

CYBER SIGURNOST I POVJERENJE U DIGITALNOM POSLOVANJU- PREDUSLOV EVROPSKIH INTEGRACIJA / CYBER SECURITY AND TRUST IN DIGITAL BUSINESS - A PREREQUISITE FOR EUROPEAN INTEGRATION

doc. dr. Nehad Gaši¹

¹Internacionalni Univerzitet Travnik, Aleja Konzula – Meljanac bb, 72270 Travnik, BiH

e-mail: nehad.gasi@iu-travnik.com

Pregledni članak

<https://www.doi.org/10.58952/zr20251403360>

UDK / UDC 004.056.5:658.8:323.1

Sažetak

Digitalna transformacija poslovanja u zemljama Zapadnog Balkana otvara značajne mogućnosti za ekonomski rast i jačanje regionalne konkurentnosti, ali istovremeno donosi i nove rizike vezane za cyber sigurnost. Sigurnosni izazovi, uključujući zaštitu podataka, prevenciju kibernetičkih napada i regulaciju digitalnih transakcija, postaju ključni preduslov za izgradnju povjerenja među poslovnim subjektima, građanima i institucijama. Uspostavljanje visokih standarda zaštite i pravne regulative u skladu s europskim direktivama predstavlja temeljni korak u procesu evropskih integracija. Poseban značaj imaju usklađivanje sa Općom uredbom o zaštiti podataka (GDPR) i implementacija politika koje osiguravaju transparentnost i odgovornost u digitalnom poslovanju. Samo integrisan pristup, koji povezuje tehnološke inovacije, pravni okvir i podizanje svijesti o važnosti cyber sigurnosti, može omogućiti stabilan razvoj digitalne ekonomije i jačanje povjerenja na tržištu. Time cyber sigurnost postaje ne samo tehnički, već i društveno-pravni imperativ, a povjerenje glavni faktor održivog razvoja i evropske perspektive Zapadnog Balkana.

Ključne riječi: cyber sigurnost, digitalno poslovanje, povjerenje, evropske integracije, zaštita podataka, GDPR, pravna regulative

JEL klasifikacija: L86, K24, F36, O33

Abstract

The digital transformation of business in the Western Balkan countries opens up significant opportunities for economic growth and strengthening regional competitiveness, but at the same time brings new risks related to cybersecurity. Security challenges, including data protection, prevention of cyber attacks and regulation of digital transactions, are becoming a key prerequisite for building trust among business entities, citizens and institutions. Establishing high standards of protection and legal regulation in accordance with European directives is a fundamental step in the process of European integration. Of particular importance are the harmonization with the General Data Protection Regulation (GDPR) and the implementation of policies that ensure transparency and accountability in digital business. Only an integrated approach, which connects technological innovations, the legal framework and raising awareness of the importance of cybersecurity, can enable the stable development of the digital economy and strengthen trust in the market. This makes cybersecurity not only a technical but also a socio-legal imperative, and trust a key factor in the sustainable development and European perspective of the Western Balkans.

Keywords: cybersecurity, digital business, trust, European integration, data protection, GDPR, legal regulation

