijom između pilota i kontrolora, data je u tabeli 1 Na osnovu preliminarne liste opasnosti, može se sprovesti analiza različitih opasnosti, među kojima su i opasnosti koje nastaje usled ljudske greške.

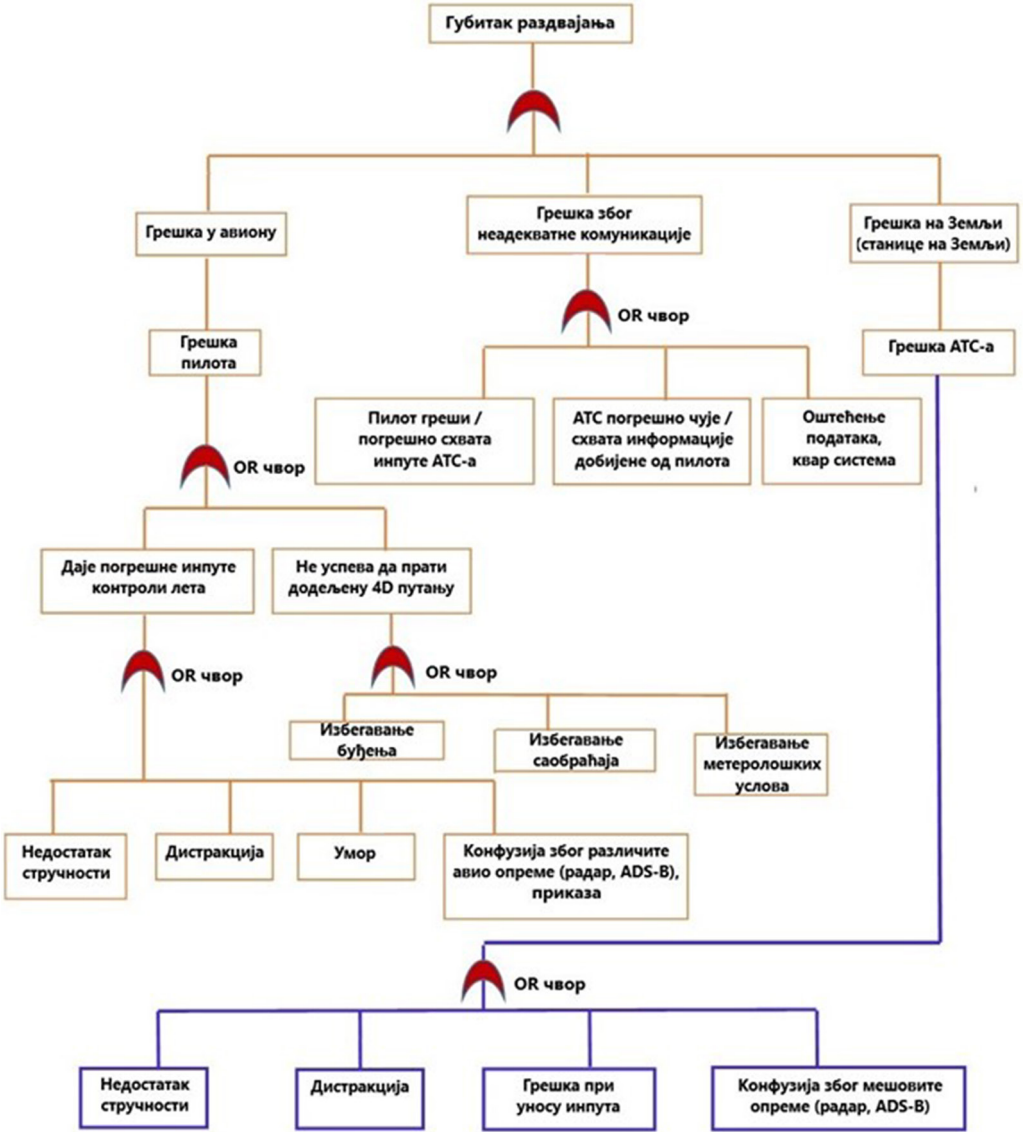
Kako je pomenuto, ADS-B kao veoma složen sistem, može biti izložen različitim vrstama opasnosti, a od identifikovanih vrsta, u radu Olaganathan R.¹⁷, razmatrane su samo one koje nastaju usled ljudske greške, i to, greške pilota, kontrolora i greške usled neadekvatne komunikacije između njih, koje se zatim analiziraju korišćenjem postojećeg metodološkog pristupa – analiza stabla grešaka.¹⁸ Suštine ove analize primenjene na konkretnu situaciju, a to je opasnost od gubitka razdvajanja uzrokovane ljudskim faktorom, tj. greškom pilota (u avionu, tj. vazduhu), kontrolora (ATC sistema) ili pogrešnom komunikacijom između pilota i kontrolora, šematski je prikazana na slici 1.

Šema analize ljudskog faktora (slika 1) sadrži pojedinačne faktore (među kojima su i ljudski), a koji utiču na gubitak razdvajanja. Ovi faktori povezani su OR čvorovima, tj. logičkim operaterima, s obzirom na to da bilo koji od datih faktora (pojedinačno) može prouzrokovati gubitak razdvajanja vazduhoplova. Na primer, faktori koji dovode do greške pilota su input netačnih podataka u ATC sistem i nemogućnost praćenja dodeljene 4D putanje; ovi faktori međusobno su zavisni, tj. povezani OR čvorom, jer bilo koji od ova dva faktora može prouzrokovati gubitak razdvajanja vazduhoplova. Takođe, problemi uzrokovani neadekvatnom komunikacijom između pilota i kontrolora, greške u unosu ulaznih podataka i konfuzija usled korišćenja različite opreme (radar u ADS-B) od strane kontrolora, nedostatak stručnosti, ometanje pažnje, itd., povezani su OR čvorom, jer bilo koji od ovih faktora može dovesti do gubitka razdvajanja.

Tabela 1. Preliminarna analiza opasnosti ADS-B izazvanih ljudskom greškom

Opis opasnosti	Uzrok	Efekat	Oznaka	Preventivne mere/ ublažavanje	Oznaka
Neemitovanje podataka	Neadekvatna upotreba – podešavanje pogrešnog režima transpondera od strane pilota	Povećanje opterećenja pilota; gubitak svesnosti situacije	3B	Podsećanje od strane kopilota ili proverom dokumentacije za let	4B
Pre poletanja, pilot može uneti pogrešan pritisak u visinomer	Nestručnost – pogrešna vrednost podešavanja pritiska koju je dao ATC	Sudar na zemlji ili u vazduhu	3C	Može se izbeći, ukoliko pilot ponovi vrednost ili ako je kontrolor stručan	4B
Pilot unosi pogrešan pritisak u visinomer	Nestručnost pilota	Sudar na zemlji ili u vazduhu	3C	Dvostruka provera podešavanja visinomera	4D
Utiče na sve operacije	Nestručnost-nepoznavanje ADS-B sistema	Gubitak razdvajanja	3B	Adekvatna obuka u vezi sa novim sistemima	4B
Pilot unosi pogrešan pritisak u visinomer	Nesporazum u komunikaciji – pilot pogrešno svata saopštenu vrednost podešavanja pritiska od strane ATC	Sudar na zemlji ili u vazduhu	3C	Može se izbeći, ukoliko pilot ponovi vrednost	4D
Pogrešan broj leta/registracija	Nedostatak svesnosti situacije od strane ATC- pogrešan pozivni znak u planu leta	Povećanje radnog opterećenja kontrolora	3D	Unakrsna provera plana leta od strane kontrolora	4D
Nepravilno povezivanje sa planom leta	Nedostatak svesnosti situacije pilota – netačan broj leta/registracija u FMS	Emitovanje netačnih podataka	3D	Podsećanje od strane kopilota/provera dokumentacije za let	4B
ATC može biti zbunjena vrednostima prikazanim na osnovu različitih izvora podataka	Konfuzija – različiti izvori podataka visine mogu zbuniti ATC	Različiti prikazi dovode do konfuzije	3D	Obavezna obuka u vezi sa funkcionisanjem ADS-B sistema	4C
ATC može primeniti različite standarde razdvajanja, radar ili ADS-B u odnosu na plan leta	Zbunjenost	Neadekvatno razdvajanje	3D	Obavezna obuka u vezi sa funkcionisanjem ADS-B	4B

Preuzeto i modifikovano iz: Olganathan R. (2018): "Safety analysis of automatic dependent surveillance – broadcast (ADS-B) system", Int. J. Aerosp. Eng., 5(2)/2018, p. 15.



Slika 1. ADS-B sistem: analiza ljudskih faktora primenom FTA

Izvor: Kožović, D. (2023): „Multidisciplinarni aspekti sajber bezbednosti avio sistema ADS-B”, Doktorska disertacija, Fakultet za civilno vazduhoplovstvo, Megatrend univerzitet, Beograd, str. 179.

Ovakve i slične preliminarne analize opasnosti i primena metodološkog pristupa PHA, tj. FTA, koriste se u cilju identifikacije, rangiranja opasnosti i odbrane od različitih opasnosti po sigurnost sistema/operacije, kao i preporuka za sprečavanje/ublažavanje identifikovanih opasnosti. Na osnovu PHA, utvrđuju se neprihvatljivi, tj. kritični rizici (kvar na interfejsu ADS-B i povezanih sistema, kvar Cockpit Display

of Traffic Information, CDTI (displeja i prijemne antene), visoki rizici (npr. kvar GPS prijemnika, data linka, transponder/ADS-B emitera, satelita, itd.) koji zahtevaju više pažnje i kontinuirano praćenje, zatim, opasnosti koje imaju srednji nivo rizika ali se ne smeju ignorisati (npr. one rangirani kao 3B, 3C i 3D, tabela 1), kao i opasnosti niskog nivoa (minorne) koje zahtevaju povremenu inspekciju i održavanje (npr. opasnosti označene/rangirane sa 4B i 4C, tabela 1). Svakako, adekvatno postupanje u skladu sa preporukama može umanjiti rizike, a krucijalno je obezbediti relevantnu obuku pilota i kontrolora u vezi sa ADS-B tehnologijom, zatim, bezbednosnim aspektima u vezi sa komunikacionim sistemima vazduh-zemlja, donošenju odluka, kao i upravljanja resursima posade. Preporuka je i podsticanje, tj. zahtevanje da piloti, kao i ATC koriste visokokvalitetne komunikacione sisteme – transpondere (režim C i S) i ACAS (*Airborne Collision Avoidance System*). Naročito je važno koncipirati i primenjivati periodičnu obuku pilota kako bi se potvrdila njihova kurentnosti i odredio tip rejtinga za upotrebu ADS-B tehnologije, a što bi značajno smanjilo rizike u vezi sa implementacijom ADS-B sistema.

Dakle, pitanja ljudskog faktora su prihvatanje i korišćenje od strane pilota i kontrolora leta, izgradnja saradnje između pilota, kontrolora leta i sertifikacionih tela, i način na koji se delegiraju njihove uloge i odgovornosti, koje obezbeđuju sigurnost. Na primer, u slučaju koji je razmatran (procesa razdvajanja), primenom FTA, predviđaju se tri pristupa, koji se mogu prilagoditi: prvi - odgovornost za razdvajanje mora uvek biti na kontroloru, drugi - odgovornost se može delimično podeliti između pilota i kontrole leta, posebno tokom faze na ruti i treći - posada leta može modifikovati i koordinirati svoje odluke uz odobrenje kontrolora letenja.

4. ZAKLJUČAK

U eri digitalnih tehnologija, vazduhoplovna industrija postaje sve sofisticiranija s razvojem novih tehnologija kao što su ADS-B, *Head-Up* displeji (HUD), *Controlled Pilot Data-Link Communication* (CPDLC), *Flight Information Service* (FIS), itd. One su efikasan alat u zajedničkom donošenju odluka, kada su integrisane u ATM i kada ih koriste piloti i kontrolori leta.

Uvođenje ADS-B sistema je najnoviji doprinos efikasnom nadzoru aviona međusobno, kao i aviona i zemaljskih stanica, tj. ostvarivanju neometanih operacija vazdušnog saobraćaja. Veoma značajno pitanje u vezi sa ovom tehnologijom, je način na koji se ADS-B podaci/informacije mogu efikasno koristiti od strane različitih operatera, kao što su piloti i kontrolori, a u okviru svojih relevantnih nadležnosti. Jedna od zajedničkih perspektiva i pilota i kontrolora leta o implementaciji ADS-B jeste odgovornost. Pri tome, neophodno je da sertifikaciona tela dodele

odgovornost na način koji će poboljšati ukupnu sigurnost/bezbednost. Dakle, pitanja ljudskog faktora su prihvatanje i korišćenje ADS-B tehnologije od strane pilota i kontrolora leta, izgradnja saradnje između njih i sertifikacionih tela, kao i način na koji se delegiraju njihove uloge i odgovornosti, sve u cilju ostvarivanja sigurnosti/bezbednosti avio sistema/operacija. Uključivanje i insistiranje na osnovnim principima svesnosti situacije, trebalo bi da budu inkorporirane u napredne obuke pilota i kontrolora letenja u vezi sa donošenjem odluka, a ove obuke i primena adekvatnih mera ublažavanja opasnosti, mogu u značajnom meri smanjiti opasne situacije izazvane ljudskim greškama. ADS-B tehnologija omogućava smanjenja standarda razdvajanja, povećanje efikasnosti i kapaciteta vazdušnog prostora/avio operacija, pruža fleksibilnost, kao i povećava svesnost situacije. Istovremeno, ADS-B ima značajnu ulogu u poboljšanju kvaliteta životne sredine, smanjenjem emisija gasova staklene bašte i buke, kao i doprinosi finansijskim uštedama, smanjenjem troškova goriva. Glavni izazov koji je pred vazduhoplovnom industrijom je razvoj sistema upravljanja vazdušnim saobraćajem integracijom ljudske komponente, kao i adekvatnom raspodelom odgovornosti između pilota i kontrolora, tako obezbeđujući da ceo sistem funkcioniše efikasno.

LITERATURA

- Ericson, C. A. (2015): *Hazard analysis techniques for system safety*, (2nd Ed.), Wiley Inter Science, New York, NY.
- FAA (2025): *Automatic dependent surveillance – broadcast (ADS-B)*, https://www.faa.gov/air_traffic/technology/adsb (01/10/2025).
- Hegarty, C., Shallberg, K., Walter, T., Alexander, K. (2018): "Spoofing detection for airborne GNSS equipment", in *Proceedings of 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, Miami, FL, 2018, 1350-1368.
- Kožović, D., Đurđević, D. (2019): "Sajber bezbednost u avijaciji", *Megatrend revija*, 16(2)/2019, 39-56.
- Kožović, D., Đurđević, D. (2021): "Spufing u civilnoj avijaciji: Bezbednost i sigurnost GPS/GNSS i ADS-B sistema", *Megatrend revija*, 18(3)/2021, 281-306.
- Kožović, D. (2023): *Multidisciplinarni aspekti sajber bezbednosti avio sistema ADS-B*, Doktorska disertacija, Fakultet za civilno vazduhoplovstvo, Megatrend univerzitet, Beograd.
- Kraemer A.D., Villani E., Arjoni D.H., (2019): "Aircraft FDI and human factors analysis of a take-off maneuver using SIVOR flight simulator", *IFAC-Paper OnLine*, 51(34)/2019, 184–189. doi:10.1016/j.ifacol.2019.01.063

- McLean D. (2003): "Operational Requirements for Fully Automatic Flight", *Aircr. Eng. Aerosp. Technol.*, 75(6)/2003, 570–574. DOI: 10.1108/00022660310503039
- Olaganathan R. (2018): "Safety analysis of automatic dependent surveillance – broadcast (ADS-B) system", *Int. J. Aerosp. Eng.*, 5(2)/2018, 9–18.
- Pavić A., Lalić B., Đurđević M. (2014): "Osnove ADS-B tehnologije i osmatranje područja Republike Srbije bez radarske pokrivenosti", *Zbornik radova Infoteh–Jahorina*, 13, 419–424, <https://infotech.etf.ues.rs.ba/zbornik/2014/radovi/KST-2/KST-2-4.pdf> (04/10/2025).
- Pierpaoli, P., Egerstedt, M., Rahmani, A. (2015): "Altering UAV flight path by threatening collision", in: *Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th (2015)*, IEEE, 4A4-1-4A4-10.
- Sathaye, H., Schepers, D., Ranganathan, A., Noubir, G. (2019): "Wireless attacks on aircraft instrument landing systems", in: *28th USENIX Security Symposium, August 14–16, 2019, Santa Clara, CA, USA*, 1-16.
- Silva S.S., Cho H., Hansman R.J. (2014): "Human factors studies of an ADS-B based traffic alerting system for general aviation", in: *Proceedings of the 29th Congress of the International Council of the Aeronautical Sciences (ICAS 2014)*, St. Petersburg, Russia, 10p, https://www.icas.org/icas_archive/ICAS2014/data/papers/2014_0419_paper.pdf (01/10/2025).
- Stevanović, D. M., Đurđević, D. (2016): "Internet stvari, lična i materijalna bezbednost", *Bezbednost*, 3/2016, 113-128.
- Ying X., Mazer J., Bernieri G., Conti M., Buschell L., Poovendran R. (2019): "Detecting ADS-B spoofing attacks using deep neural networks", in: *Proceeding of the IEEE Conference on Communications and Network Security (CNS2019)*, Washington D.C., USA, 9 p. DOI: 10.1109/CNS.2019.8802732.

