Procjena sajber rizika vođena vještačkom inteligencijom u savremenim poslovnim informacionim sistemima

Gradimirka Popović
Akademija strukovnih studija kosovsko metohijska
Leposavić, Republika Srbija
gradimirkapopovic@akademijakm.edu.rs
https://orcid.org/0009-0007-9045-6739

Alen Kamiš
Visoka škola za uslužni biznis
Sokolac – Istočno Sarajevo, Bosna i Hercegovina,
alen@vub.edu.ba
https://orcid.org/0009-0004-6224-3515

Aleksandar Zakić
Alfa BK Univerzitet
Fakultet informacionih tehnologija
Beograd, Republika Srbija
aleksandar.zakic@alfa.edu.rs
https://orcid.org/0000-0002-9251-7706

Bogdan Ignjatović
Hiting Frankfurter
Groß-Gerau, Njemačka
https://orcid.org/0009-0004-4425-1378

Dejan Milić
Akademija za nacionalnu bezbednost
Beograd, Republika Srbija
dejsnmilic00@gmail.com
https://orcid.org/0000-0002-0229-5960

Đorđe Šarčević
Akademija strukovnih studija
Šabac, Republika Srbija
sarcevicdjordje@gmail.com
https://orcid.org/0000-0003-0746-744X

***Sažetak*—U radu je predstavljen i detaljno objašnjen novi tip metodologije AI-Driven Cyber Risk Assessment prožet kroz studije slučaja kojeg čine četiri kompanije iz Bosne i Hercegovine. Savremeni pristupi informacionoj sigurnosti provođenjem i sve više se oslanjaju na dinamične i adaptivne modele procjene rizika, koji prvazilaze statičke periodične provjere i omogućavaju stalno praćenje stanja sistema. AI-Driven Cyber Risk Assessment predstavlja jednu od novih metodologija u informacionoj sigurnosti, koja se fokusira na analizu i smanjenje sajber rizika.**

***Ključne riječi* - informaciona sigurnost; dinamička procjena prijetnji AI-Driven Cyber Risk Assessment; studija slučaja;**

I. UVOD

AI-Driven Cyber Risk Assessment predstavlja paradigmatski pomak u ovom smislu, jer koristi modele mašinskog učenja za obradu velikih količina podataka iz različitih izvora i donošenje odluka u realnom vremenu [1]. Takav pristup nije ograničen na otkrivanje postojećih prijetnji već je sposoban predviđati potencijalne ranjivosti na osnovu obrazaca aktivnosti i anomalija. Time se organizacijama nudi prilika da reaguju preventivno, umjesto reaktivno, čime se smanjuje vjerovatnoća nastanka štetnih posljedica. U nacionalnim okvirima zaštita informacionih sistema postala je prioritet državne sigurnosne politike zbog opasnosti koje proizlaze iz aktivnosti organizovanog sajber kriminala, industrijske špijunaže i geopolitički motivisanih napada [4]. Naročito su industrijski sektori koji upravljaju kritičnom infrastrukturom ili ekonomskim podacima targetirani sofisticiranim metodama napada. U tom kontekstu, integracija veštačke inteligencije sa procesima kontrole može značajno smanjiti vrijeme potrebno za detekciju incidenata, što direktno utiče na sposobnost adekvatnog odgovora. Analizom četiri studije slučaja iz Bosne i Hercegovine biće prikazan način primjene nove metodologije u različitim industrijskim sektorima. Iako profili rizika variraju u zavisnosti od broja zaposlenih, tipa radnih stanica, strukture serverskog okruženja i rješenja za rezervne kopije podataka, rezultati pokazuju ujednačen trend povećanja otpornosti na sajber prijetnje kod svih subjekata nakon implementacije ovih pristupa.[2] Posebno je važno naglasiti da su firme koje su posjedovale formalizovane procedure informacionog bezbjednosnog menadžmenta bile spremnije da ove metode inkorporiraju u svoje poslovne tokove. Interesantno je posmatrati kako tradicionalni alati funkcionišu u sinergiji sa AI-vođenim analizama rizika