JEL klasifikacija: L86, K24, F36, O33

UVOD

Razvoj digitalnih tehnologija u posljednjim decenijama značajno je promijenio način na koji se odvija poslovanje, komunikacija i razmjena vrijednosti. Elektronsko poslovanje, digitalne finansijske usluge, platforme za elektronsku trgovinu i digitalna javna uprava postali su sastavni dio svakodnevnog života. Međutim, paralelno sa rastom digitalnih usluga raste i izloženost različitim oblicima cyber prijetnji, uključujući krađu podataka, finansijske prevare, industrijsku špijunažu i napade na kritičnu infrastrukturu, što je potvrđeno u strateškim dokumentima Evropske unije²¹⁵. U takvom okruženju, povjerenje korisnika u digitalne sisteme postaje odlučujući faktor njihove šire prihvaćenosti i dugoročne održivosti. Za Evropsku uniju, digitalno povjerenje nije samo ekonomsko, već i političko i pravno pitanje. Funkcionisanje jedinstvenog digitalnog tržišta podrazumijeva visok stepen sigurnosti informacionih sistema, zaštitu ličnih i poslovnih podataka, te pouzdane mehanizme odgovornosti i nadzora²¹⁶. Države koje se nalaze u procesu evropskih integracija moraju pokazati sposobnost da obezbijede stabilan i siguran digitalni ambijent, usklađen sa evropskim normama i standardima, kako bi mogle ravnopravno učestvovati u zajedničkom tržištu.

1. CYBER SIGURNOST KAO TEMELJ DIGITALNOG POSLOVANJA

Digitalno poslovanje predstavlja okosnicu savremenih organizacija, omogućavajući bržu komunikaciju, efikasnije procese i pristup globalnom tržištu. Međutim, sa rastućom digitalizacijom poslovnih aktivnosti raste i izloženost organizacija različitim cyber prijetnjama. U tom kontekstu, cyber sigurnost postaje ključni faktor stabilnosti, povjerenja i održivosti digitalnog poslovanja. Cyber sigurnost obuhvata skup tehničkih, organizacionih i pravnih mjera koje imaju za cilj zaštitu informacionih sistema, mreža, aplikacija i podataka od neovlaštenog pristupa, zloupotrebe, gubitka ili uništenja²¹⁷. Bez adekvatne cyber sigurnosti, digitalno poslovanje postaje izuzetno ranjivo, što može dovesti do finansijskih gubitaka, narušavanja reputacije i pravnih posljedica.

1.1 ULOGA CYBER SIGURNOSTI U DIGITALNOM POSLOVANJU

Jedan od osnovnih ciljeva cyber sigurnosti u digitalnom poslovanju jeste očuvanje povjerljivosti, integriteta i dostupnosti podataka (CIA model). Povjerljivost osigurava da osjetljivi poslovni i lični podaci budu dostupni isključivo ovlaštenim korisnicima. Integritet podataka garantuje da informacije nisu neovlašteno izmijenjene, dok dostupnost omogućava kontinuiran pristup sistemima i podacima u svakom trenutku²¹⁸. U digitalnom poslovanju, gdje se transakcije, ugovori i komunikacija odvijaju putem interneta, sigurnost informacionih sistema direktno utiče na povjerenje korisnika i poslovnih partnera. Kupci su sve svjesniji rizika vezanih za zaštitu ličnih podataka, te organizacije koje ne ulažu u cyber sigurnost gube konkurentsku prednost²¹⁹.

1.2 CYBER PRIJETNJE I IZAZOVI DIGITALNOG POSLOVANJA

Savremeno digitalno okruženje karakteriše veliki broj sofisticiranih cyber napada, uključujući phishing napade, ransomware, malware, DDoS napade i krađu identiteta. Ovi napadi često imaju za cilj krađu osjetljivih poslovnih informacija, finansijskih sredstava ili prekid poslovnih procesa²²⁰.

²¹⁵ European Commission, The EU Cybersecurity Strategy for the Digital Decade, Brussels, 2020.

²¹⁶ European Commission, Shaping Europe's Digital Future, Brussels, 2020.

²¹⁷ Stallings, W. *Network Security Essentials: Applications and Standards*. Pearson Education, 2017.

²¹⁸ Whitman, M. E., Mattord, H. J. *Principles of Information Security*. Cengage Learning, 2019.

²¹⁹ OECD. *Digital Security Risk Management for Economic and Social Prosperity*, 2015.

²²⁰ Kaspersky Lab. *Cybersecurity Essentials*, 2020.