ADS-B AVIATION SYSTEM SAFETY: A HUMAN FACTORS ANALYSIS

Abstract: *Automatic Dependent Surveillance-Broadcast (ADS-B) is one of the important systems integrated in the Next Generation Air Transportation System (NextGen) and Single European Sky Air Traffic Management Research (SESAR) programs, which enables the realization of a safer/safer and more efficient airspace system. In addition to numerous advantages, such as simple implementation, cheap hardware and high positioning accuracy, this wireless communication protocol has some significant drawbacks and they are reliance on the satellite navigation system (which can be physically damaged/corrupted/exposed to interference) as well as a oversimple protocol that does not provide authentication and encryption. Thus, in addition to being real, threats to the cyber security of ADS-B systems are also constantly increasing. In spite of all this, a very important aspect of using ADS-B is the human factor, which in aviation most often refers to the aspects of human error in aviation accidents and aviation system failures. As ADS-B provides data from which numerous advanced applications can be derived, the implementation of new ADS-B equipment and procedures expands the spectrum of human factors issues, such as understanding the use of automated on-board systems, which are becoming increasingly complex. That is why the analysis of the safety of the ADS-B system is of great importance, i.e. considering potential hazards and analyzing them, using certain methodological approaches, such as Preliminary Hazard Analysis (PHA), i.e. Preliminary Hazard Analysis/Fault Tree. This approach relies on evaluating identified hazards in hazards preliminary list as well as previously unrecognized hazards identification in the early stages of system development, all, in order to provide recommendations for preventing/mitigating the identified hazards.*

Keywords: ADS-B, civil aviation, human factor, preliminary hazard analysis, safety, security

Dragan Nikolić**

<https://orcid.org/0009-0000-0054-6861>

Dejana Radović*

<https://orcid.org/0009-0007-0762-5352>

UDC: 327:811.111

DOI: 10.5937/MegRev2502245N

Original scientific paper

Received 11.08.2025.

Approved 13.10.2025.

ENGLISH LANGUAGE PROFICIENCY AS A STRATEGIC TOOL IN INTERNATIONAL RELATIONS AND CORPORATE SECURITY

Abstract: *In a world where globalization and digital integration are transforming organizational dynamics, English has become an indispensable asset in both international relations and corporate security. This paper investigates the significant role that English language skills play for security professionals in multinational and diplomatically sensitive contexts, where clear, timely, and precise communication is essential. The study examines how English not only provides access to important security information and facilitates cross-border collaboration but also enhances diplomatic coordination and alignment with international regulatory standards. The theoretical framework draws from linguistic research, cognitive decision-making theories, and the real challenges we face in security communication. It highlights the urgent need for specialized English language training in high-stakes international contexts. Taking Hurricane Katrina as an example, it clearly illustrates the challenges that language barriers can present, particularly in diverse and multicultural contexts. The paper delves into the increasingly important connection between digital fluency and language skills, highlighting how crucial they are for boosting corporate resilience and fostering international collaboration. From a cybersecurity standpoint, any communication breakdowns between executives and global partners can significantly hinder our ability to tackle global threats, putting both business continuity and diplomatic trust at risk. This study highlights the essential nature of English for Specific Purposes (ESP) training, particularly aimed at meeting the specific needs of the security and international relations sectors. It underscores how crucial language is as a tool for global communication, risk management, and international collaboration. The findings call for more investment in language access and specialized training to enhance organizational security, trust, and effectiveness on a global level.*

Keywords: *international relations, corporate security, english for specific purposes (ESP)*

** E-mail: nikolic.dragan.0314@gmail.com

* E-mail: littlemissmuffet08@gmail.com

1. INTRODUCTION

In our increasingly interconnected global economy, English has really cemented its role as the leading language for international business, technology, and security communications. The corporate sector, especially in the realm of security, relies on the quick and accurate exchange of information, and the widespread use of English as a common language makes this essential communication possible among multinational organizations. Grasping the English language goes beyond just chatting with others; it's a vital asset for security professionals who need to access, interpret, and apply complex security guidelines, protocols, and threat intelligence that are often crafted in English-speaking settings.¹ A shared language is key for security teams spread across different locations to work together, especially since cyber threats and corporate risks know no borders.²

Corporate security is a dynamic and technical area that demands ongoing learning and flexibility, which is often facilitated by resources available in English. A lot of academic research, white papers, government regulations, and real-time threat reports are primarily published in English, which means that being proficient in the language is crucial for accessing the latest knowledge and innovative security solutions.³ To effectively share knowledge and coordinate activities, the global cybersecurity community often engages in international conferences, journals, and collaborative platforms where English is the main language.⁴ This trend is bolstered by multinational companies that designate English as their official language, particularly in security divisions, to maintain uniformity in policy execution and crisis management.⁵

In international relations, the importance of English cannot be overstated. Diplomatic talks, treaty discussions, and multilateral policymaking are frequently carried out in English. Organizations such as the United Nations, NATO, and the European Union often rely on English for their working documents and international communications. In the fields of security and diplomacy, mastering English

¹ Knight, R., & Nurse, J. R. C. (2020): "A framework for effective corporate communication after cyber security incidents", *arXiv*, <https://arxiv.org/abs/2009.09210>.

² Aghaei, E., Niu, X., Shadid, W., & Al-Shaer, E. (2022): "SecureBERT: A domain-specific language model for cybersecurity", *arXiv*, <https://arxiv.org/abs/2204.02685>.

³ Ranade, P., Mittal, S., Joshi, A., & Joshi, K. (2018): "Using deep neural networks to translate multi-lingual threat intelligence", *arXiv*, <https://arxiv.org/abs/1807.07517>.

⁴ Mavlonova, S. A., Morozova, A. V., & Oromidinova, D. P. (2025): "The role of the English language in global communication and its importance in the education system", *International Journal of Artificial Intelligence*, 5(2), 702–705.

⁵ Swift, J. S., & Wallace, J. (2011): "Using English as the common corporate language in a German multinational", *Journal of European Industrial Training*, 35(9), 892–913. DOI: 10.1108/03090591111185574

is essential for engaging meaningfully in global governance. It enables professionals to create alliances, confront international challenges, and negotiate security deals with assurance. Therefore, proficiency in English goes beyond being beneficial for business; it's a must for representing national interests internationally.

The role of English in corporate security training programs is incredibly important. By providing specialized language training for security professionals, we equip them with the right terminology and communication skills needed to understand technical manuals, write incident reports, and coordinate across borders smoothly and accurately.⁶ English for Specific Purposes (ESP) programs designed for the security sector not only boost language skills but also enhance cognitive and operational effectiveness by helping employees get familiar with the specific jargon and nuances of their field.⁷ As a result, we end up with a workforce that's more agile, allowing them to proactively address security vulnerabilities and respond rapidly to incidents.⁸

Mastering English is key to establishing a strong corporate security culture. It fosters open and effective communication among everyone involved, including management, technical teams, and outside partners. Companies with staff who speak multiple languages often run into issues like miscommunication and delays, which can be particularly harmful in security situations where quick decisions are essential.⁹ By using English as a common language, these organizations can minimize risks and foster a shared understanding of security priorities, protocols, and best practices. This strategy ultimately boosts their overall resilience.¹⁰

When it comes to corporate security, using English isn't just about practicality; it also helps companies comply with international regulations and standards, most of which are created and shared in English. This alignment in language capabilities enables organizations to fulfill global governance expectations and engage with international cybersecurity alliances, highlighting the strategic necessity of English proficiency in the contemporary corporate security environment.¹¹ Given

⁶ Brilianti, D. F., & Rokhim, A. (2024): "The importance of English for specific purposes based on the engineering students' perceptions", *Academic Journal Perspective: Education, Language, and Literature*, 11(1), 70–78. DOI: 10.33603/wc0gnm38.

⁷ Xie, Q. (2016): *English language training in the workplace: Case studies of corporate programs in China*, Springer. DOI: 10.1007/978-3-319-30157-0

⁸ EF Corporate Learning (2024): *Driving talent retention and development through language learning*, <https://corporatelearning.ef.com/en/resources/articles/talent-language-learning/>

⁹ Yoqutxon, M., & Feruzjon, K. (2025): "The crucial role of English in advancing information security in Uzbekistan", *Trends in the Use of Foreign Languages for Professional Priority*, Uzbekistan. DOI: 10.5281/zenodo.15666116

¹⁰ Alekseeva, E. A. (2020): "Language diversity development as a phenomenon of European security", *European Proceedings of Social & Behavioural Sciences*, 11, 15–22. DOI: 10.15405/epsbs.2020.11.03.2

¹¹ Shahriar, A. H. (2022): *The importance of English in multinational companies in Bangladesh: Corporate expectation vs reality*, Brac University, <http://hdl.handle.net/10361/21885>.

the challenges posed by a globalized economy, the role of English as a key tool for improving security and facilitating international partnerships is increasingly vital for businesses.

2. THEORETICAL FRAMEWORK

Approximately 6,500 different languages are spoken worldwide now. Although English and French are frequently regarded as world languages, the languages of China and India are by far the most widely spoken because of their sizable populations. Although English is still the most widely used language in business and science in the West, most speakers actually speak it as a second language. When speaking in their second language, people make riskier choices. However, research only found slight effects. Another theory put forth by other research is strategic risk-taking. Compared to those who struggle with their first language, those who struggle with their second language tend to make more objective assessments. Moderating factors exist that make sense intuitively.¹²

With 940 million native speakers, English surpasses Mandarin Chinese, which is spoken by almost 1.14 billion people worldwide, as the most spoken language when non-native speakers are included. Even with 1.46 billion English speakers, less than 20% of the world's population still speaks the language.¹³

In the field of international relations, language is incredibly important in shaping how countries behave diplomatically and how power is distributed globally. English has become a key tool for sharing political norms, values, and ideologies. The dominance of English in multilateral institutions offers both opportunities and challenges for nations with varying language backgrounds. Those who are fluent in English often have greater access to soft power channels, such as public diplomacy, strategic communication, and international media, while others may find themselves marginalized in global discussions. This linguistic gap emphasizes the necessity for inclusive language policies and improved access to ensure that everyone can participate fairly in international decision-making.

Since World War II, English has been the accepted lingua franca. Social media, business, entertainment, politics, and diplomacy have all been overtaken by English. Non-native English speakers most frequently communicate with one another in English, which is a very effective tool. Having said that, it is only one tool in

¹² Kreamer, M. (2023): *Language makes us tick – how do we make security training stick?*, <https://martin-kraemer.net/language-makes-us-tick-how-do-we-make-security-training-stick/>.

¹³ Richter, F. (2024): *The Most Spoken Languages: On the Internet and in Real Life*, <https://www.statista.com/chart/26884/languages-on-the-internet/?srsltid=AfmBOoqlQi1HLj2gbKNecXjhn0vXbygeHfG1HNVblv2ti8MUQ0SwAsd4>.

a multilingual toolkit. Only 7% of non-native English speakers at multinational corporations think they can communicate well at work, according to statistics. If so, there is a compelling commercial argument for companies to make additional investments in corporate language training initiatives that genuinely improve the working lives of their staff members.¹⁴

This uncovers a significant challenge in business settings where employees lack proficiency in English, despite it being the official *lingua franca*. Language barriers can cause misunderstandings that might compromise operational efficiency and safety, especially in security contexts where accuracy and clarity are paramount.¹⁵ Therefore, investing in language training for security professionals is not only beneficial but necessary to mitigate communication risks and enhance workplace safety.

In any industry, workplace security and safety are critical. One important component that is frequently disregarded is English language training, even if businesses make significant investments in tools, procedures, and training initiatives to guarantee a safe workplace. Effective communication becomes the cornerstone of operational efficiency and safety in a multicultural and diverse workforce. Misunderstandings, errors, and confusion can result from language problems. An employee who doesn't speak English well, for example, could misunderstand safety instructions or an emergency announcement. Workers may not correctly follow safety protocols or may not be able to respond quickly in an emergency as a result of this ignorance, which raises the risk of accidents. The foundation of occupational safety is trust. Employees are more likely to collaborate and perform effectively when they have faith that their coworkers comprehend and adhere to safety procedures. By ensuring that everyone on the team is aware of the same safety and operational protocols, English language training helps to foster this trust.¹⁶

Professionals who grew up in tech-savvy environments, often referred to as "digital natives," tend to have an entrepreneurial spirit that highlights creativity, adaptability, and a knack for self-directed learning.¹⁷ By fostering proactive problem-solving skills, resilience in the face of evolving challenges, and a strong

¹⁴ Learnlight (2019): 5 Reasons Why Language Training is Business Critical, <https://www.learnlight.com/en/articles/why-language-training-business-critical/>.

¹⁵ Hinds, P., Liu, L. & Lyon, J. (2011): "Putting the Global in Global Work: An Intercultural Lens on the Practice of Cross-National Collaboration", *Academy of Management Annals*, 5(1), 135–188. DOI: 10.5465/19416520.2011.586108

¹⁶ Inlingua Utah (2024): *Why English language training is important for work floor safety and security*, <https://www.inlinguautah.com/why-english-language-training-is-important-for-work-floor-safety-and-security/>.

¹⁷ Kwiatek, P., Papakonstantinidis, S. & Baltezarevic, R. (2021): "Digital Natives' Entrepreneurial Mindset: A Comparative Study in Emerging Markets", In: S. Rezaei, L. Jizhen, S. Ashourizadeh, V. Ramadani, & S.e Gërguri-Rashiti (Eds.): *The Emerald Handbook of Women*

command of digital tools and protocols, these traits can significantly enhance workplace safety. In the realm of corporate security, having a good grasp of technology and language is incredibly important. Both skills are vital for quickly identifying and addressing digital threats. When security teams harness these strengths, they can share information about vulnerabilities, make sense of threat intelligence reports, and act swiftly.¹⁸

By failing to invest in language access capabilities, organisations risk betraying the confidence of the public. For people who speak little or no English, even a simple misunderstanding might get worse. In certain situations, ignoring language limitations may even be a violation of someone's civil rights. These and other factors make language services, such as translation and interpreting, more and more important for community relations, public safety, and security. Language and cultural differences may cause unwarranted escalation, which may result in preventable harm or even death. These dangers are reduced by proactively implementing language services, which guarantees clearer communication in otherwise uncomfortable situations. When Hurricane Katrina hit New Orleans in 2006, many Latino citizens chose not to leave the city. The community was not fully aware of the storm's intensity because so few of the storm's warnings were transmitted in Spanish. A lot of people couldn't leave until it was too late. Although it is encouraging to see a more coordinated effort by the Federal Emergency Management Agency (FEMA) and its regional partners to prioritise language access, inclusive emergency communications still have a long way to go, especially at the local and regional levels. The storm's aftermath brought hard lessons.¹⁹

Creating effective security communication in international teams comes with its own set of challenges, one of which is silence. This silence often stems from unexpressed thoughts or worries that arise when team members feel insecure about their language skills or are anxious about miscommunication.²⁰ It really underscores the importance of having focused English language training and strong communication skills to help lessen these moments.

For companies and organisations of all sizes and industries, cybersecurity is essential. Businesses may experience severe or even catastrophic outcomes from cyberattacks, including data loss, operational disruptions, or non-compliance with

and Entrepreneurship in Developing Economies, Chapter 15. (295-316), Emerald Publishing Limited.