II. DEFINICIJA I ZNAČAJ INFORMACIONE SIGURNOSTI

Informaciona sigurnost se u najširem smislu definiše kao skup tehničkih, administrativnih i pravnih mjera kojima se štite podaci i informacioni sistemi od neovlašćenog pristupa, izmjene, uništavanja ili ometanja rada. Ona obuhvata zaštitu integriteta, povjerljivosti i dostupnosti informacija, što je prepoznato kao temelj normalnog funkcionisanja savremenih organizacija [3]. Njena važnost proizlazi iz činjenice da digitalni sistemi predstavljaju centralni nervni sistem poslovanja, infrastrukture i državnih institucija. Bilo kakve zloupotrebe ili prekidi u njihovom radu mogu imati domino efekat na šire okruženje. Savremeni koncepti informacione sigurnosti nadilaze tradicionalno shvatanje zaštite podataka kroz statičke mehanizme. Umesto periodične evaluacije, uvodi se kontinuirano praćenje i procjena rizika. AI-Driven Cyber Risk Assessment funkcioniše tako što algoritmi mašinskog učenja analiziraju obrasce upotrebe sistema i detektuju anomalije koje mogu ukazivati na prijetnje u nastajanju [1]. Na ovaj način moguće je reagovati čak i prije nego što dođe do incidenta, dok su tradicionalne metode često ograničene na naknadnu analizu. Uz tehničku verifikaciju implementiranih bezbjednosnih kontrola, ovdje posebno mjesto zauzimaju procedure vezane za upravljanje digitalnim certifikatima i enkripcijskim ključevima kako bi se osigurala autentifikacija svih učesnika komunikacije. Sa stanovišta tehničke implementacije, informaciona sigurnost obuhvata višeslojnu zaštitu (defense in depth) informacionih sistema. U IoT okruženjima se primjenjuju mehanizmi kao što su nadzor prijava na sistem, antivirusna rešenja, sistemi za detekciju i prevenciju napada te softverski analizatori mrežnog saobraćaja [1]. Podaci iz ovih izvora se automatski obrađuju kroz SIEM platforme koje povezuju događaje na način da olakšaju otkrivanje složenih scenarija napada koji se inače mogu previdjeti. Važnost informacione sigurnosti raste proporcionalno zavisnosti poslovanja od mrežne i serverske infrastrukture [6]. Sada i sektori male privrede danas koristi

servisne modele koji povezuju lokalne resurse s eksternim cloud platformama, što dodatno proširuje površinu potencijalnog napada. Zbog toga je sinergija između tehnologije poput AI-driven analitike i stalnog unapređenja svijesti zaposlenih o sajber rizicima postala jedan od glavnih preduslova otpornog informacionog okruženja.

Komponente informacione sigurnosti se u praksi posmatraju kroz tri osnovna principa: integritet, povjerljivost i dostupnost podataka. Integritet osigurava da informacija nije izmenjena bez ovlaštenja, čuvajući konzistentnost zapisa od momenta kreiranja do krajnje upotrebe. Povjerljivost sprečava neovlašćen pristup osjetljivim podacima, dok dostupnost garantuje da ovlašćeni korisnici mogu doći do informacija i sistema kada im je to potrebno [3]. Ovi principi se međusobno prožimaju i čine osnovu na kojoj se nadograđuju klasične sa savremenim metodologije poput AI-Driven Cyber Risk Assessment-a Primjena AI-Driven Cyber Risk Assessment-a dodaje sloj proaktivnosti ovim komponentama, jer algoritmi mašinskog učenja analiziraju tokove podataka radi detekcije anomalija koje bi mogle ukazivati na kompromitovane sisteme [1].The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. PRAVNI I REGULATORNI OKVIR