Poseban izazov predstavlja činjenica da se digitalno poslovanje sve više oslanja na cloud servise, mobilne tehnologije i Internet stvari (IoT), čime se dodatno proširuje površina napada. Nedovoljno zaštićeni sistemi mogu postati laka meta cyber kriminalaca, što zahtijeva kontinuirano unapređenje sigurnosnih mjera i strategija²²¹.

1.3. CYBER SIGURNOST KAO STRATEŠKA KOMPONENTA POSLOVANJA

Cyber sigurnost više se ne posmatra isključivo kao tehničko pitanje, već kao strateška komponenta upravljanja organizacijom. Menadžment mora aktivno učestvovati u definisanju sigurnosnih politika, procjeni rizika i donošenju odluka vezanih za ulaganja u sigurnosnu infrastrukturu²²². Implementacija međunarodnih standarda, poput ISO/IEC 27001, doprinosi sistematskom upravljanju informacijskom sigurnošću i jačanju povjerenja korisnika. Također, edukacija zaposlenih o cyber prijetnjama i sigurnosnim procedurama predstavlja jedan od ključnih elemenata uspješne cyber sigurnosne strategije²²³.

1.4 PRAVNA I REGULATORNA DIMENZIJA CYBER SIGURNOSTI

U kontekstu digitalnog poslovanja, cyber sigurnost ima i značajnu pravnu dimenziju. Propisi poput Opće uredbe o zaštiti podataka (GDPR) nameću organizacijama obavezu adekvatne zaštite ličnih podataka i prijavljivanja sigurnosnih incidenata. Neusklađenost sa regulatornim zahtjevima može rezultirati visokim novčanim kaznama i gubitkom reputacije²²⁴. Stoga je usklađivanje tehničkih sigurnosnih mjera sa važećim zakonodavstvom neophodno za zakonito i održivo digitalno poslovanje.

2. POVJERENJE U DIGITALNOM POSLOVANJU

Povjerenje u digitalnom poslovanju podrazumijeva uvjerenje korisnika da su digitalne transakcije sigurne, da se njihovi podaci obrađuju zakonito i da postoje efikasni pravni mehanizmi zaštite u slučaju zloupotrebe. Istraživanja pokazuju da je povjerenje jedan od ključnih faktora koji utiču na prihvatanje digitalnih usluga i razvoj elektronske trgovine²²⁵. Bez povjerenja, digitalne tehnologije ne mogu ostvariti svoj puni potencijal, jer korisnici izbjegavaju korištenje online usluga ili ih koriste sa rezervom. U tom smislu, povjerenje nije isključivo tehničko pitanje, već i pravno i institucionalno. Transparentni propisi, jasno definisana prava i obaveze, kao i efikasne institucije nadzora, ključni su za izgradnju stabilnog digitalnog okruženja. Evropska unija je kroz regulatorne mehanizme nastojala da uspostavi jedinstvena pravila koja jačaju povjerenje građana i poslovnih subjekata u digitalno tržište²²⁶.

²²¹ Roman, R., Zhou, J., Lopez, J. "On the Features and Challenges of Security and Privacy in Distributed Internet of Things." *Computer Networks*, 2013.

²²² Von Solms, R., Von Solms, S. "Cybersecurity and Information Security – What Goes Where?" *Information & Computer Security*, 2018.

²²³ ISO/IEC 27001:2013 – Information Security Management Systems.

²²⁴ European Union. *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679

²²⁵ World Economic Forum, *Global Risks Report*, Geneva, 2023.

²²⁶ European Central Bank, *Cyber Resilience Oversight Expectations*, Frankfurt, 2021.