¹⁸ Prensky, M. (2001): "Digital Natives, Digital Immigrants", *On the Horizon*, 9(5), 1-6. DOI: 10.1108/10748120110424816

¹⁹ Thomas, P. (2024): *The Role of Language Services in Public Safety and Security*, <https://piedmontglobal.com/language-services-in-public-safety-and-security/>.

²⁰ Baltezarević, R., Kwiatek, P., Baltezarević, B. & Baltezarević, V. (2022): "The meaning of silence in personal communication: spiral of silence or a stimulant of creativity?", *Creativity Studies*, 15(1), 58-73. DOI: 10.3846/cs.2022.11374

regulations. They may also have a direct effect on earnings, harm one's reputation, or erode the confidence of suppliers, customers, and staff. Executives must thus recognise the importance of cyber security for businesses and take the necessary precautions to safeguard their digital assets. A recent study found that 44% of CEOs said their organisations do not place a high priority on cybersecurity. This is because the terminology employed in this field is unclear. "The language used is confusing and hinders threat understanding," according to Europa Press, is the reason for this. A third of the executives who responded to the study said they had no idea what "malware" (malicious software) was, and nearly another third had no idea what "ransomware" (data hijacking) was. Executives must thus comprehend the importance of cybersecurity beyond words since it affects every facet of the company, including business continuity. Cybersecurity needs to be a top corporate and strategic priority.²¹

3. CONCLUSION

You can't underestimate the role of the English language in corporate security. In a fast-paced world where threats, both digital and physical, can cross borders in mere seconds, having a common language is vital for clear communication, coordination, and response. English has become the go-to language for sharing security protocols, intelligence reports, regulatory frameworks, and best practices worldwide. This common tongue helps multinational teams collaborate more effectively, cuts down on miscommunication during stressful times, and builds a shared understanding of security roles across different cultures and locations.

When it comes to international relations, English serves as a vital tool that helps countries participate in security dialogues and work together on counter-terrorism strategies. Mastering the language becomes a valuable form of strategic capital, allowing both states and corporations to join global efforts, shape diplomatic discussions, and bolster compliance with international laws. On the other hand, a lack of language skills can lead to missed collaboration opportunities and reduced credibility in multilateral discussions.

The paper highlights a crucial point: having limited English skills can create significant operational risks. This ranges from misunderstanding safety protocols to failing to respond adequately to cyber threats. The insights into decision-making in a second language really emphasize how vital structured language training is, especially in situations where being objective, quick, and clear is essential. As the

²¹ Palou, N. (2023): *How language puts business Cybersecurity at risk*, <https://telefonicatech.com/en/blog/how-language-puts-business-cybersecurity-at-risk>.

cybersecurity landscape grows increasingly intricate, it's not just about having the right technical skills; being able to communicate effectively is just as important. This is particularly important for executives and decision-makers who need to handle unfamiliar terms and make smart choices under pressure.

By investing in English for Specific Purposes (ESP) programs tailored for the security sector, organizations can effectively enhance their resilience while protecting their people, assets, and information. These programs seamlessly link language skills with professional needs, equipping employees with the communication tools they require to work confidently and accurately. As businesses around the globe keep growing and changing, English will continue to be a vital tool, not just for smooth operations, but also for fostering trust, ensuring compliance, and ultimately safeguarding what's most important. Companies that recognize this and take proactive steps will be better equipped to face the intricate security challenges that lie ahead.

LITERATURE

- Aghaei, E., Niu, X., Shadid, W., & Al-Shaer, E. (2022): "SecureBERT: A domain-specific language model for cybersecurity", *arXiv*, <https://arxiv.org/abs/2204.02685>.
- Alekseeva, E. A. (2020): "Language diversity development as a phenomenon of European security", *European Proceedings of Social & Behavioural Sciences*, 11, 15–22. DOI: 10.15405/epsbs.2020.11.03.2
- Baltezarević, R., Kwiatek, P., Baltezarević, B. & Baltezarević, V. (2022): "The meaning of silence in personal communication: spiral of silence or a stimulant of creativity?", *Creativity Studies*, 15(1), 58–73. DOI: 10.3846/cs.2022.11374
- Brilianti, D. F., & Rokhim, A. (2024): "The importance of English for specific purposes based on the engineering students' perceptions", *Academic Journal Perspective: Education, Language, and Literature*, 11(1), 70–78. DOI: 10.33603/wc0gnm38
- EF Corporate Learning (2024): *Driving talent retention and development through language learning*, <https://corporatelearning.ef.com/en/resources/articles/talent-language-learning/>.
- Hinds, P., Liu, L. & Lyon, J. (2011): "Putting the Global in Global Work: An Inter-cultural Lens on the Practice of Cross-National Collaboration", *Academy of Management Annals*, 5(1), 135–188. DOI: 10.5465/19416520.2011.586108
- Inlingua Utah (2024): *Why English language training is important for work floor safety and security*, <https://www.inlinguautah.com/why-english-language-training-is-important-for-work-floor-safety-and-security/>.

- Knight, R., & Nurse, J. R. C. (2020): "A framework for effective corporate communication after cyber security incidents", *arXiv*, <https://arxiv.org/abs/2009.09210>.
- Kreamer, M. (2023): *Language makes us tick – how do we make security training stick?*, <https://martin-kraemer.net/language-makes-us-tick-how-do-we-make-security-training-stick/>.
- Kwiatek, P., Papakonstantinidis, S. & Baltezarevic, R. (2021): "Digital Natives' Entrepreneurial Mindset: A Comparative Study in Emerging Markets", In: S. Rezaei, L. Jizhen, S. Ashourizadeh, V. Ramadani, & S.e Gërguri-Rashiti (Eds.): *The Emerald Handbook of Women and Entrepreneurship in Developing Economies*, Chapter 15. (295-316), Emerald Publishing Limited.
- Learnlight (2019): 5 Reasons Why Language Training is Business Critical, <https://www.learnlight.com/en/articles/why-language-training-business-critical/>.
- Mavlonova, S. A., Morozova, A. V., & Oromidinova, D. P. (2025): "The role of the English language in global communication and its importance in the education system", *International Journal of Artificial Intelligence*, 5(2), 702–705.
- Palou, N. (2023): *How language puts business Cybersecurity at risk*, <https://telefonicatech.com/en/blog/how-language-puts-business-cybersecurity-at-risk>.
- Prensky, M. (2001): "Digital Natives, Digital Immigrants", *On the Horizon*, 9(5), 1-6. DOI: 10.1108/10748120110424816
- Ranade, P., Mittal, S., Joshi, A., & Joshi, K. (2018): "Using deep neural networks to translate multi-lingual threat intelligence", *arXiv*, <https://arxiv.org/abs/1807.07517>.
- Richter, F. (2024): *The Most Spoken Languages: On the Internet and in Real Life*, <https://www.statista.com/chart/26884/languages-on-the-internet/?srsltid=AfmBOoqlQi1HLj2gbKNecXjhn0vXbygeHfG1HNVblv2ti8MUQ0SwAsd4>.
- Shahriar, A. H. (2022): *The importance of English in multinational companies in Bangladesh: Corporate expectation vs reality*, Brac University, <http://hdl.handle.net/10361/21885>.
- Swift, J. S., & Wallace, J. (2011): "Using English as the common corporate language in a German multinational", *Journal of European Industrial Training*, 35(9), 892–913. DOI: 10.1108/03090591111185574
- Thomas, P. (2024): *The Role of Language Services in Public Safety and Security*, <https://piedmontglobal.com/language-services-in-public-safety-and-security/>.
- Xie, Q. (2016): *English language training in the workplace: Case studies of corporate programs in China*, Springer. DOI: 10.1007/978-3-319-30157-0
- Yoqutxon, M., & Feruzjon, K. (2025): "The crucial role of English in advancing information security in Uzbekistan", *Trends in the Use of Foreign Languages for Professional Priority*, Uzbekistan. DOI: 10.5281/zenodo.15666116

ZNANJE ENGLESKOG JEZIKA KAO STRATEŠKI ALAT U MEĐUNARODNIM ODNOSIMA I KORPORATIVNOJ BEZBEDNOSTI

Sažetak: *U svetu gde globalizacija i digitalna integracija transformišu organizacionu dinamiku, engleski jezik je postao nezaobilazan resurs kako u međunarodnim odnosima, tako i u korporativnoj bezbednosti. Ovaj rad istražuje značajnu ulogu koju veštine engleskog jezika igraju za stručnjake za bezbednost u multinacionalnim i diplomatski osetljivim kontekstima, gde je jasna, blagovremena i precizna komunikacija neophodna. Studija ispituje kako engleski jezik ne samo da omogućava pristup važnim bezbednosnim informacijama i olakšava prekograničnu saradnju, već i poboljšava diplomatsku koordinaciju i usklađenost sa međunarodnim regulatornim standardima. Teorijski okvir se zasniva na lingvističkim istraživanjima, teorijama kognitivnog odlučivanja i stvarnim izazovima sa kojima se suočavamo u bezbednosnoj komunikaciji. Ističe hitnu potrebu za specijalizovanom obukom engleskog jezika u međunarodnim kontekstima sa visokim ulozima. Uzimajući uragan Katrina kao primer, jasno ilustruje izazove koje jezičke barijere mogu predstavljati, posebno u raznovrsnim i multikulturalnim kontekstima. Rad se bavi sve važnijom vezom između digitalne tečnosti i jezičkih veština, ističući koliko su one ključne za jačanje korporativne otpornosti i negovanje međunarodne saradnje. Sa stanovišta sajber bezbednosti, svaki prekid komunikacije između rukovodilaca i globalnih partnera može značajno ometati našu sposobnost da se nosimo sa globalnim pretnjama, dovodeći u opasnost i kontinuitet poslovanja i diplomatsko poverenje. Ova studija ističe suštinsku prirodu obuke za engleski jezik za posebne namene (ESP), posebno usmerene na zadovoljavanje specifičnih potreba sektora bezbednosti i međunarodnih odnosa. Ona naglašava koliko je jezik ključan kao alat za globalnu komunikaciju, upravljanje rizicima i međunarodnu saradnju. Rezultati zahtevaju veća ulaganja u pristup jeziku i specijalizovanu obuku kako bi se poboljšala organizaciona bezbednost, poverenje i efikasnost na globalnom nivou.*

Ključne reči: međunarodni odnosi, korporativna bezbednost, engleski jezik za posebne svrhe (ESP)

Vladimir Lović*

<https://orcid.org/0009-0004-5110-8369>

Miloš Azdejković**

<https://orcid.org/0009-0009-3509-6384>

UDK: 327:911.3

004.8

DOI: 10.5937/MegRev2502255L

Pregledni naučni rad

Primljen 06.09.2025.

Odobren 12.11.2025.

IZAZOVI DIGITALNOG OKRUŽENJA: MEDJUNARODNOPRAVNI, GEOPOLITIČKI I BEZBEDNOSNI ASPEKTI

Apstrakt: Ovaj rad kritički ispituje dubok uticaj digitalnih tehnologija, sa posebnim fokusom na veštačku inteligenciju (AI), na domene međunarodnog prava, geopolitike i bezbednosti u kontekstu Četvrte industrijske revolucije. Tekuća digitalna transformacija je izazvala transformativne promene u ekonomskim, društvenim i bezbednosnim sferama, dok istovremeno predstavlja složene izazove u vezi sa suverenitetom, odgovornošću države i sajber pravom. Kako digitalne inovacije prožimaju globalne interakcije, pitanja u vezi sa regulacijom i upravljanjem AI postaju sve istaknutija, što zahteva razvoj sveobuhvatnih pravnih i etičkih okvira.

Kao odgovor na ova nova pitanja, Evropska unija (EU) i Ujedinjene nacije (UN) su preduzele napore da uspostave normativne smernice za odgovoran razvoj i primenu AI tehnologija. Konkretno, analiza razmatra ključne rezolucije UN-a—A/RES/78/265 i A/RES/79/239—koje naglašavaju važnost obezbeđivanja bezbednosti veštačke inteligencije i zalažu se za nemilitarizaciju takvih tehnologija. Ove rezolucije odražavaju usklađen međunarodni pokušaj da se umanje rizici povezani sa širenjem veštačke inteligencije i da se promoviše miroljubiva i etička upotreba.

Štaviše, rad istražuje geopolitičku konkurenciju između velikih sila, posebno Sjedinjenih Država, koje nastoje da uspostave tehnološko vođstvo dok se bave bezbednosnim problemima u vezi sa veštačkom inteligencijom. Ovo takmičenje utiče na međunarodne pravne norme i bezbednosne strategije, naglašavajući kritičnu potrebu za multilateral-nom saradnjom kako bi se upravljalo izazovima upravljanja veštačkom inteligencijom u globalnom okruženju koje se brzo razvija.

Ključne reči: veštačka inteligencija, digitalna transformacija, geopolitika, međunarodno pravo, bezbednost.

* Međunarodni centar za ekonomiju i javne politike – MCEJP, Niš, Srbija
E-mail: vladalovic@yahoo.com

** Univerzitet "Union Nikola Tesla", Beograd, Srbija
E-mail: azdejkovic.milos@gmail.com

1. UVOD

Pojava Četvrte industrijske revolucije predstavlja značajne izazove za postojeći međunarodni pravni poredak, primoravajući globalne organizacije da preduzmu opsežne istraživačke inicijative kako na regionalnom tako i na međunarodnom nivou. Ove inicijative zahtevaju značajna ulaganja u različite sektore primene digitalne tehnologije. Među ovim naporima, program Evropske unije pod nazivom „Evropa spremna za digitalno doba“ ističe se kao glavna inicijativa, koja odražava jedan od najvažnijih prioriteta Evropske komisije u unapređenju agende digitalne transformacije. Savremeni međunarodni odnosi i geopolitičke promene uz tehnološki i IT napredak, duboko su preoblikovali društvene percepcije i funkcionalnu ulogu digitalizacije u izuzetno kratkom periodu.¹ Integracija digitalnih tehnologija postala je neophodna u brojnim domenima, uključujući zapošljavanje, obrazovanje, zabavu, društvenu interakciju, trgovinu, zdravstvenu zaštitu i kulturni pristup. Savremene okolnosti su razotkrile značajne ranjivosti u digitalnom domenu, kao što su neovlašćeno hakovanje, daljinsko upravljanje računarima, sabotaza digitalnih sistema, sajber prevara, krađa identiteta u virtuelnim prostorima, proliferacija malvera, kršenja ličnih podataka, smetnje u elektronskim komunikacijama i izazovi u vezi sa bezbednošću elektronskih ugovora i digitalnih ugovora. Rešavanje ovih pitanja zahteva napore međunarodne zajednice da uspostavi sveobuhvatan pravni okvir koji bi mogao ublažiti takve pretnje. Veštačka inteligencija, robotika, autonomna vozila, Internet stvari i Internet inteligentnih uređaja predstavljaju primere različitih kategorija digitalnih tehnologija koje su trenutno u centru opsežnih doktrinarnih diskusija.

S obzirom da proliferacija i korišćenje ovih digitalnih inovacija često prevazilaze regulatorne kapacitete pojedinih država, razvoj okvira međunarodne saradnje postaje suštinska neophodnost. Ovo uključuje formulisanje odgovarajućih univerzalnih i regionalnih normi u okviru međunarodnog prava, čiji je cilj rešavanje višestrukih uticaja digitalizacije i pojave informacionog društva – napora vođenih glavnim globalnim trendovima u digitalnoj transformaciji.

Dok digitalne tehnologije predstavljaju značajne mogućnosti za ekonomski rast i međunarodnu saradnju, one takođe uvode značajne rizike—uključujući sajber napade na vitalnu infrastrukturu, širenje dezinformacija i kršenje privatnosti. Shodno tome, međunarodni pravni okviri moraju uravnotežiti promociju slobodne komunikacije i ljudskih prava sa imperativima globalne bezbednosti i odgovornosti. Utvrđeni principi međunarodnog prava – uključujući suverenitet, zabranu upotrebe sile, odgovornost države i ljudska prava – moraju se preispitati i prilagoditi digitalnom miljeu. Ovo postavlja kritična pitanja u vezi sa

¹ BALTEZAREVIC, B., MILUTINOVIC, O., BALTEZAREVIC, R., & BALTEZAREVIC, V. (2020). Digital storage and online mediated memory. *International Review*, (1-2), 34.

primenljivošću klasičnih pravnih normi, kao što su Povelja UN i međunarodno običajno pravo, u sajber prostoru, gde su fizičke granice fluidne i nedržavni akteri – kao što su privatne korporacije, hakerske grupe i pojedinci – igraju sve istaknutiju ulogu. Napredak digitalnih tehnologija tokom poslednjih decenija ubrzao je duboke transformacije u domenima međunarodnih odnosa, komunikacija, trgovine i bezbednosti. Inovacije kao što su Internet, veštačka inteligencija, alati za sajber ratovanje i digitalna infrastruktura uveli su nove pravne izazove, s obzirom da se međunarodno pravo prvenstveno razvijalo u kontekstu analognih interakcija i tradicionalnih međudržavnih odnosa.