3. EVROPSKI REGULATORNI OKVIR

Evropska unija je razvila sveobuhvatan pravni okvir kojim se uređuje oblast cyber sigurnosti i digitalnog povjerenja. Direktiva o sigurnosti mrežnih i informacionih sistema (NIS Direktiva), kao i njen unaprijeđeni oblik poznat kao NIS2, postavljaju obaveze državama članicama i ključnim subjektima u pogledu upravljanja rizicima i prijavljivanja sigurnosnih incidenata²²⁷. Paralelno s tim, Opća uredba o zaštiti podataka (GDPR) uspostavlja stroga pravila o obradi i zaštiti ličnih podataka, čime se dodatno jača povjerenje korisnika u digitalne usluge²²⁸. Za države koje teže članstvu u Evropskoj uniji, usklađivanje sa ovim propisima predstavlja jedan od ključnih izazova. Proces harmonizacije zakonodavstva zahtijeva ne samo formalno preuzimanje evropskih normi, već i izgradnju institucionalnih kapaciteta, edukaciju kadrova i razvoj tehničke infrastrukture, što je jasno naglašeno u izvještajima Evropske komisije²²⁹.

4. CYBER SIGURNOST I EVROPSKE INTEGRACIJE

Proces evropskih integracija podrazumijeva političko, pravno, ekonomsko i institucionalno usklađivanje država kandidata sa standardima i politikama Evropske unije. U savremenom digitalnom okruženju, cyber sigurnost postaje jedno od ključnih područja tog usklađivanja, jer stabilni i sigurni informacioni sistemi predstavljaju osnovu funkcionisanja jedinstvenog evropskog tržišta, javne uprave i zaštite osnovnih prava građana. Evropska unija prepoznaje cyber sigurnost kao strateško pitanje od zajedničkog interesa, posebno u kontekstu digitalne transformacije, prekogranične razmjene podataka i rastuće zavisnosti od informaciono-komunikacionih tehnologija. Zbog toga je cyber sigurnost postala sastavni dio pregovaračkih poglavlja i reformskih procesa u okviru evropskih integracija²³⁰.

4.1. CYBER SIGURNOST KAO DIO EVROPSKOG DIGITALNOG PROSTORA

Jedan od osnovnih ciljeva Evropske unije jeste izgradnja Jedinstvenog digitalnog tržišta (Digital Single Market), koje omogućava slobodan protok robe, usluga, kapitala i podataka. Ovakav prostor ne može funkcionisati bez visokog nivoa povjerenja u sigurnost digitalnih sistema i mreža²³¹. Cyber sigurnost u ovom kontekstu ima dvostruku ulogu: s jedne strane, omogućava nesmetano funkcionisanje digitalne ekonomije, a s druge strane štiti građane i institucije od cyber prijetnji koje ne poznaju državne granice. Upravo zbog prekogranične prirode cyber napada, EU insistira na zajedničkim pravilima, standardima i mehanizmima saradnje među državama članicama i državama kandidatima²³².

4.2. EVROPSKI PRAVNI OKVIR CYBER SIGURNOSTI

Evropska unija je razvila sveobuhvatan pravni i institucionalni okvir za cyber sigurnost. Među najznačajnijim pravnim aktima ističe se Direktiva o sigurnosti mrežnih i informacionih sistema (NIS Direktiva), koja obavezuje države članice da uspostave nacionalne strategije cyber sigurnosti, nadležna tijela i mehanizme za upravljanje cyber incidentima²³³.

²²⁷ Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2).

²²⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).

²²⁹ European Commission, *Enlargement Package – Annual Reports*, Brussels, 2022.

²³⁰ European Commission. *EU Cybersecurity Strategy for the Digital Decade*, 2020.

²³¹ European Commission. *Shaping Europe's Digital Future*, 2020.

²³² Carrapico, H., Barrinha, A. "The EU as a Coherent Cybersecurity Actor." *Journal of Common Market Studies*, 2017.

²³³ Directive (EU) 2016/1148 – NIS Directive.