2. EVROPSKI STANDARDI REGULISANJA OBLASTI DIGITALNOG OKRUŽENJA

Interakcija između zakona, bezbednosti i tehnologije u domenu veštačke inteligencije (AI) predstavlja višestruki izazov koji zahteva pažljivo ispitivanje. Za razliku od konvencionalnih softverskih sistema, AI tehnologije poseduju sposobnost da uče iz podataka, donose autonomne odluke i prilagođavaju svoje ponašanje tokom vremena, uvodeći na taj način nivo nepredvidljivosti koji komplikuje tradicionalne regulatorne okvire. Autonomna priroda sistema veštačke inteligencije, posebno kada rade bez ljudskog nadzora, dovodi do novih pravnih i bezbednosnih problema, uključujući pitanja u vezi sa odgovornošću, privatnošću i potencijalnom zlonamernom upotrebom. Kako AI sve više prožima različite sektore – kao što su javna uprava, trgovina, obrazovanje i industrija – postaje očigledna hitnost uspostavljanja sveobuhvatnih propisa. Efikasno upravljanje mora uravnotežiti podsticanje inovacija sa očuvanjem društvenih interesa. Ključno za ovaj poduhvat je određivanje odgovarajućih organa nadležnih za formulisanje, primenu i sprovođenje propisa o veštačkoj inteligenciji. Da li regulatorni nadzor treba da bude centralizovan unutar vladinih agencija, da ga nadgledaju međunarodna tela, ili da bude poveren zainteresovanim stranama u industriji, ostaje predmet tekuće debate, naglašavajući potrebu za koordinisanim, multidisciplinarnim pristupom upravljanju veštačkom inteligencijom.²

Digitalne tehnologije postale su fundamentalna komponenta savremenog društva i međunarodnih odnosa. Njihov uticaj seže dalje od ekonomskog razvoja i komunikacije, obuhvatajući kritične domene kao što su bezbednost, ljudska prava i globalno upravljanje. Shodno tome, države i međunarodne organizacije su aktivno

² Zirojević, I. (2024): "Veštačka inteligencija – bezbednosni, tehnološki i pravni aspekti", *Megatrend revija*, Vol. 21, № 2, 2024, Megatrend univerzitet, Beograd, 100. DOI: 10.5937/MegRev2402093Z

angažovane na uspostavljanju odgovarajućih zakonskih okvira za promovisanje bezbednog, transparentnog i odgovornog korišćenja digitalnog prostora.³

Analiza njihovih pristupa pruža vredan uvid u različite nivoe regulative – u rasponu od regionalno fokusiranih, normativnih pravnih instrumenata do mehanizama za zaštitu ljudskih prava i sveobuhvatnih smernica globalne politike.⁴ Ovo shvatanje služi kao osnova za ispitivanje određenih domena regulative digitalne tehnologije i procenu efikasnosti postojećih međunarodnih pravnih okvira.

Ovaj finansijski podsticaj odražava intenziviranje procesa započetog tokom protekle decenije za ubrzanje digitalne transformacije Evrope, prvenstveno izgradnjom napretka ka potpuno funkcionalnom jedinstvenom digitalnom tržištu i intenziviranjem aktivnosti navedenih u strategiji „Oblikovanje digitalne budućnosti Evrope“.⁵ Strategija ocrtava osnovne principe digitalne transformacije prvenstveno u skladu sa standardima utvrđenim Uredbom o upravljanju podacima, Uredbom o digitalnim uslugama, Uredbom o digitalnim tržištima i Strategijom sajber bezbednosti.⁶

Savet Evrope je takođe priznao imperativ razvoja sveobuhvatnih regionalnih međunarodnih standarda u vezi sa primenom digitalnih tehnologija. S tim u vezi, organizacija je aktivno uključena u suočavanje sa izazovima koje predstavljaju digitalne tehnologije u okviru zaštite i održavanja osnovnih ljudskih prava i sloboda kao što su sadržana u Evropskoj konvenciji o ljudskim pravima i osnovnim slobodama, zajedno sa njenim dopunskim protokolima.

Jedan od najvažnijih strateških dokumenata koje je Savet Evrope usvojio u oblasti digitalnih tehnologija je dokument „Strategija upravljanja internetom Saveta Evrope“.⁷ Strategija je podvukla imperativ zaštite pojedinaca od sajber kriminala i nesigurnosti na mreži, kao i od neovlašćenog nadzora njihovih aktivnosti. Naglašava zabrinutost koja se odnosi na usluge i uređaje povezane sa internetom, uključujući kritične aspekte infrastrukture i operativnih mehanizama koji imaju potencijal da utiču na ljudska prava i slobode.⁸

³ Koch, B. A. (2020): “Liability for Emerging Digital Technologies: An Overview”, *Journal of European Tort Law*, 11(2), 115.

⁴ Prlja, D., Reljanović, M., & Ivanović, Z. (2012): *Internet pravo*, Institut za uporedno pravo, 7.

⁵ *Oblikovanje digitalne budućnosti Evrope (Shaping Europe's digital future, 19 February 2020.)*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en (07.10.2025).

⁶ *Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions 2030 Digital Compass: The European way for the Digital Decade*, COM/2021/118.

⁷ Council of Europe (2016): *Internet governance – Council of Europe strategy 2016–2019*, <https://rm.coe.int/internet-governance-strategy-2016-2019-updated-version-06-mar-2018/1680790ebe> (07.10.2025).

⁸ Vuletić, D., & Đorđević, B. (2021): “Problemi i izazovi upravljanja internetom na međunarodnom nivou”, *Međunarodni problemi = International problems*, 73, 235.

Na međunarodnom nivou, posebno u okviru Ujedinjenih nacija, različitim aspektima korišćenja digitalne tehnologije bavi se nezavisni globalni entitet poznat kao Forum za upravljanje internetom. Osnovan 2005. tokom Svetskog samita o informacionom društvu u Tunisu, Forum funkcioniše pod pokroviteljstvom generalnog sekretara Ujedinjenih nacija. Od svog početka, Forum je sazvaio više sesija fokusiranih na kritična pitanja kao što su upravljanje internetom, premošćavanje digitalnog jaza, obezbeđivanje bezbednosti informacija, zaštita privatnosti podataka na mreži, promovisanje digitalne inkluzije i druge relevantne teme.⁹

Integracija digitalnih tehnologija kao osnovne komponente u potrazi za održivim razvojem artikulisana je u okviru Agende Ujedinjenih nacija 2030. Kao odgovor na brzi napredak digitalizacije društva, Program Ujedinjenih nacija za razvoj (UNDP) je sredinom 2019. godine predstavio svoju inauguralnu Digitalnu strategiju.¹⁰

Sledeći strateški okvir, pod nazivom Digitalna strategija 2022–2025, osmišljen je da održi i unapredi napore na digitalnoj transformaciji koje preduzima UNDP kroz niz ciljanih inicijativa. Strategija je strukturisana oko tri osnovne komponente: (1) vodećih principa i predloga vrednosti, koji ocrtavaju sveobuhvatni pristup UNDP-a digitalnoj transformaciji; (2) strateški pravac, koji obuhvata viziju, ciljeve i očekivane rezultate koji će voditi aktivnosti UNDP-a u narednom četvorogodišnjem periodu; i (3) metodologiju implementacije i procenu učinka, sa detaljima o pristupima za sprovođenje strategije i procenom njene efikasnosti.¹¹

Pod okriljem Ujedinjenih nacija, poseban akcenat je stavljen na razvoj standarda za olakšavanje ostvarivanja ljudskih prava u digitalnoj sferi, kao što je artikulisano kroz Rezoluciju o unapređenju, zaštiti i ostvarivanju ljudskih prava na Internetu iz 2021. godine.¹² Rezolucija je zasnovana na osnovnim ljudskim pravima i slobodama artikulisanim u Univerzalnoj deklaraciji o ljudskim pravima, Međunarodnom paktu o građanskim i političkim pravima i Međunarodnom paktu o socijalnim, ekonomskim i kulturnim pravima, uz uvažavanje posebnosti povezanih sa njihovom primenom u digitalnoj sferi.

Značaj korišćenja digitalnih tehnologija u kontekstu održavanja globalnog mira i stabilnosti prepoznala je Generalna skupština Ujedinjenih nacija još 1975. godine, kada je usvojila Deklaraciju o korišćenju naučnog i tehnološkog progressa u interesu mira i za dobrobit čovečanstva.¹³ O primarnom cilju pomenutog zakonodavstva svedoči

⁹ Ibid. 239.

¹⁰ United Nations (2019): *Declaration of digital interdependence*, <https://news.un.org/en/story/2019/06/1040131> (07.10.2025).

¹¹ UNDP, *Digital Strategy 2022-2025*, <https://digitalstrategy.undp.org/> (01.10.2025).

¹² United Nations (2021): *The promotion, protection and enjoyment of human rights on the Internet: Resolution / adopted by the Human Rights Council on 13 July 2021, A/HRC/RES/32/13*.

¹³ United Nations (1975): "Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind", *Proclaimed by General Assembly resolution 3384 (XXX) of 10 November 1975*.

njegov naglasak na ograničavanju primene savremenih tehnologija koje bi mogle da naruše međunarodni mir i bezbednost, kao i da naruše suverenitet suverenih država.

Da bi se razvilo sveobuhvatno razumevanje međunarodnih pravnih standarda koji regulišu korišćenje digitalnih tehnologija, ova studija će se fokusirati na analizu trenutnih inicijativa koje preduzimaju istaknute međunarodne organizacije u oblastima veštačke inteligencije, zaštite podataka, visokotehnološkog kriminala i digitalne ekonomije. U analizi će se posebno ispitati aktivnosti Evropske unije, Saveta Evrope i Ujedinjenih nacija, s obzirom na njihovu značajnu ulogu u formulisanju i razvoju međunarodnopravnih normi. Odabrane oblasti primene digitalne tehnologije određene su na osnovu sistematske kategorizacije koja se nalazi u postojećoj pravnoj literaturi, koja se smatra odgovarajućom obimu i ciljevima ovog istraživanja.¹⁴

3. MEDJUNARODNOPRAVNI, GEOPOLITIČKI I BEZBEDNOSNI IZAZOVI VEŠTAČKE INTELIGENCIJE (AI)

Veštačka inteligencija se široko smatra jednim od najznačajnijih, ako ne i najvažnijim, tehnološkim napretkom savremene ere, zahvaljujući svom dubokom uticaju na individualne stilove života i uticaju na percepciju društvenih i ekoloških fenomena. Koncept veštačke inteligencije obuhvata različite definicije unutar naučnog diskursa. Opšteprihvaćena perspektiva unutar akademske zajednice karakteriše veštačku inteligenciju kao podeljak računarske nauke posvećen kreiranju kompjuterskih algoritama i aplikacija sposobnih za izvršavanje zadataka koji su tradicionalno povezani sa ljudskom inteligencijom.¹⁵

Veštačka inteligencija (AI) obuhvata dizajn i primenu digitalnih sistema i robota sposobnih da izvršavaju zadatke koji su tradicionalno povezani sa ljudskom spoznajom. Ovi zadaci uključuju rasuđivanje, učenje, rešavanje problema i generalizaciju, koji su fundamentalni za inteligentno ponašanje. Primarni cilj istraživanja i razvoja veštačke inteligencije je da simulira ljudske kognitivne procese, čime se omogućava mašinama da izvrše složeno donošenje odluka u različitim kontekstima i okruženjima. Oponašajući ljudsku inteligenciju, AI ima za cilj da poboljša automatizaciju, poboljša efikasnost i omogući inovativna rešenja u oblastima koje se kreću od zdravstvene zaštite i finansija do autonomnih sistema i obrade prirodnog jezika.¹⁶

¹⁴ Bainbridge, D. (2000): *Introduction to Computer Law*, Longman.

¹⁵ Filipovski Z., Galetin M. (2022): "Uloga Saveta Evrope u kreiranju pravne regulative u oblasti veštačke inteligencije", *Zbornik radova XIX Međunarodnog naučnog supa „Pravnički dani – prof. dr Slavko Carić“ pod nazivom „Pravo, nauka i društvo – aktuelna pitanja i perspektive“*, Pravni fakultet za privredu i pravosuđe u Novom Sadu. 280.

¹⁶ Baltezarević, R. (2023): „Uticaj veštačke inteligencije na globalnu ekonomiju“, *Megatrend revija*, Vol. 20, № 3, 2023, Megatrend univerzitet, Beograd, 15. DOI: 10.5937/MegRev2303013B

Veštačka inteligencija (AI) je postala sastavni deo širokog spektra društvenih i političkih domena, obuhvatajući oblasti kao što su medicinska dijagnostika, platforme društvenih medija, korišćenje mobilnih uređaja i finansijsko trgovanje. Moguće je da će AI sve više dominirati čak i u sektorima društva u kojima je njeno prisustvo trenutno minimalno. Opažanje autora naučne fantastike Vilijama Gibsona — da je „budućnost već tu, ali nije ravnomerno raspoređena“ — mogla bi se uskoro shvatiti kao opipljiva stvarnost.¹⁷

Analiza pravnih okvira koji regulišu uticaj različitih vrsta veštačke inteligencije na živote pojedinaca predstavlja primarni fokus brojnih međunarodnih organizacija. S obzirom na prisustvo brojnih neregulisanih pitanja u oblasti korišćenja veštačke inteligencije koja zahtevaju globalnu koordinaciju, očekuje se da ove organizacije primenjuju propise osmišljene da obezbede bezbedno korišćenje veštačke inteligencije. Pored toga, oni imaju za cilj da uspostave pravne mehanizme za ublažavanje potencijalnih štetnih efekata povezanih sa usvajanjem i primenom ove tehnologije.

Ujedinjene nacije su 2015. godine osnovale Centar za veštačku inteligenciju i robotiku u okviru Instituta Ujedinjenih nacija za istraživanje kriminala i pravde. Njegov primarni cilj je da unapredi razumevanje i znanje u vezi sa veštačkom inteligencijom, robotikom i novim informacionim tehnologijama, sa posebnim naglaskom na njihovoj primeni u prevenciji kriminala, promovisanju pravde i održavanju bezbednosti. Pod okriljem ovog centra, 2020. godine usvojena je značajna studija pod nazivom „Veštačka inteligencija i robotika za sprovođenje zakona“. Ova studija istražuje različite potencijalne primene ovih naprednih tehnologija u domenu sprovođenja zakona.¹⁸ Iako su se brojne zemlje zalagale za standardizaciju propisa o veštačkoj inteligenciji kroz konvenciju pod okriljem Ujedinjenih nacija, ovaj predlog ostaje na nivou pojedinačnih inicijativa.¹⁹

Ujedinjene nacije su preduzele značajne korake ka uspostavljanju sveobuhvatnog okvira za etički razvoj i primenu veštačke inteligencije (AI) kroz usvajanje ključnih rezolucija. Ove rezolucije imaju za cilj da promovišu bezbednost, bezbednost i poštovanje standarda ljudskih prava u okruženju tehnologije veštačke inteligencije koja se brzo razvija. Rezolucija usvojena 21. marta 2024. (A/RES/78/265) naglašava važnost podsticanja razvoja pouzdanih sistema veštačke inteligencije koji poštuju osnovna ljudska prava i poštuju međunarodne pravne norme. Takođe se bavi kritičnim pitanjem digitalne nejednakosti, pozivajući na povećanu saradnju među nacijama—posebno naglašavajući podršku zemljama u razvoju—kako bi se

¹⁷ Dempsey, J. (2020): *Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues*, Berkeley Center for Law & Technology.

¹⁸ Andonović, S. N. (2020): „Strateško-pravni okvir veštačke inteligencije u uporednom pravu“, *Strani pravni život*, 64(3), 116.