Pored NIS Direktive, važnu ulogu ima i Opća uredba o zaštiti podataka (GDPR), koja postavlja visoke standarde zaštite ličnih podataka i direktno utiče na sigurnosne prakse organizacija u digitalnom okruženju²³⁴. U procesu evropskih integracija, države kandidati su obavezne da svoje zakonodavstvo usklade sa ovim propisima, čime cyber sigurnost postaje i pravno, a ne samo tehničko pitanje.

4.3. INSTITUCIONALNA SARADNJA I ULOGA EU AGENCIJA

Evropske integracije u oblasti cyber sigurnosti podrazumijevaju i jačanje institucionalne saradnje. Ključnu ulogu ima **Agencija Evropske unije za cyber sigurnost (ENISA)**, koja pruža stručnu podršku državama članicama, razvija smjernice i promoviše najbolje prakse u oblasti cyber sigurnosti²³⁵. Države koje teže članstvu u EU ohrabruju se da aktivno sarađuju sa ENISA-om, učestvuju u zajedničkim vježbama i razmjeni informacija o cyber prijetnjama. Ovakva saradnja doprinosi jačanju nacionalnih kapaciteta i bržem prilagođavanju evropskim standardima cyber sigurnosti²³⁶.

4.4. CYBER SIGURNOST KAO USLOV EVROPSKIH INTEGRACIJA DRŽAVA ZAPADNOG BALKANA

Za države Zapadnog Balkana, uključujući Bosnu i Hercegovinu, cyber sigurnost predstavlja sve važniji segment procesa evropskih integracija. Evropska komisija u svojim izvještajima o napretku redovno ukazuje na potrebu jačanja institucionalnih kapaciteta, donošenja strateških dokumenata i unapređenja zakonodavnog okvira u oblasti cyber sigurnosti²³⁷. Nedovoljno razvijeni sistemi cyber sigurnosti mogu predstavljati prepreku evropskim integracijama, jer ugrožavaju stabilnost digitalne infrastrukture i povjerenje u institucije. S druge strane, usklađivanje sa evropskim standardima doprinosi modernizaciji javne uprave, jačanju digitalne ekonomije i sigurnijem učešću na jedinstvenom evropskom tržištu.

4.5. STRATEŠKI ZNAČAJ CYBER SIGURNOSTI U KONTEKSTU EU INTEGRACIJA

Cyber sigurnost u okviru evropskih integracija ima i širi strateški značaj, posebno u kontekstu hibridnih prijetnji, dezinformacija i zaštite kritične infrastrukture. Evropska unija sve više povezuje cyber sigurnost sa pitanjima nacionalne i kolektivne sigurnosti, naglašavajući potrebu koordinisanog odgovora na cyber incidente²³⁸. U tom smislu, države koje teže članstvu u EU moraju razvijati dugoročne strategije cyber sigurnosti, koje uključuju saradnju javnog i privatnog sektora, edukaciju kadrova i kontinuirano ulaganje u sigurnosne tehnologije.

5. KOMPARATIVNA ANALIZA CYBER SIGURNOSTI: EVROPSKA UNIJA I ZAPADNI BALKAN

Razlike u stepenu razvoja cyber sigurnosti između Evropske unije i država Zapadnog Balkana rezultat su različitog nivoa institucionalne zrelosti, regulatornog okvira, tehničkih kapaciteta i ulaganja u digitalnu infrastrukturu.

²³⁴ Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR).

²³⁵ ENISA. *About ENISA and EU Cybersecurity*, 2021.

²³⁶ Klimburg, A. *The Darkening Web: The War for Cyberspace*. Penguin Press, 2017.

²³⁷ European Commission. *Bosnia and Herzegovina 2023 Report*, Enlargement Package.

²³⁸ Council of the European Union. *Cybersecurity: strengthening Europe's resilience*, 2021.

Komparativna analiza ukazuje na ključne izazove sa kojima se suočavaju države Zapadnog Balkana u procesu usklađivanja sa evropskim standardima cyber sigurnosti, ali i na mogućnosti za unapređenje u okviru procesa evropskih integracija.