¹⁹ Fournier-Tombs, E. (2021): „Towards a United Nations Internal Regulation for Artificial Intelligence“, *Big Data & Society*, 8(2), DOI: 10.1177/20539517211039493.

osigurao jednak pristup prednostima veštačke inteligencije. Iako je ova rezolucija neobavezujuća, ona služi kao moralni i politički podsticaj koji podstiče odgovorne inovacije i upravljanje veštačkom inteligencijom.

Štaviše, rezolucija usvojena 24. decembra 2024. (A/RES/79/239) koncentriše se na implikacije primene veštačke inteligencije u vojnim kontekstima. Naglašava neophodnost da se obezbedi da vojne tehnologije vođene veštačkom inteligencijom funkcionišu u granicama međunarodnog humanitarnog prava, uključujući principe razlikovanja, proporcionalnosti i odgovornosti. Rešavanjem ovih zabrinutosti, rezolucija ima za cilj da spreči potencijalnu zloupotrebu veštačke inteligencije u ratu, istovremeno promovišući razvoj autonomnih sistema koji podržavaju etičke standarde. Zajedno, ove rezolucije odražavaju posvećenost UN-a usmeravanju razvoja veštačke inteligencije ka mirnim, poštenim i zakonitim ciljevima.²⁰

Prvi strateški dokument u ovoj oblasti Evropska unija je usvojila 2018. godine pod nazivom „Veštačka inteligencija za Evropu“.²¹ Primarni cilj artikulisan u pomenutom dokumentu je unapređenje tehnoloških i industrijskih sposobnosti Unije, sa posebnim naglaskom na integraciju veštačke inteligencije u čitav privredni sektor.²²

U februaru 2020. godine, Evropska komisija je objavila „Belu knjigu o veštačkoj inteligenciji — evropski pristup izvrsnosti i poverenju“, potvrđujući važnost uspostavljanja sveobuhvatnog i koherentnog pravnog okvira unutar Evropske unije za upravljanje ovim tehnološkim domenom u nastajanju.²³ U oktobru 2020. godine, nekoliko meseci nakon toga, Evropski parlament je doneo više rezolucija koje imaju za cilj regulisanje primene i primene tehnologija veštačke inteligencije:²⁴

- Rezolucija o etičkim aspektima veštačke inteligencije, robotike i srodnih tehnologija,²⁵
- Rezolucija o režimu građanske odgovornosti za veštačku inteligenciju,²⁶
- Rezolucija o pravima intelektualne svojine u vezi razvoja veštačke inteligencije.²⁷

²⁰ <https://press.un.org/en/2024/ga12588.doc.htm> (05.10.2025).

²¹ European Commission, *Artificial Intelligence for Europe*, COM (2018).

²² Prlja, D., Gasmi, G., & Korać, V. (2021): *Veštačka inteligencija u pravnom sistemu EU*, Institut za uporedno pravo, Beograd, 98.

²³ European Commission, *White Paper - A European approach to excellence and trust*, COM (2020) 65 final.

²⁴ Prlja, D., Gasmi, G., & Korać, V. (2021): *Veštačka inteligencija u pravnom sistemu EU*, Institut za uporedno pravo, Beograd, 98, 99.

²⁵ European Parliament, *Resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, 2020/2012 (INL), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html, (02.10.2025).

²⁶ European Parliament, *Resolution on a civil liability regime for artificial intelligence*, 2020/2014 (INL), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html, (01.09.2022).

²⁷ European Parliament, *Resolution on intellectual property rights for the development of artificial intelligence technologies*, 2020/2015 (INI), <https://www.europarl.europa.eu/doceo/>

- Shodno tome, proizilazeći iz pomenutih inicijativa i aktivnosti koje je Evropska unija preduzela u oblasti veštačke inteligencije, Evropski parlament i Evropski savet usvojili su 2021. godine predlog uredbe za usklađivanje pravnog okvira koji reguliše veštačku inteligenciju.²⁸ Dalji rad oko pravnog utvrđivanja konsekvenci AI nije suštinski presudan za dalje istraživanje jer se nadovezuje na navedene normative.

3.1. Ključni geopolitički trendovi i tenzije u veštačkoj inteligenciji

Brzi napredak veštačke inteligencije (AI) pojavio se kao ključna karakteristika savremene geopolitike, preoblikujući pejzaž međunarodne moći, bezbednosti i ekonomske konkurencije. Kako se nacije trče u razvoju, primeni i kontroli tehnologija VI, razvija se složena mreža strateških interesa, tehnoloških zavisnosti i normativnih debata. Ključni geopolitički trendovi i tenzije u AI obuhvataju strateške težnje velikih sila, centralnu ulogu infrastrukture i suvereniteta podataka, geopolitičke implikacije tehnoloških standarda i novu ulogu AI u asimetričnom i hibridnom ratovanju.

3.2. Dinamika velikih sila u konkurenciji AI

Globalnu trku AI prvenstveno pokreću strateški imperativi Sjedinjenih Država, Kine, Evrope i Rusije, pri čemu svaka od njih teži različitim putevima usklađenim sa svojim geopolitičkim ciljevima i tehnološkim kapacitetima.

Sjedinjene Države: SAD imaju za cilj da održe svoju tehnološku nadmoć u AI podsticanjem inovacija u okviru svog robusnog ekosistema univerziteta, firmi privatnog sektora i istraživačkih institucija. Američke kompanije poput Gugla, Majkrosofta i OpenAI su pioniri u napretku u modelima velikih jezika i neuronskim mrežama, učvršćujući vodeću poziciju SAD u fundamentalnim istraživanjima veštačke inteligencije. Pristup vlade SAD naglašava kombinaciju podsticanja inovacija, zaštite intelektualne svojine i uspostavljanja međunarodnih normi i standarda za oblikovanje globalnog upravljanja veštačkom inteligencijom. Ova strategija teži očuvanju tehnološke dominacije, a istovremeno rešavanju problema vezanih za bezbednost, privatnost i etičku upotrebu.

Kina: Kinesku strategiju za veštačku inteligenciju karakteriše fokus na tehnološku samostalnost, vođen željom da se zaobiđu ranjivosti povezane sa oslanjanjem na stranu tehnologiju, posebno usred eskalacije tenzija i sankcija između SAD i Kine. Peking naglašava razvoj domaćeg hardvera za veštačku inteligenciju, uključujući čipove i infrastrukturu za veštačku inteligenciju, kao deo svoje šire inicijative

document/TA-9-2020-0277_EN.html, (02.10.2025).

²⁸ European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, Brussels, 21.4.2021, COM(2021).

„Proizvedeno u Kini 2025“.²⁹ Kineski pristup uključuje značajnu državnu podršku startapovima za veštačku inteligenciju, integraciju veštačke inteligencije u vojne i bezbednosne sisteme i težnju ka „domaćim inovacijama“ kako bi se smanjila zavisnost od zapadne tehnologije. Kineska vlada takođe koristi ogromne domaće baze podataka za obuku modela veštačke inteligencije, ciljajući na postizanje strateškog tehnološkog pariteta i pozicioniranje Kine kao globalnog lidera u oblasti veštačke inteligencije.

Evropa: Evropska unija usvaja balansiranje, nastojeći da se takmiči sa SAD i Kinom, a da pritom zadrži svoj normativni i regulatorni suverenitet. Evropski kreatori politike naglašavaju etički razvoj veštačke inteligencije, zaštitu podataka i prava korisnika, zalažući se za „suverenitet veštačke inteligencije“ koji minimizira oslanjanje na strane platforme – posebno američke i kineske. Pristup EU podrazumeva rigoroznu regulativu, kao što je predloženi Zakon o veštačkoj inteligenciji, koji ima za cilj da uspostavi sveobuhvatne standarde za transparentnost, odgovornost i bezbednost. Dajući prioritet etičkim razmatranjima i regulatornoj kontroli, Evropa nastoji da oblikuje razvoj veštačke inteligencije na način koji je u skladu sa njenim vrednostima i da zadrži stratešku nezavisnost.

Rusija: Ruske ambicije u vezi sa veštačkom inteligencijom su relativno skromne, ali strateški usmerene na vojne i bezbednosne primene. S obzirom na ograničene resurse i tehnološke kapacitete, Rusija se koncentriše na razvoj autonomnih sistema naoružanja, alata za nadzor i mogućnosti hibridnog ratovanja. Moskva veštačku inteligenciju doživljava kao sredstvo za poboljšanje svog strateškog odvrćanja i sajber operacija, koristeći kampanje dezinformacije i sajber napade vođene veštačkom inteligencijom kako bi uticala na geopolitičke rivale. Naglasak zemlje na vojnim primenama odražava njenu širu bezbednosnu doktrinu, koja teži da iskoristi veštačku inteligenciju za asimetrične prednosti protiv tehnološki naprednih protivnika.

3.3. Kontrola nad infrastrukturom, podacima i hardverskim komponentama

Centralno za geopolitičko takmičenje u veštačkoj inteligenciji je kontrola nad kritičnom infrastrukturom, hardverom i resursima podataka. Sistemi veštačke inteligencije u velikoj meri zavise od visokoperformansnog računarskog hardvera, kao što su grafičke procesorske jedinice (GPU), tenzorske procesorske jedinice (TPU) i specijalizovani akceleratori. Kontrola izvoza ovih komponenti postala je strateški alat sličan tradicionalnim merama kontrole naoružanja. Na primer, Sjedinjene Države su uvele ograničenja kineskim proizvođačima čipova poput SMIC i Huawei, navodeći zabrinutost zbog nacionalne bezbednosti i tehnološkog širenja.

²⁹ [https://www.tanjug.rs/ekonomija/svet/192599/kineski-operator-izgradio-ogroman-centar-podataka-koji-pokrecu-domaci-ai-cipovi/vest, \(07.10.2025\).](https://www.tanjug.rs/ekonomija/svet/192599/kineski-operator-izgradio-ogroman-centar-podataka-koji-pokrecu-domaci-ai-cipovi/vest, (07.10.2025).)

Zavisnost od hardvera takođe uključuje pristup esencijalnim sirovinama. Retki zemni elementi poput litijuma, kobalta, neodimijuma i drugih ključnih minerala su osnova proizvodnje baterija, magneta i poluprovodnika. Zemlje bogate ovim resursima – poput Demokratske Republike Kongo, Australije i zemalja Centralne Azije – imaju značajan geopolitički uticaj. Kontrola nad lancima snabdevanja ovim materijalima utiče na globalni razvoj i primenu hardvera za veštačku inteligenciju, često pogoršavajući tenzije vezane za resurse.

Podaci, koji se često opisuju kao „novo gorivo“ veštačke inteligencije, podjednako su važni. Sposobnost prikupljanja, obrade i kontrole ogromnih skupova podataka pruža značajne konkurentske prednosti, omogućavajući obuku sofisticiranih i preciznijih modela veštačke inteligencije. Zemlje sa velikim, raznovrsnim i pristupačnim skupovima podataka – poput SAD i Kine – mogu ubrzati inovacije veštačke inteligencije, stvarajući povratnu spregu koja jača tehnološko liderstvo. S druge strane, zabrinutost oko suvereniteta podataka dovela je do napora da se ograniče prekogranični tokovi podataka, obaveže lokalno skladištenje podataka i uspostave nacionalni fondovi podataka, što sve utiče na globalno upravljanje podacima i strukture moći.

3.4. Normativno i standardno definisanje postulata u veštačkoj inteligenciji

Međunarodne norme i standardi su od vitalnog značaja za oblikovanje budućnosti upravljanja veštačkom inteligencijom. Kontrola nad ovim normama pruža značajan strateški uticaj. Debate se vrte oko pitanja transparentnosti, odgovornosti, bezbednosti i interoperabilnosti. Zemlje i regioni se značajno razlikuju u svojim pristupima: dok SAD i Kina daju prioritet brzim inovacijama – ponekad na račun sveobuhvatne regulacije – Evropa se zalaže za oprezan, etički utemeljen razvoj.

Zalaganje Evropske unije za regulatorne okvire, kao što je predloženi Zakon o veštačkoj inteligenciji, ilustruje napore da se etički standardi ugrade u tkivo razvoja veštačke inteligencije. Ovi standardi imaju za cilj da spreče zloupotrebu, obezbede ljudski nadzor i podstaknu poverenje. Međutim, takva regulativa može takođe delovati kao prepreka inovacijama ili stvoriti regulatornu fragmentaciju, komplikujući međunarodnu saradnju.

U međuvremenu, Sjedinjene Države nastoje da utiču na globalne standarde putem multilateralnih organizacija i bilateralnih sporazuma, naglašavajući upravljanje vođeno inovacijama. Kina promovise sopstvene standarde usklađene sa svojim razvojnim prioritetima, nastojeći da proširi svoj uticaj na novonastale globalne norme.

3.5. Uloga veštačke inteligencije u asimetričnom i hibridnom ratovanju

Strateški značaj veštačke inteligencije proteže se izvan ekonomskih i normativnih dimenzija na vojnu i bezbednosnu sferu. Njena sposobnost da pojača asimetrične i hibridne pretnje povećala je tenzije i uvela nove ranjivosti.

Autonomni sistemi naoružanja, uključujući dronove i robotske platforme, prete da snize prag za sukob i zakomplikuju odvracanje. Zemlje poput Rusije i Kine razvijaju vojna sredstva omogućena veštačkom inteligencijom koja mogu da deluju polunezavisno, što podiže etičke i strateške zabrinutosti oko odgovornosti i eskalacije.

Sajber ratovanje je još jedna oblast u kojoj veštačka inteligencija igra transformativnu ulogu. Sajber napadi vođeni veštačkom inteligencijom mogu da identifikuju ranjivosti, automatizuju pokušaje upada i da se prilagode odbrani u realnom vremenu. Ove mogućnosti povećavaju rizik od destabilizacije sajber sukoba, posebno kada se kombinuju sa dezinformacijskim kampanjama i manipulacijom društvenim medijima – fenomenima koji se često pojačavaju kroz tehnologiju dipfejkova i sadržaj generisan veštačkom inteligencijom.

Dezinformacijske i propagandne kampanje, podržane dipfejkovima generisanim veštačkom inteligencijom, predstavljaju značajan rizik za demokratske procese i društvenu stabilnost.³⁰ Zemlje koriste veštačku inteligenciju da bi uticale na javno mnjenje, destabilizovale protivnike i sprovodile tajne operacije – dodajući novu dimenziju hibridnom ratovanju.

Pristup Republike Srbije hibridnim pretnjama i kroz AI, kao i njeni širi međunarodni odnosi značajno su oblikovani dinamičnom interakcijom velikih globalnih sila, posebno Kinesko-SAD u razvoju. odnos. Od 2008. godine, tenzije između Sjedinjenih Država i Kine su se intenzivirale, koje karakteriše niz sankcija, ograničenja i strateških konfrontacija koje su, u mnogim aspektima, prevazišle rivalstvo uočeno tokom ere Hladnog rata. Kina je značajno proširila svoj uticaj kroz sveobuhvatna ulaganja u infrastrukturu, tehnologiju i odbranu, čime je ojačala svoje geopolitičko prisustvo u različitim regionima. Ono što je važno, Peking je nastojao da izbegne direktno angažovanje u sukobima u stilu hladnog rata, umesto toga sledi strategiju ekonomske diplomatije i projekcije meke moći. Ova dešavanja utiču na geopolitičku perspektivu Srbije tako što naglašavaju važnost snalaženja u složenom međunarodnom okruženju koje je obeleženo konkurencijom velikih sila. Srbija, stoga, zauzima oprezan stav, dajući prioritet nacionalnom suverenitetu i bezbednosti, istovremeno prepoznajući neophodnost održavanja konstruktivnih odnosa i sa Kinom i sa Sjedinjenim Državama. Ovo nijansirano pozicioniranje naglašava strateški naglasak Srbije

³⁰ <https://cybercrime.rs/2023/09/19/dipfejkovi-vestacka-inteligencija-i-protesti-kada-je-istina-pod-znakom-pitanja/>, (07.10.2025).

na balansiranju spoljnih uticaja kako bi se očuvala njena stabilnost i suverenitet usred promenljive globalne dinamike moći.³¹

Geopolitički pejzaž veštačke inteligencije karakteriše intenzivna konkurencija, strateška kontrola resursa, normativne borbe i širenje naprednih vojnih i sajber kapaciteta. Velike sile se bore za tehnološku dominaciju, uticaj na globalne standarde i kontrolu nad kritičnom infrastrukturu i podacima. Ove težnje su inherentno isprepletene, stvarajući složenu mrežu tenzija i ranjivosti koje ugrožavaju međunarodnu stabilnost. Kako se veštačka inteligencija nastavlja razvijati, važnost normativnih okvira, multilateralne saradnje i strateškog ograničenja postaje sve važnija za sprečavanje trke u naoružanju ili destabilizujućih sukoba koje omogućava veštačka inteligencija. Razumevanje ovih ključnih trendova i tenzija je neophodno za kreatora politike, tehnologe i naučnike koji žele da se snađu u budućnosti globalnog upravljanja i bezbednosti veštačke inteligencije.