5.1. REGULATORNI I STRATEŠKI OKVIR

Evropska unija posjeduje razvijen i harmonizovan regulatorni okvir u oblasti cyber sigurnosti, koji se zasniva na NIS Direktivi, GDPR-u, kao i novijim inicijativama poput NIS2 Direktive i EU Cybersecurity Acta. Ovi akti obavezuju države članice na uspostavljanje nacionalnih strategija cyber sigurnosti, funkcionalnih CERT/CSIRT timova i jasnih mehanizama koordinacije između institucija²³⁹. Nasuprot tome, u državama Zapadnog Balkana regulatorni okvir je često fragmentiran i neujednačen. Iako većina zemalja ima usvojene strategije cyber sigurnosti, njihova implementacija je ograničena nedostatkom institucionalnih kapaciteta i finansijskih resursa. U pojedinim slučajevima, zakoni nisu u potpunosti usklađeni sa evropskim direktivama, što usporava proces evropskih integracija²⁴⁰.

5.2. INSTITUCIONALNI KAPACITETI I UPRAVLJANJE CYBER SIGURNOŠĆU

Države članice EU imaju razvijene institucionalne mehanizme za upravljanje cyber sigurnošću, uključujući specijalizovana nacionalna tijela, koordinaciju sa ENISA-om i redovno učešće u zajedničkim cyber vježbama. Ovakav pristup omogućava brzu razmjenu informacija i koordinisan odgovor na cyber incidente²⁴¹. U državama Zapadnog Balkana institucionalni kapaciteti su značajno slabiji. Nacionalni CERT timovi često nemaju dovoljan broj stručnjaka, a saradnja između javnog i privatnog sektora je nedovoljno razvijena. Dodatni problem predstavlja složena administrativna struktura, posebno u državama sa decentralizovanim sistemom vlasti, što otežava efikasno upravljanje cyber sigurnošću²⁴².

5.3. TEHNIČKA INFRASTRUKTURA I NIVO DIGITALNE OTPORNOSTI

Evropska unija kontinuirano ulaže u jačanje digitalne otpornosti kroz razvoj sigurnih mreža, zaštitu kritične infrastrukture i primjenu naprednih sigurnosnih tehnologija. Poseban fokus stavljen je na zaštitu sektora energetike, saobraćaja, finansija i zdravstva, koji se smatraju ključnim za stabilnost društva²⁴³. Za razliku od EU, države Zapadnog Balkana često se suočavaju sa zastarjelom IT infrastrukturom i nedovoljnim ulaganjima u cyber sigurnost. Digitalna otpornost sistema je ograničena, što povećava rizik od uspješnih cyber napada i ugrožavanja kritičnih servisa. Ovakvo stanje dodatno naglašava potrebu za finansijskom i tehničkom podrškom EU kroz pretpristupne fondove i regionalne projekte²⁴⁴.

²³⁹ European Union Agency for Cybersecurity (ENISA). *EU Cybersecurity Act*, 2019.

²⁴⁰ European Commission. *Western Balkans Digital Agenda*, 2020.

²⁴¹ NIS Cooperation Group. *EU Coordinated Response to Cyber Incidents*, 2021.

²⁴² OECD. *Cybersecurity Policy Framework for the Western Balkans*, 2022.

²⁴³ European Commission. *Critical Infrastructure Protection in the EU*, 2021.

²⁴⁴ World Bank. *Cybersecurity and Digital Resilience in the Western Balkans*, 2020.

5.4. LJUDSKI RESURSI I EDUKACIJA

Evropska unija prepoznaje značaj ljudskog faktora u cyber sigurnosti i aktivno ulaže u edukaciju, istraživanje i razvoj digitalnih vještina. Programi poput *Digital Europe* i *Horizon Europe* omogućavaju kontinuirano usavršavanje stručnjaka i razvoj inovativnih sigurnosnih rješenja²⁴⁵. U državama Zapadnog Balkana postoji izražen nedostatak kvalifikovanih stručnjaka za cyber sigurnost. Obrazovni sistemi često ne prate potrebe tržišta rada, dok odlazak stručnog kadra u države EU dodatno produbljuje problem. Ipak, proces evropskih integracija otvara prostor za jačanje obrazovnih programa i regionalne saradnje u ovoj oblasti²⁴⁶.

5.5. USKLAĐENOST SA EU STANDARDIMA KAO RAZVOJNA PRILIKA

Iako zaostajanje Zapadnog Balkana u oblasti cyber sigurnosti predstavlja izazov, ono istovremeno može biti i razvojna prilika. Usklađivanje sa EU standardima ne znači samo ispunjavanje formalnih uslova za članstvo, već i unapređenje digitalne otpornosti, jačanje povjerenja investitora i sigurnije učešće u jedinstvenom evropskom tržištu. Evropska unija kroz mehanizme tehničke pomoći, regionalne inicijative i finansijsku podršku podstiče države Zapadnog Balkana da ubrzaju reforme u oblasti cyber sigurnosti, čime se ova oblast potvrđuje kao jedan od ključnih stubova evropskih integracija²⁴⁷.

²⁴⁵ European Commission. *Digital Europe Programme*, 2021.

²⁴⁶ Regional Cooperation Council (RCC). *Cybersecurity Skills Gap in the Western Balkans*, 2022.

²⁴⁷ European Commission. *EU Enlargement and Cybersecurity Reforms*, 2023.

ZAKLJUČAK

Digitalna transformacija savremenog poslovanja neodvojivo je povezana s pitanjem cyber sigurnosti, koja se u današnjem okruženju nameće kao ključni uslov stabilnosti, povjerenja i dugoročne održivosti digitalne ekonomije. Analiza provedena u ovom radu potvrđuje da cyber sigurnost više ne predstavlja isključivo tehnički izazov, već složen društveno-pravni i institucionalni fenomen koji direktno utiče na razvoj digitalnog poslovanja i integraciju u jedinstveni evropski digitalni prostor. Povjerenje korisnika, poslovnih subjekata i institucija u digitalne sisteme izgrađuje se prvenstveno kroz pouzdanu zaštitu podataka, transparentne regulatorne mehanizme i efikasne institucionalne kapacitete za prevenciju i odgovor na cyber prijetnje. Evropska unija je kroz uspostavljanje sveobuhvatnog regulatornog okvira, uključujući GDPR, NIS i NIS2 direktivu, jasno definisala cyber sigurnost kao jedan od temelja funkcionisanja Jedinstvenog digitalnog tržišta. Time je cyber sigurnost postala sastavni dio evropskih integracijskih procesa, a ne samo pitanje tehničke usklađenosti. Države koje teže članstvu u EU suočavaju se s obavezom ne samo formalnog preuzimanja evropskih normi, već i njihove dosljedne implementacije kroz jačanje institucionalnih kapaciteta, razvoj tehničke infrastrukture i ulaganje u ljudske resurse. U tom kontekstu, cyber sigurnost dobija strateški značaj, jer direktno utiče na konkurentnost ekonomije, zaštitu osnovnih prava građana i stabilnost digitalnih javnih servisa. Komparativna analiza Evropske unije i država Zapadnog Balkana ukazuje na izražen jaz u nivou regulatorne zrelosti, institucionalne koordinacije i digitalne otpornosti. Iako su u zemljama Zapadnog Balkana ostvareni određeni pomaci u donošenju strateških dokumenata i zakonodavnih rješenja, njihova praktična primjena ostaje ograničena nedostatkom finansijskih sredstava, stručnog kadra i efikasne međuinstitucionalne saradnje. Takvo stanje predstavlja prepreku bržem procesu evropskih integracija, ali istovremeno otvara prostor za razvoj kroz usklađivanje sa evropskim standardima i korištenje mehanizama tehničke i finansijske podrške Evropske unije. Na osnovu iznesenih nalaza može se zaključiti da je jačanje cyber sigurnosti u državama Zapadnog Balkana neophodan preduslov izgradnje povjerenja u digitalnom poslovanju i uspješne evropske perspektive regiona. Samo integrisan pristup, koji povezuje tehnološka rješenja, pravni okvir, institucionalnu saradnju i kontinuiranu edukaciju, može osigurati siguran i pouzdan digitalni ambijent. U tom smislu, cyber sigurnost se potvrđuje kao jedan od ključnih stubova savremenog digitalnog razvoja i nezaobilazan element procesa evropskih integracija, dok povjerenje ostaje centralna vrijednost na kojoj se gradi održiva i konkurentna digitalna ekonomija.