4. ZAKLJUČAK

U radu je pokazano da digitalna transformacija, sa veštačkom inteligencijom u središtu, predstavlja ključni izazov savremenog međunarodnog sistema — ne samo u tehnološkom i ekonomskom, već i u pravnom, bezbednosnom i geopolitičkom smislu. Brzi razvoj digitalnih tehnologija izmenio je tradicionalne paradigme suvereniteta, bezbednosti i međunarodne odgovornosti, otvarajući nova pitanja o primeni međunarodnog prava u digitalnom prostoru.

Geopolitički aspekt veštačke inteligencije ukazuje na intenzivnu trku velikih sila (SAD, Kina, EU, Rusija) za dominaciju u razvoju, kontroli i standardizaciji AI tehnologija. Ta konkurencija ne oblikuje samo tehnološki napredak, već i globalnu preraspodelu moći, u kojoj kontrola nad podacima, infrastrukturnim kapacitetima i normativnim okvirima postaje strateški resurs.

Evropska unija nastoji da izgradi etički i regulatorno zasnovan pristup, usklađen sa zaštitom ljudskih prava i vladavinom prava, dok SAD i Kina favorizuju inovaciju i brz razvoj radi očuvanja globalnog uticaja. Rusija, s druge strane, koristi AI pretežno u bezbednosne i vojne svrhe, naglašavajući dimenziju asimetričnih i hibridnih pretnji.

U takvom kontekstu, međunarodno pravo i globalne institucije, pre svega Ujedinjene nacije, imaju presudnu ulogu u formiranju univerzalnih normi i etičkih smernica koje bi sprečile militarizaciju i zloupotrebu AI. Rezolucije UN iz 2024.

³¹ Lović, V. Stojanović, M. (2024): „Odnos sistema nacionalne bezbednosti Republike Srbije prema savremenim hibridnim pretnjama“, *Megatrend revija*, Vol. 21, № 2, 2024, Megatrend univerzitet, Beograd, 137 – 140. DOI: 10.5937/MegRev2402135L

godine (A/RES/78/265 i A/RES/79/239) potvrđuju važnost globalne saradnje i odgovorne primene veštačke inteligencije u skladu sa međunarodnim humanitarnim i ljudskim pravom.

Zaključno, budućnost međunarodne bezbednosti zavisi od sposobnosti država i međunarodnih organizacija da uspostave ravnotežu između tehnološkog napretka i etičke odgovornosti, između inovacije i regulacije. Samo kroz multilateralnu saradnju, transparentnost i zajedničke standarde, moguće je obezbediti da razvoj veštačke inteligencije doprinese miru, stabilnosti i održivom razvoju — umesto novim oblicima globalne nejednakosti i sukoba.

LITERATURA

- Andonović, S. N. (2020): “Strateško-pravni okvir veštačke inteligencije u uporednom pravu”, *Strani pravni život*, 64(3).
- Bainbridge, D. (2000): *Introduction to Computer Law*, Longman.
- Baltezarević, R. (2023): “Uticaj veštačke inteligencije na globalnu ekonomiju”, *Megatrend revija*, Vol. 20, № 3, 2023, Megatrend univerzitet, Beograd. DOI: 10.5937/MegRev2303013B
- BALTEZAREVIC, B., MILUTINOVIC, O., BALTEZAREVIC, R., & BALTEZAREVIC, V. (2020). Digital storage and online mediated memory. *International Review*, (1-2), 34-41.
- *Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions 2030 Digital Compass: the European way for the Digital Decade*, COM/2021/118.
- Council of Europe (2016): *Internet governance – Council of Europe strategy 2016–2019*, <https://rm.coe.int/internet-governance-strategy-2016-2019-updated-version-06-mar-2018/1680790ebe> (07.10.2025).
- Dempsey, J. (2020): *Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues*, Berkeley Center for Law & Technology.
- European Commission, *White Paper - A European approach to excellence and trust*, COM (2020) 65 final.
- European Parliament, *Resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, 2020/2012 (INL), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html (02.10.2025).
- European Parliament, *Resolution on a civil liability regime for artificial intelligence*, 2020/2014 (INL), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html (01.09.2022).

- European Parliament, *Resolution on intellectual property rights for the development of artificial intelligence technologies*, 2020/2015(INI), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html, (02.10.2025).
- European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial intelligence Act) and Amending Certain Union Legislative Acts*, Brussels, 21.4.2021, COM(2021).
- Koch, B. A. (2020): "Liability for Emerging Digital Technologies: An Overview", *Journal of European Tort Law*, 11(2).
- European Commission, *Artificial Intelligence for Europe*, COM (2018).
- Lović, V. Stojanović, M. (2024): "Odnos sistema nacionalne bezbednosti Republike Srbije prema savremenih hibridnim pretnjama", *Megatrend revija*, Vol. 21, № 2, 2024, Megatrend univerzitet, Beograd, 137 – 140. DOI: 10.5937/MegRev2402135L
- Zirojević, I. (2024): "Veštačka inteligencija – bezbednosni, tehnološki i pravni aspekti", *Megatrend revija*, Vol. 21, № 2, 2024, Megatrend univerzitet, Beograd. DOI: 10.5937/MegRev2402093Z
- Prlja, D., Reljanović, M., & Ivanović, Z. (2012): *Internet pravo*, Institut za uporedno pravo, Beograd.
- *Oblikovanje digitalne budućnosti Evrope (Shaping Europe's digital future*, 1 – 9 February 2020.), https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en (07.10.2025).
- Vuletić, D., & Đorđević, B. (2021): "Problemi i izazovi upravljanja internetom na međunarodnom nivou", *Međunarodni problemi = International problems*, 73, 235.
- United Nations (2019): *Declaration of digital interdependence*, <https://news.un.org/en/story/2019/06/1040131> (07.10.2025).
- UNDP, *Digital Strategy 2022-2025*, <https://digitalstrategy.undp.org/> (01.10.2025).
- United Nations (2021): *The promotion, protection and enjoyment of human rights on the Internet : resolution / adopted by the Human Rights Council on 13 July 2021*, A/HRC/RES/32/13.
- United Nations (1975): "Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind", *Proclaimed by General Assembly resolution 3384 (XXX) of 10 November 1975*.
- Filipovski Z., Galetin M. (2022): "Uloga Saveta Evrope u kreiranju pravne regulative u oblasti veštačke inteligencije", *Zbornik radova XIX Međunarodnog naučnog supa „Pravnički dani – prof. dr Slavko Carić“ pod nazivom „Pravo, nauka i društvo – aktuelna pitanja i perspektive“*, Pravni fakultet za privredu i pravosuđe u Novom Sadu.

- Fournier-Tombs, E. (2021): "Towards a United Nations Internal Regulation for Artificial Intelligence", *Big Data & Society*, 8(2), DOI: 10.1177/20539517211039493.
- <https://press.un.org/en/2024/ga12588.doc.htm>, (05.10.2025).
- <https://www.tanjug.rs/ekonomija/svet/192599/kineski-operatar-izgradio-ogroman-centar-podataka-koji-pokrecu-domaci-ai-cipovi/vest>, (07.10.2025).
- <https://cybercrime.rs/2023/09/19/dipfejkovi-vestacka-inteligencija-i-protesti-kada-je-istina-pod-znakom-pitanja/> (07.10.2025).

CHALLENGES OF THE DIGITAL ENVIRONMENT: INTERNATIONAL LEGAL, GEOPOLITICAL AND SECURITY ASPECTS

Abstract: *This paper critically examines the profound impact of digital technologies, with a particular focus on artificial intelligence (AI), on the domains of international law, geopolitics and security in the context of the Fourth Industrial Revolution. The ongoing digital transformation has triggered transformative changes in the economic, social and security spheres, while at the same time posing complex challenges regarding sovereignty, state accountability and cyber law. As digital innovations permeate global interactions, issues related to the regulation and governance of AI are becoming increasingly prominent, requiring the development of comprehensive legal and ethical frameworks.*

In response to these emerging issues, the European Union (EU) and the United Nations (UN) have undertaken efforts to establish normative guidelines for the responsible development and application of AI technologies. Specifically, the analysis examines key UN resolutions—A/RES/78/265 and A/RES/79/239—that emphasize the importance of ensuring the security of AI and advocate for the demilitarization of such technologies. These resolutions reflect a concerted international effort to mitigate the risks associated with the proliferation of AI and to promote its peaceful and ethical uses.

Moreover, the paper explores the geopolitical competition among major powers, particularly the United States, as they seek to establish technological leadership while addressing security concerns related to AI. This competition impacts international legal norms and security strategies, highlighting the critical need for multilateral cooperation to address the challenges of managing AI in a rapidly evolving global environment.

Keywords: *artificial intelligence, digital transformation, geopolitics, international law, security*

SPISAK RECENZENATA / LIST OF REVIEWERS

Prof. dr BALTEZAREVIĆ Vesna – Srbija
Prof. dr BALTEZAREVIĆ Radoslav – Srbija
Prof. dr BAZIĆ Miljojko – Srbija
Prof. dr BOGIĆEVIĆ Jasmina, vanredni profesor – Srbija
Doc. dr BRČIĆ Aleksandar - BiH
Prof. dr CVETKOVSKI Tatjana – Srbija
Prof. dr CVIJANOVIĆ Gorica – Srbija
Prof. dr CVIJANOVIĆ Drago – Srbija
Prof. dr DAVIDOV Vladimir – Rusija
Prof. dr DE MONSERAT LJAJO Marija – Argentina
Prof. dr ĐURĐEVIĆ Dragan – Srbija
Prof. dr ILIĆ Radan – Srbija
Prof. dr JOVANOVIĆ Tomislav – Srbija
Doc. dr JOVIČIĆ Aleksandar – Srbija
Akademik KAMBOVSKI Vlado – Makedonija
Prof. dr KAPOR Nenad - Srbija
Prof. dr KOMARISOV Vladimir S. – Rusija
Dr LABOVIĆ Dragana, vanredni profesor – Srbija
Prof. dr LAĐEVAC Ivona – Srbija
Prof. dr LANGOVIĆ-MILIĆEVIĆ Ana – Srbija
Prof. dr LAZAREVIĆ Žarko – Slovenija
Prof. dr LENGHARTOVA Jana – Slovačka
Prof. dr LUTOVAC Jelena – Srbija
Prof. dr LESAKOVA Dagmar – Slovačka
Doc. dr MANDARIĆ Marija – Srbija
Prof. dr MILANOVIĆ R. Milan – Srbija
Prof. dr MILIVOJEVIĆ Tatjana – Srbija
Prof. dr NIKODIJEVIĆ Dragan – Srbija
Prof. dr NOVAKOVIĆ Ivan – Srbija
Akademik OČIĆ Časlav – Srbija
Prof. dr OZGERCIN Kevin V. – SAD
Prof. dr PAP Norbert – Mađarska
Prof. dr PARK Sung-Đo – Nemačka
Prof. dr PAVLOVIĆ Milivoje – Srbija
Prof. dr PERIŠIĆ Saša – Srbija
Prof. dr POPOVIĆ Borko – Srbija
Dr PREMOVIĆ Jelena, naučni saradnik
Prof. dr SALVATORE Dominik – Italija
Doc. dr SPASIĆ Dragoljub - Srbija

Prof. dr ŠANARON Žan Žak – Francuska
Prof. dr ŠARIĆ Branko – Srbija
Prof. dr ŠKULIĆ Milan – Srbija
Prof. dr TANČIĆ Dragan – Srbija
Prof. dr VESELINOVIĆ Petar – Srbija
Prof. dr VUJIČIĆ Milan – Srbija
Prof. dr ZENOVIĆ Ivona - Srbija
Dr ZIMONJIĆ Marijana – Srbija
Prof. dr ŽIVANOVIĆ Vladimir – Srbija

OSNOVNE INFORMACIJE O ČASOPISU I UPUTSTVO ZA AUTORE

I. OSNOVNE INFORMACIJE O ČASOPISU

1. Opšte. – „Megatrend revija“ je naučno glasilo Megatrend univerziteta (Megatrend University).

Časopis je, prema klasifikaciji CEON visoko pozicioniran kao vodeći nacionalni naučni časopis u Republici Srbiji (M51) i prema klasifikaciji Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije (M52).

„Megatrend revija“ izlazi od 2004. godine, na srpskom i engleskom jeziku. Otvorena je za sve kvalitetne radove i autore iz čitavog sveta. Ima međunarodnu redakciju i međunarodni izdavački savet. Putem razmene i na druge načine, stiže do čitalaca i van granica Srbije.

Časopis „Megatrend revija“ je interdisciplinarni časopis iz oblasti društvenih nauka, u kojem se objavljuju radovi iz sledećih tematskih oblasti:

- Ekonomija
- Pravo
- Politika i bezbednost
- Menadžment i marketing
- Međunarodni odnosi
- Javne politike
- Informaciono društvo
- Komunikacije i kultura
- Umetnost i dizajn
- Saobraćajno inženjerstvo

2. Recenzije. - Svaki rad se recenzira od strane dva recenzenta. Radovi su podložni proverbi na plagijat.

Rad koji dobije pozitivnu recenziju oba recenzenta objavljuje se u skladu sa standardnom kategorizacijom radova u naučnim časopisima kao: originalni naučni rad, pregledni naučni članak, stručni članak, saopštenje ili osvrt, prikaz knjige i prevod.

O kategorizaciji rada odlučuju recenzenti i glavni urednik, s tim da se u slučaju sumnje prihvata rešenje koje je povoljnije za autora (ako je jedan recenzent kategorisao rad na jedan, a drugi recenzent na drugi način, prihvatiće se viša kategorizacija).

U slučaju da jedan recenzent predloži da se rad objavi, a drugi da se ne objavi, rad se daje na recenziju trećem recenzentu i njegova odluka je konačna.

3. Anonimnost autora i recenzenata. - Redakcija se strogo drži pravila o međusobnoj anonimnosti autora i recenzenata. Drugim rečima, recenzenti ne znaju ko je i odakle je autor rada, kao što ni autor ne zna imena recenzenata. Pored ostalog, autor koji nije zadovoljan načinom na koji su recenzenti vrednovali njegov rad, ima pravo da dobije na uvid recenzije, ali bez imena recenzenata.

II. ORIGINALNOST RADA I BORBA PROTIV PLAGIJATA

Molimo autore da imaju u vidu sledeće.

1. Pisana potvrda o tome da je rad originalan. - Prilikom dostavljanja rukopisa autor je dužan da u pisanom obliku potvrdi da je njegov rad originalan, tj. da već nije negde drugde objavljen. Radovi koji budu poslani bez pisane potvrde autora o tome da je reč o originalnom delu, neće biti uzimani u obzir.

2. Rad koji je već negde prethodno objavljen. - Ako iz nekog razloga kandiduje rad koji je već negde objavljen (u inostranstvu, na stranom jeziku), autor je dužan da precizno navede gde je rad objavljen (u kom časopisu, kom broju, na kojim stranama) i da priloži pisanu saglasnost redakcije časopisa u kome je rad prvobitno objavljen. Ukoliko su ispunjeni ovi uslovi, a Redakcija „Megatrend revije“ (dalje: „Revija“) zaključi da je rad iz nekog razloga posebno interesantan i da ga treba objaviti, rad će biti objavljen, s tim što će biti naznačeno gde je prvi put objavljen i da se štampa uz odobrenje.

Ukoliko je, međutim, rad već negde objavljen, a predat je za objavljivanje u „Reviji“ bez informacije o tome, rad neće biti objavljen. Uz to, kao sankcija za nekorektan odnos, u prvom narednom broju „Revije“ u posebnoj rubrici biće objavljena informacija o tome da je odnosni autor na nekorektan način pokušao da ponovo objavi isti rad. Takođe, radovi istog autora neće se ubuduće objavljivati u „Reviji“.