LITERATURA

1. European Commission, *The EU Cybersecurity Strategy for the Digital Decade*, Brussels, 2020.
2. European Commission, *Shaping Europe's Digital Future*, Brussels, 2020.
3. OECD, *Digital Security Risk Management for Economic and Social Prosperity*, Paris, 2015.
4. ENISA, *Cybersecurity and Trust in the Digital Economy*, Athens, 2021.
5. World Economic Forum, *Global Risks Report*, Geneva, 2023.
6. European Central Bank, *Cyber Resilience Oversight Expectations*, Frankfurt, 2021.
7. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2).
8. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).
9. European Commission, *Enlargement Package – Annual Reports*, Brussels, 2022.
10. European Union Agency for Cybersecurity (ENISA). *EU Cybersecurity Act*, 2019.
11. European Commission. *Western Balkans Digital Agenda*, 2020.
12. NIS Cooperation Group. *EU Coordinated Response to Cyber Incidents*, 2021.
13. OECD. *Cybersecurity Policy Framework for the Western Balkans*, 2022.
14. European Commission. *Critical Infrastructure Protection in the EU*, 2021.
15. World Bank. *Cybersecurity and Digital Resilience in the Western Balkans*, 2020.
16. European Commission. *Digital Europe Programme*, 2021.
17. Regional Cooperation Council (RCC). *Cybersecurity Skills Gap in the Western Balkans*, 2022.
18. European Commission. *EU Enlargement and Cybersecurity Reforms*, 2023.
19. European Commission. *EU Cybersecurity Strategy for the Digital Decade*, 2020.
20. European Commission. *Shaping Europe's Digital Future*, 2020.
21. Carrapico, H., Barrinha, A. "The EU as a Coherent Cybersecurity Actor." *Journal of Common Market Studies*, 2017.
22. Directive (EU) 2016/1148 – NIS Directive.
23. Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR).
24. ENISA. *About ENISA and EU Cybersecurity*, 2021.
25. Klimburg, A. *The Darkening Web: The War for Cyberspace*. Penguin Press, 2017.
26. European Commission. *Bosnia and Herzegovina 2023 Report*, Enlargement Package.
27. Council of the European Union. *Cybersecurity: strengthening Europe's resilience*, 2021.
28. Stallings, W. *Network Security Essentials: Applications and Standards*. Pearson Education, 2017.
29. Whitman, M. E., Mattord, H. J. *Principles of Information Security*. Cengage Learning, 2019.
30. OECD. *Digital Security Risk Management for Economic and Social Prosperity*, 2015.
31. Kaspersky Lab. *Cybersecurity Essentials*, 2020.
32. Roman, R., Zhou, J., Lopez, J. "On the Features and Challenges of Security and Privacy in Distributed Internet of Things." *Computer Networks*, 2013.
33. Von Solms, R., Von Solms, S. "Cybersecurity and Information Security – What Goes Where?" *Information & Computer Security*, 2018.
34. ISO/IEC 27001:2013 – Information Security Management Systems.
35. European Union. *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679.