3. Plagijat. - U slučaju da redakcija „Revije“ sama ili posredstvom recenzenta otkrije da je rad koji je predat za objavljivanje plagijat, u prvom narednom broju „Revije“ u posebnoj rubrici biće objavljena informacija o tome da je odnosni autor predao rad koji je plagijat, i biće navedeno originalno delo iz kog je plagijat uzet. Takođe, radovi istog autora neće se ubuduće objavljivati u „Reviji“. Po potrebi, biće obavešteni autor čiji je rad prepisan odn. redakcija časopisa u kome je objavljen originalni rad.

III. UPUTSTVO ZA AUTORE

Radove treba pripremiti u skladu sa sledećim uputstvom:

1. Rukopis

Rukopis se predaje u elektronskom obliku (MS Word). Predviđeni format stranice je A4, font Times New Roman (veličina 12 pt za tekst, uključujući i apstrakt, bez proreda). Radovi na srpskom jeziku se dostavljaju u srpskoj latinici. Rad se šalje na e-mail adresu: megatrendrevija@megatrend.edu.rs

Uz rad se obavezno dostavlja i pisana izjava autora o tome da je rad originalno delo (potpisan i skenirana izjava), ORCID broj i godine rođenja za sve autore.

Uslov da rad uđe u proceduru recenziranja jeste da u potpunosti zadovoljava tehničke kriterijume koji su propisani ovim uputstvom. Rad mora biti lektorisan, tj. mora da zadovoljava jezičke i pravopisne standarde srpskog odnosno engleskog jezika.

2. Broj autora

Prednost imaju članci koje je napisao samo jedan autor (autor pojedinac), ali redakcija sprovodi aktuelne propise (*Pravilnik o postupku i načinu vrednovanja, i kvantitativnom iskazivanju naučnoistraživačkih rezultata istraživača*, Službeni glasnik RS br. 24/2016 i 21/2017), po kojima se rad prihvata ako nema više od tri koautora.

3. Jezik

Tekst se predaje na srpskom ili engleskom jeziku. Ako bude prihvaćen, biće objavljen na jeziku na kome je predat.

Izuzetno, redakcija ima pravo da zbog posebno opravdanih razloga odluči da se tekst koji je predat na srpskom prevede i objavi na engleskom jeziku, ili obrnuto.

4. Obim

Članak treba da ima približno 30.000 slovnih znakova, računajući i beline (1 autorski tabak). On može da bude i nešto kraći odn. nešto duži, s tim da broj slovnih znakova sa belinama ne bude manji od 20.000 niti veći od 45.000.

Iz naročito opravdanih razloga (poseban društveni značaj teme, koautorstvo nekoliko međunarodno priznatih naučnika i sl.), redakcija izuzetno može dozvoliti i objavljivanje članka većeg obima, ali ne većeg od 2,5 autorska tabaka (75.000 slovnih znakova).

5. Tabele i formule

Tabele praviti isključivo alatom za tabele u programu MS Word. Tabele moraju da imaju naslove i biti numerisane arapskim ciframa.

Formule raditi uz pomoć editora formula u programu MS Word.

6. Grafički prilozi i fotografije

Grafički prilozi mogu se predati nacrtani na papiru ili u elektronskom obliku. Kada se crteži predaju u elektronskom obliku, to treba da je u nekom od sledećih formata: EPS, AI, CDR, TIF ili JPG. Ako autor ne zna ili koristi neki specifičan program, potrebno je da se dogovori o formatu zapisa sa tehničkim urednikom. **Ne treba crtati crteže u programu MS Word!**

Fotografije moraju biti jasne, kontrastne i neoštećene. Autoru se ne preporučuje da slike skenira sam, već da taj osetljivi posao prepusti redakciji.

Ako u verziju na papiru nisu uključeni crteži i fotografije, moraju se jasno obeležiti mesta gde treba da se nalaze. Oznake u tekstu moraju se poklapati sa onima na priloženim slikama (ili fajlovima).

Crteži i fotografije moraju da imaju potpise i da budu numerisani arapskim ciframa.

7. Organizacija rukopisa

Članak mora da sadrži sledeće elemente i to ovim redom:

1. Podatke o autoru. - Ime i prezime, zvanje (titula) autora, naziv institucije u kojoj je autor zaposlen (afilijacija); obavezno navesti e-mail adresu autora i ORCID broj.

2. Naslov rada. - Naslov treba da je jasan i precizan.

3. Sažetak (apstrakt). - To je kratak informativni prikaz sadržaja članka, koji sadrži cilj istraživanja, metode, rezultate i zaključak. Treba da je na istom jeziku na kome je napisan i sam rad. U pogledu obima, treba da ima od 100 do 250 reči odn. 4 do 8 rečenica ili od jedne trećine do polovine štampane strane i da stoji između naslova rada i ključnih reči, nakon kojih sledi tekst članka.

4. Ključne reči. - Predstavljaju termine ili fraze koji najbolje opisuju sadržaj članka. Dozvoljeno je navesti do pet reči odn. fraza.

5. Tekst članka. - Centralni deo predstavlja tekst članka u kojem autor uz upotrebu odgovarajuće aparature obrađuje određeni naučni problem.

6. Popis korišćene literature. - Posle teksta članka, daje se popis korišćene literature i to abecednim redom po prezimenima autora. Navodi se isključivo literatura koja je citirana u radu.

Popis se daje prema Uputstvu za citiranje, s tim da se godina izdanja stavlja odmah iza imena autora odn. urednika. Na kraju navođenja članka ili rada u zborniku navode se stranice na kojima se nalazi citirani rad.

Primeri:

- Knjiga: Akehurst Michael (1984): *A Modern Introduction to International Law*, London
 - Poglavlje u knjizi više autora: Buchanan Allen (2010): "The Legitimacy of International Law", 79-96, in: Besson Samantha, Tasioulas John (eds.): *The Philosophy of International Law*, Oxford

- Članak: Osakwe Chris (1971): "Contemporary Soviet Doctrine on the Juridical Nature of Universal International Organizations", *American Journal of International Law* 3/1971, 502-521

Radovi istog autora navode se hronološkim redom, a ako se navodi više radova istog autora objavljenih u istoj godini, uz godinu izdanja dodaju slova "a", "b", "c" itd.

Primeri:

- Cassese Antonio (1999a): "Ex iniuria ius oritur. Are We Mowing towards International Legitimation of Forcible Humanitarian Countermeasures in the World Community?", *European Journal of International Law*, 1/1999, 23-30

- Cassese Antonio (1999b): "A Follow-Up: Forcible Humanitarian Countermeasures and Opinio Necessitatis", *European Journal of International Law*, 4/1999, 791-799

7. Rezime (Summary). - Na samom kraju daje se rezime tj. sažetak rada, koji može biti isti kao i sažetak (apstrakt), ali može biti i nešto većeg obima, ali ne više od 1 strane. Ako je rad pisan na srpskom jeziku, obavezno se dostavlja rezime na engleskom jeziku.

8. Nivoi naslova. - Zavisno od konkretnog teksta naslovi imaju različite nivoe, s tim da se koristi sledeći metod:

1. Prvi nivo naslova

(sredina, regular, bold, arapski brojevi)

1.1. Drugi nivo naslova

(sredina, italik, arapski brojevi)

1.1.1. Treći nivo naslova

(iznad početka pasusa, italik, arapski brojevi)

Za slučaj da ipak nešto nije jasno, autorima se savetuje da pogledaju prethodne brojeve „Megatrend revije“ ili da se obrate direktno sekretaru ili tehničkom uredniku časopisa.

Redakcija zadržava pravo da, u zavisnosti od specifičnosti teksta, a u cilju njegove bolje preglednosti, uredi naslove na nešto drugačiji način, ostajući u osnovnim okvirima izložene deobe naslova.

9. Citiranje. - Korišćenu literaturu citirati prema niže izloženom uputstvu za citiranje.

10. Adresa redakcije. - Radovi se šalju u elektronskoj formi na sledeću e-mail adresu: **megatrendrevija@megatrend.edu.rs**

Redakcija „Megatrend revije / Megatrend Review“
Megatrend univerzitet
Bulevar Mihajla Pupina 117
11070 Beograd

IV. UPUTSTVO ZA CITIRANJE

1. Opšta pravila

1. Ime autora. - Navodi se prvo prezime, pa ime autora. Ako postoji srednje slovo, ono se navodi između prezimena i imena.

Primer: Shaw N. Malcolm

2. Više autora. - Ako postoji više autora rada, razdvajaju se zapetama.

Primer: Simma Bruno, Alston Philip

Ako je više od 3 autora rada, navodi se prezime i ime samo prvog autora i dodaje se kurzivom (italikom) et al. (od *et alia*).

Primer: Henkin Louis et. al. (1993): *International Law: cases and Materials*, St. Paul. Minn.

3. Strane. - Kada se navodi određena strana (knjige, članka), ona se navodi samo brojem bez ikakvih dodataka (s., str., p., pp., стр., S., i sl.).

Primer: Akehurst Michael (1984): *A Modern Introduction to International Law*, London, 9.

4. Fusnote. - Kada se navodi fusnota, iza broja strane piše se skraćenica „fn“ i onda navodi broj citirane fusnote.

Primer: Akehurst Michael (1984): *A Modern Introduction to International Law*, London, 9, fn 2.

5. Ponovno citiranje istog rada. - Kada se rad koji je već citiran ponovo navodi, to se vrši tako što se navodi prezime i ime autora, pa iza toga, razdvojeno zapetom, stranica koja se citira. Sve bez korišćenja op. cit., nav. delo i slično.

Primer: Akehurst Michael, 15.

Ako je navedeno nekoliko radova istog autora, navodi se prezime i ime autora, u zagradi godina u kojoj je odnosni rad objavljen i strana.

Primer: Akehurst Michael (1984), 15.

Ako je navedeno nekoliko radova istog autora objavljenih u istoj godini, radovi se u spisku korišćene literature (koji se obavezno daje na kraju rada) iza godine publikovanja dopunski obeležavaju latiničnim slovima „a“, „b“, „c“ itd. i tako navode kod citiranja u fusnotama.

Primer: Akehurst Michael (1984a), 15.

6. Ponovno citiranje prethodno citiranog rada. - Ako se citira podatak sa iste strane istog dela koje je citirano u prethodnoj fusnoti, koristi se samo latinična skraćenica Ibid. (od ibidem), bez navođenja bilo kakvih drugih podataka.

Primer: Ibid.

Ako se citira podatak iz dela koje je citirano u prethodnoj fusnoti, ali sa različite strane, navodi se Ibid, a zatim zapeta i broj strane.

Primer: Ibid, 54.

7. Strana imena. - U radovima koji se predaju na srpskom jeziku, strana imena se transkribuju na srpski jezik, kako se izgovaraju, a prilikom prvog pominjanja u tekstu njihovo ime i prezime navode se u zagradi u izvornom obliku.

Primer: Tomas Hobs (Thomas Hobbes)

2. Knjige

1. Opšte. - Knjige se navode na sledeći način: 1) prezime autora, 2) njegovo ime, 3) godina izdanja (u zagradi), 4) dve tačke, 5) naziv knjige kurzivom (italikom), 6) mesto izdanja kurentom (obično), 7) strana (bez ikakvih dodataka), 8) fusnota koja se citira.

Ako se navodi i izdavač, piše se kurentom (obično) pre mesta izdanja.

Primer: Scott V. Shirley (2010): International Law in World Politics, Lynne Rienner Publishers Inc., Boulder – London, 71, fn 45.

2. Više izdanja. - Ako knjiga ima više izdanja može se (ne mora) navesti broj izdanja u superskriptu.

Primer: Scott V. Shirley (2010²): International Law in World Politics, Lynne Rienner Publishers Inc., Boulder - London (objašnjenje: 2010² - drugo izdanje, objavljeno 2010)

3. Urednici. - Ako knjiga ima jednog ili više urednika, prvo se navode prezimena i imena urednika, razdvojena zapetama, zatim naznaka „(ur.)“ odnosno „ed.“ ili (ako ih je više) „eds.“, pa godina izdanja u zagradi, dvotačka, naziv knjige kurzivom (italikom), i mesto.

Primer: Besson Samantha, Tasioulas John (eds.) (2010): The Philosophy of International Law, Oxford.

Ako je broj urednika veći od tri, navode se podaci samo za prvog urednika, zatim se posle zapete navodi „et al.“ i posle toga se navodi „ur.“.

Primer: Hamilton P. et al. (eds.) (1999): The Permanent Court of Arbitration: International Arbitration and Dispute Resolution, Kluwer International, The Hague-London-Boston.

4. Poglavlje u knjizi. - Poglavlje u knjizi koja ima urednika navodi se tako što se: 1) navode prezime i ime autora, 2) godina izdanja u zagradi, 3) dve tačke, 4) naziv poglavlja kurentom (pod navodnicama), 5) zapeta, 6) brojevi strana koje se citiraju, 7) „u“ odn. „in“, 8) prezime i ime urednika, 9) „(ur.)“ odn. „(eds.)“, 10) naziv knjige u kojoj je citirano delo, kurzivom (italikom) i 11) mesto izdanja.

Primer: Buchanan Allen (2010): “The Legitimacy of International Law”, 79-96, in: Besson Samantha, Tasioulas John (eds.): The Philosophy of International Law, Oxford.

3. Članci

1. Opšte. - Članci se navode na sledeći način: 1) prezime autora, 2) ime autora, 3) godina izdanja, 4) dve tačke, 5) naziv članka kurentom (obično) pod navodnicama, 6) naziv časopisa (zbornika i sl.) kurzivom (italikom), 7) broj i godište spojeni kosom crtom, 8) broj strane (bez ikakvih dodataka), 9) broj citirane fusnote.

Primer: Osakwe Chris (1971): "Contemporary Soviet Doctrine on the Juridical Nature of Universal International Organizations", *American Journal of International Law* 3/1971, 502, fn 1.

2. Skraćenica naziva časopisa. - Ako je naziv časopisa (zbornika i sl.) dug, prilikom prvog citiranja u zagradi sa navodi skraćenica pod kojom će se časopis (zbornik i sl.) nadalje pojavljivati.

Primer: Osakwe Chris (1971): "Contemporary Soviet Doctrine on the Juridical Nature of Universal International Organizations", *American Journal of International Law (AJIL)* 3/1971, 502-521.

4. Propisi

1. Opšte. - Propisi se navode na sledeći način: 1) naziv propisa se navodi u kurentu (obično), 2) kurzivom (italikom) navodi se glasilo u kojem je propis objavljen, 3) na kraju se navodi broj i godina glasila u kojem je propis objavljen.

Primer: Zakon o osnovama uređenja službi bezbednosti Republike Srbije, *Službeni glasnik Republike Srbije*, 116/2007.

2. Ponovno pominjanje propisa. - Ako se propis pominje kasnije, prilikom njegovog prvog pominjanja navodi se u zagradi njegov skraćeni naziv, s tim da se ispred skraćenog naziva stavlja objašnjenje „u daljem tekstu“.

Primer: Zakon o osnovama uređenja službi bezbednosti Republike Srbije (u daljem tekstu: Zakon o službama bezbednosti), *Službeni glasnik Republike Srbije*, 116/2007.

3. Izmene i dopune. - Ako je propis naknadno menjan i dopunjavan, navode se jedan za drugim brojevi i godine glasila u kojima su objavljeni izvorni tekst odn. izmene i dopune.

Primer: Zakon o osnovama uređenja službi bezbednosti Republike Srbije, *Službeni glasnik Republike Srbije*, 116/2007, 72/2012.

4. Članovi, stavovi i tačke propisa. - Članovi, stavovi, tačke (alineje) itd. propisa navode se kroz kosu crtu, tako što se prvo navodi broj člana, zatim stava, pa alineje itd.

Primer: Konvencija UN o pravu mora (1982) čl. 1/1/5/a/i.

5. Tekstovi sa interneta

Citiranje tekstova sa interneta treba da sadrži: 1) ime autora citiranog teksta (ako je reč o autorskom tekstu), 2) naziv citiranog teksta pod navodnicima, 3) podatke o tome gde je tekst objavljen (ako je objavljen u papirnoj verziji), 4) internet stranicu, 5) datum pristupa stranici.

Primer: Bradley A. Curtis, Gulati Mitu: "Withdrawing from International Custom", *The Yale Law Journal* 2/2010, 233-241, <http://yalelawjournal.org/images/pdfs/912.pdf> (18.11.2012).

GENERAL INFORMATION ON THE JOURNAL AND THE INSTRUCTIONS FOR AUTHORS

I. GENERAL INFORMATION ON THE JOURNAL

1. General. – “Megatrend Review” is the scientific journal published by Megatrend University (Megatrend univerzitet).

According to the classification of CEON the journal is highly ranked amongst the leading national scientific journals in Serbia (M51) and by the Ministry of Education, Science and Technological Development of the Republic of Serbia (M52).

“Megatrend Review” journal has been published since 2004 in Serbian and English language. It is open to all high-quality papers and authors from around the world. It has an international Editorial Board and international Publishing Council. Through international exchange it reaches readers beyond the borders of Serbia.

“Megatrend Review” journal is a multidisciplinary journal in the fields of social sciences. Papers on following scientific fields are published:

- Economics
- Law
- Politics and Security
- Management and Marketing
- International Relations
- Public Policies
- Information Society
- Communications and culture
- Art and design
- Traffic engineering

2. Reviews. – Each paper is reviewed by two reviewers. Paper that has received two positive reviews will be published according to standard categorization of the scientific journals: original scientific paper, review scientific article, expert article, preliminary report or overview, translation and book review.

The categorization of the paper is determined by the reviewers and Editor in chief. If there is any doubt regarding the categorisation, the given higher category will be applied.

In case that one of the reviewers suggests that the paper should be published and the other that it should not, the paper is going to be given to the third reviewer whose decision is final.

3. Anonymity of the authors and reviewers. – Editorial of the “Megatrend review” journal abides by the rule on mutual anonymity between authors and reviewers. Further, if the author is not satisfied with the reviews of the paper, he / she, has the right to receive the reviews.

II. PAPER ORIGINALITY AND FIGHTING AGAINST PLAGIARISM

We kindly ask the authors to take into consideration the following:

1. Written confirmation that the work is original. - When submitting a manuscript the author is required to confirm in writing that his/her paper is original and that it has not been published elsewhere. The paper that is sent without this written confirmation by the author, will not be accepted.

2. The paper that has previously been published elsewhere. - If for any reason the author submits the paper that has already been published elsewhere (abroad, in a foreign language), he/she is obliged to specify where the paper was published (the journal, issue and number, the number of pages) and enclose the written consent of the editorial board of the journal in which the paper was originally published. If these requirements are met, and editors conclude that the paper is for some reason of particular interest and should therefore be published, it will be published with indication where it was published first and that it is republished in "Megatrend Review" with permission.

However, if the paper has already been published elsewhere, and also submitted for publication in "Megatrend Review" with no information about previous publication, the paper will not be published. In addition, as a sanction for unfairness, in the next issue of "Megatrend Review" the information that a particular author has unfairly tried to re-publish the same paper will be published in a special section. Apart from that, the papers by the same author will not be published in "Megatrend Review" in the future.

3. Plagiarism. - Should the editors of "Megatrend Review" journal or through reviewers discover that the paper submitted for publication is plagiarism, in a special section of its next issue the information that a particular author has plagiarized a paper will be published, and the original paper from which the plagiarism is taken will be cited. In addition, the papers by the same author will not be published in "Megatrend Review" in the future. If necessary, the author whose paper has been copied or the editorial board of the journal that has published the original paper will be notified.

III. INSTRUCTIONS FOR AUTHORS

The papers are to be prepared in accordance with the following instructions:

1. The Manuscript

The manuscript is submitted in electronic form (MS Word). Page size: A4, font Times New Roman (size 12 pt for text including abstract, line spacing: single. The papers written in Serbian language are submitted in Serbian Latin script. The papers are submitted to the following e-mail address: **megatrendrevija@megatrend.edu.rs**

A written statement by the author stating that the work is an original work (signed and scanned statement), ORCID number and year of birth for all authors must be submitted with the work.

Precondition for the paper to be accepted for the reviewing procedure is that it fully satisfies technical criteria according to the instructions given here. Also, the paper must meet the criteria regarding the language (Serbian and English) and spelling. The paper has to be proofread before submission

2. Number of authors

As a rule, papers written only by one author are preferable for publication (an author as an individual). However, if consider justified, according to current Rules of Procedure, the Method of Evaluation and Quantitative Expression of Scientific Research Results of the Researchers (*Pravilnik o postupku, načinu vrednovanja i kvantitativnom iskazivanju naučnoistraživačkih rezultata istraživača*, Službeni glasnik RS no. 24/2016 and 21/2017), editors can decide to publish papers written by co-authors, but not more than three.

3. Language

The text is submitted in Serbian or English language. If accepted, it will be published in the language in which it was submitted.

Exceptionally, the editors will decide that the text submitted in Serbian language is to be translated and published in English, or vice versa.

4. Volume

The paper should approximately have 30.000 characters, including spaces (one author's sheet). Alternatively, it could be shorter or longer, the number of characters with spaces not being smaller than 20,000 nor bigger than 45,000.

Due to particularly justified reasons (the special social importance of the topic, the co-authorship of a number of internationally recognized scientists, etc.) the editorial board could exceptionally allow the publication of an article of a larger volume, but not larger than 2.5 author's sheets (75,000 characters).

5. Tables and Formulae

The tables should only be made by means of table tools in MS Word. The tables must have titles and be numbered in Arabic numerals.

The formulae should be written by means of the equation editor in MS Word.

6. Graphs, Figures and Photographs

Graphs and figures can be submitted drawn on paper or in electronic form. When the graphs and figures are submitted in electronic form, they should be in one of the following formats: EPS, AI, EPS, TIF or JPG. If the author uses these or uses a specific program, it is necessary to agree on the format with the technical editor. **Graphs and figures should not be made in MS Word!**

Photographs must be sharp, in good contrast and undamaged. The authors are not advised to scan the images themselves, but to leave this sensitive job to the editorial office.

If the version on the paper does not include graphs, figures and photographs, the spaces must be clearly marked where they should be inserted. The markings in the text must match the ones in the submitted photos (or files).

Graphs, figures and photographs must have the signatures and be numbered in Arabic numerals.

7. Organization of manuscript

The article must contain the following elements, in the following order:

1 Information about the author – Name and surname, title of the author, name of the institution where the author is employed (affiliation) and the author's e-mail address.

2. Title of the paper. – The title should be clear and precise.

3. Abstract. – This is a brief presentation of the article content, which contains the research goal, methods, results, and main conclusions. It should be in the same language in which the paper was written. In terms of volume, it should contain 100 to 250 words or 4 to 8 sentences, or a third to half of the printed page. It stands between the title and keywords, after which the text of the article follows.

4. Key words. – The terms or phrases which best describe the content of the article. It is allowed to write up to five words, i.e. phrases.

5. Text of the article. – The central part is the text of the article in which the author uses appropriate tools while processing the writing of a scientific paper.

6. List of used literature. – After the text of the article, the list of used literature is specified in alphabetical order by authors' last name.

The list is given according to the Citation instructions, with the year of publication coming right after the author's, i.e. editor's name. At the end of the information on an article or a paper in the collection of papers, the pages of the cited paper are given.

Examples:

- A book: Akehurst Michael (1984): *A Modern Introduction to International Law*, London

- A chapter in the book by several authors: Buchanan Allen (2010): "The Legitimacy of International Law", 79-96, in: Besson Samantha, Tasioulas John (eds.): *The Philosophy of International Law*, Oxford

- A paper: Osakwe Chris (1971): "Contemporary Soviet Doctrine on the Juridical Nature of Universal International Organizations", *American Journal of International Law* 3/1971, 502-521

The papers by the same author are specified in chronological order. If several papers have been written by the same author and published in the same year, the year of publication is accompanied by the letters "a", "b", "c" etc.

Examples:

- Cassese Antonio (1999a): "Ex iniuria ius oritur. Are We Mowing towards International Legitimation of Forcible Humanitarian Countermeasures in the World Community?", *European Journal of International Law*, 1/1999, 23-30

- Cassese Antonio (1999b): "A Follow-Up: Forcible Humanitarian Countermeasures and *Opinio Necessitatis*", *European Journal of International Law*, 4/1999, 791-799

7. Summary. – Summary is written at the very end of the text i.e. It can be the same as the abstract, but could also be wider in extent, yet no longer than one page. If the paper is written in Serbian language, the summary in English language should also be submitted.

8. The levels of the titles. - Depending on the text, the titles can have different levels. Therefore the following method is used for marking different title levels:

1. The First Level Title

(centre align, regular, bold, Arabic numerals)

1.1 The second level title

(centre align, italic, Arabic numerals)

1.1.1. The third level title

(Above the beginning of the paragraph, italic, Arabic numerals.)

To achieve complete clarity about the title levels, authors are advised to refer to the past issues of "Megatrend Review" journal available in PDF forms, under Archive, or contact the Editorial secretary via e-mail.

Depending on the specific characteristics of the text, and with the aim of achieving clarity of the paper's structure, the editorial office reserves the right to edit the titles in a slightly different way, leaving the original heading divisions.

9. Citations. – The used literature is to be cited according to the instructions for citations given below.

10. The address of the Editorial Board. – The papers are submitted via e-mail to the following address: **megatrendrevija@megatrend.edu.rs**

Editorial Board
Megatrend Review
Megatrend University / Megatrend univerzitet
Bulevar Mihajla Pupina 117
11070 Belgrade, Serbia

IV. INSTRUCTIONS FOR CITATIONS

1. General rules

1. Name of the author. - In writing author's name, surname is written before the first name. If there is the middle name/letter, it is written between surname and the first name.

Example: Shaw N. Malcolm

2. Several authors. – Names of the several authors are separated by commas.

Example: Simma Bruno, Alston Philip

If there are more than three authors, only the first author's surname and first name are specified, followed by the italicized et al. words (et alia).

Example: Henkin Louis *et. al.* (1993): *International Law: Cases and Materials*, St. Paul. Minn.

3. Pages. – When a particular page is specified (of the book or the paper), its number is written without any additions (p., pg., p., page, etc.).

Example: Akehurst Michael (1984): *A Modern Introduction to International Law*, London, 9.

4. Footnotes. – When a footnote is given, after the number of the page, the sign "fn" is written, followed by the number of the footnote.

Example: Akehurst Michael (1984): *A Modern Introduction to International Law*, London, 9, fn 2.

5. The repeated citation of the same article. – When an article that has been cited before is recited, the author's surname and first name are specified, followed by the cited page, separated by a comma, without using *op. cit.* etc.

Example: Akehurst Michael, 15.

If several papers by the same author are specified, the author's surname and first name are stated, followed by the brackets with the year when the paper has been published and followed by the number of the page.

Example: Akehurst Michael (1984), 15.

When specifying several papers written by the same author, published in the same year, papers are specified in the literature list (which is always given at the end of the paper) by adding Latin letters “a”, “b”, “c”, etc to each paper. They are also stated as such when cited in footnotes.

Example: Akehurst Michael (1984a), 15.

6. Recitation of the previously cited article. - If a piece of data from the same page of the same paper cited in the previous footnote is cited again, only the Latin abbreviation *Ibid.* (from *ibidem*) is used without giving any other data.

Example: Ibid.

If a piece of data cited in the previous footnote is cited again, but from a different page, the Latin abbreviation *Ibid.* is used, followed by a comma and the number of the page.

Example: Ibid, 54.

7. Foreign names. – In papers submitted in Serbian language, foreign names are transcribed, i.e. written as they are pronounced in Serbian, and when first mentioned in the text, the author’s surname and first name are given in their original form within the brackets.

Example: Tomas Hobs (Thomas Hobbes)

2. Books

1. General. – The books are cited in the following way:

1) author’s surname, 2) author’s first name, 3) the year of publication in brackets, 4) colon, 5) title of the book in italics, 6) place of the publication in lowercase (ordinary letters), 7) number of the page (without any additions), 8) footnote which is being cited.

If the information on the publisher is given as well, it is written in lowercase (ordinary letters) before the place of the publication.

Example: Scott V. Shirley (2010): *International Law in World Politics*, Lynne Rienner Publishers Inc., Boulder – London, 71, fn 45.

2. Several editions. – If a book has several editions the number of the edition need/need not be specified in the superscript.

Example: Scott V. Shirley (2010²): *International Law in World Politics*, Lynne Rienner Publishers Inc., Boulder - London (explanation: 2010² - second edition, published 2010)

3. Editors. – If a book has one or more editors, the editors’ surnames and first names are given first, separated by commas, then the sign “ed”, or “eds” is written if there are more of them, followed by the title of the book in italics, and finally the place and year of publication.

Example: Besson Samantha, Tasioulas John (eds.) (2010): *The Philosophy of International Law*, Oxford.

If there are more than three editors, the data only for the first editor is given followed by a comma, then “et al.”, and finally “ed.”.

Example: Hamilton P. et al. (eds.) (1999): *The Permanent Court of Arbitration: International Arbitration and Dispute Resolution*, Kluwer International, The Hague-London-Boston.

4. Chapters in a book. – A chapter in a book with an editor is cited by giving the following: 1) authors surname and name, 2) year of publication in brackets, 3) colon, 4) title of the chapter in lowercase (under inverted commas), 5) comma 6) number of pages that are cited, 7) “in”, 8) editor’s surname and name, 9) “(eds.)”, 10) title of the book in which the cited text is in lowercase (in italics) and 11) place of publication.

Example: Buchanan Allen (2010): “The Legitimacy of International Law”, 79-96, in: Besson Samantha, Tasioulas John (eds.): *The Philosophy of International Law*, Oxford.

3. Articles

1. General. – The articles are cited in the following way: 1) author’s surname, 2) author’s name, 3) year of publication in brackets, 4) colon, 5) title of the article in lowercase in ordinary letters under inverted commas, 6) title of the journal (book of proceedings, etc.) in italics, 7) issue and year separated by a slash, 8) number of the page (without any additions), 9) number of the cited footnote.

Example: Osakwe Chris (1971): “Contemporary Soviet Doctrine on the Juridical Nature of Universal International Organizations”, *American Journal of International Law* 3/1971, 502, fn 1.

2. The abbreviation of the journal title. – If the title of the journal (collection of papers etc.) is a long one, when cited for the first time its abbreviation is given in brackets, which is later used when the same journal (book of proceedings, etc.) is cited again.

Example: Osakwe Chris (1971): “Contemporary Soviet Doctrine on the Juridical Nature of Universal International Organizations”, *American Journal of International Law* (AJIL) 3/1971, 502-521.

4. Regulations

1. General. – Regulations are cited in the following way: 1) title of the regulation is given in lowercase (in general letters), 2) journal/magazine in which the regulation is published is given in italics, 3) number of the issue and the year in which the journal is published are given at the end.

Example: Zakon o osnovama uređenja službi bezbednosti Republike Srbije, *Službeni glasnik Republike Srbije*, 116/2007.

2. If the regulations are re-mentioned. – If a regulation is mentioned again later in the text, at the place where it appears for the first time its short title is given within the brackets, with the words “hereinafter referred to as” preceding it.

Example: Zakon o osnovama uređenja službi bezbednosti Republike Srbije (u daljem tekstu: Zakon o službama bezbednosti), *Službeni glasnik Republike Srbije*, 116/2007.

3. Amendments. – If a regulation has been changed and amended, one by one, the numbers of issues and year of the journals are given in the original text, i.e. amendments were published.

Example: Zakon o osnovama uređenja službi bezbednosti Republike Srbije, *Službeni glasnik Republike Srbije*, 116/2007, 72/2012.

4. Articles, paragraphs and items of regulations. – Articles, paragraphs and items of regulations are written separated by a slash, the number of the article comes first, followed by the number of the paragraph, and finally that of the item, etc.

Example: UN Convention on the Law of the Sea (1982) čl. 1/1/5/a/i.

5. The Internet texts

The citation of the text from the Internet should contain: 1) name of the author of the cited text (if it is the author's text), 2) title of the cited text under inverted commas, 3) data on where the text was published (if it is published in a printed version), 4) internet page, 5) date of the access to the page.

Example: Bradley A. Curtis, Gulati Mitu: “Withdrawing from International Custom”, *The Yale Law Journal* 2/2010, 233-241, <http://yalelawjournal.org/images/pdfs/912.pdf> (18.11.2012).



UNIVERZITET
MEGATREND
JOHN NAISBITT UNIVERSITY

www.megatrend.edu.rs