Pravni i regulatorni okvir informacione sigurnosti u Bosni i Hercegovini oslanja se na mješavinu entitetskih propisa, nacionalnih strategija i međunarodnih standarda, što u praksi stvara složeno okruženje za dosljednu implementaciju bezbjednosnih politika. Nedostatak jedinstvenog zakona na državnom nivou, poput onog koji postoji u Republici Srpskoj kroz Zakon o informacionoj bezbjednosti, dovodi do neusklađenosti propisa između entiteta.[12] Postojanje takve divergencije otežava digitalnu zaštitu sistema koji posluju širom države, naročito kod sektora čija infrastruktura prelazi administrativne granice. Činjenica da je Vlada Federacije BiH bila u procesu izrade sličnog zakonskog akta, ali da njegova sudbina ostaje nepoznata i nakon dvije godine od objave javnog poziva za komentare [3], ukazuje na sporost zakonodavnog odgovora u području koje zahtjeva agilnost. Sprovedene studije slučaja pokazuju da primjena metodologije AI-Driven Cyber Risk Assessment, zavise od pravne osnove koja omogućava razmjenu podataka i nesmetano praćenje bezbjednosnih parametara. Bez jasnog pravnog okvira koji definiše standarde takve obrade podataka, postoji rizik da procedure ne budu jednako primenjene ili priznate između različitih jurisdikcija unutar BiH. Finansijski sektor je zbog prirode svojih podataka naročito osjetljiv na propuste u regulativi. Po zakonima koji regulišu elektronsku obradu podataka jasno su definisane kaznene odredbe za neovlašteni pristup garantovano zaštićenim sistemima [4]. Međutim, slabosti se javljaju kod međunarodne korespondencije ili transakcija koje se odvijaju preko granice, jer nije uvijek jasno kako domaći zakon štiti podatke van teritorijalne nadležnosti. Pravna osnova za ovakvu provjeru proizlazi iz ugovornih obaveza i propisa o zaštiti intelektualne svojine te informacija poslovne tajne [3]. Ako dobavljač djeluje iz druge jurisdikcije unutar regiona ili Evropske unije, tada domaći zakon mora biti komplementaran s međunarodnim okvirima poput GDPR-a da bi evaluacija imala pravni učinak. Institucionalna dimenzija također ima značajnu ulogu; postojanje relevantnih tijela zaduženih za upravljanje sajber incidentima zavisi o organizaciono-pravnom okviru koji im daje mandat za djelovanje. Nedovoljna svest o prijetnjama i ranjivostima kod aktera ne postojanje državnog CERT (Centar za bezbjednost informaciono-komunikacionih sistema organa) smanjuje efektivnost postojećih normi [10] Područje sajber bezbjednosti na državnom nivou zahtjeva strateške dokumente koji definišu procedure zaštite kritične infrastrukture. Bez njih ni najsofisticiraniji AI-Driven sistemi neće imati potpunu pravnu podršku potrebnu za operativno reagovanje kod prijetnji koje prelaze granice pojedinačne organizacije. Postojeći zakoni ponekad ostavljaju prostor za različita tumačenja zbog specifične ustavno-političke strukture zemlje koja utiče na harmonizaciju propisa [3]. Ovo može dovesti do unutrašnjih podjela između entiteta u načinu primjene bezbjednosnih procedura pa čak i do kašnjenja pri usvajanju modernih metoda zaštite kakve se koriste u drugim jurisdikcijama. Sa aspekta praktične implikacije to znači da organizacije koje žele koristiti napredne metodologije moraju paralelno pratiti međusobno različite skupove regulatornih zahtjeva. Kombinovanje tehničkih mjera iz prethodne analize sa infrastrukturnom podrškom pravnog sistema izgleda neophodno ako se želi očuvati integritet, poverljivost i dostupnost informacija opisanih ranije u djelu rada [9]. Zakoni sami po sebi stvaraju temelje odgovornosti, dok tehnologija doslovno mjeri indikatore rizika u realnom vremenu [1]. Tek kroz ovu sinergiju moguće je efikasno reagovati na sve sofisticiranije prijetnje i napade.

IV. AI-DRIVEN CYBER RISK ASSESSMENT - NAPREDNE METODOLOGIJE PROCJENE SAJBER RIZIKA

Primjena metodologije AI-Driven Cyber Risk Assessment u različitim industrijskim granama (studija slučaja ovog rada) Bosne i Hercegovine pokazala se kao centralni alat za naprednu procjenu i neutralizaciju sajber prijetnji. Za razliku od tradicionalnih pristupa, ova metodologija se zasniva na automatizovanom modeliranju rizika kroz algoritme mašinskog učenja, sposobne da analiziraju ogromne količine operativnih podataka iz heterogenih izvora u realnom vremenu [1]. AI-Driven Cyber Risk Assessment metodologija integriše podatke iz različitih sigurnosnih i infrastrukturnih izvora, uključujući SIEM sisteme, EDR/XDR rješenja, mrežne i aplikativne logove, alate za skeniranje ranjivosti, cloud i identity platforme, koji se normalizuju i koreliraju radi stvaranja jedinstvene baze za analizu, a zatim koristi tehnike mašinskog učenja za identifikaciju poznatih i nepoznatih obrazaca napada, korelaciju ranjivosti sa aktivnim prijetnjama i modeliranje mogućih puteva napada, dok AI modeli analiziraju historijske incidente, aktuelne prijetnje i kontekstualne faktore kako bi dinamički procijenili vjerovatnoću i uticaj prijetnji na sisteme, aplikacije, korisnike i poslovne funkcije, omogućavajući kontinuirano rangiranje i prioritetizaciju rizika, prediktivnu analizu i simulaciju „šta-ako“ scenarija za proaktivno planiranje sigurnosnih mjera, te generisanje automatizovanih preporuka i odgovora za ublažavanje rizika, uključujući zakrpe, prilagođavanje politika i unapređenje kontrola pristupa, a sve u cilju povećanja otpornosti i sigurnosti organizacije.[8] Takav sistem nije ograničen na pasivnu detekciju već aktivno predviđa potencijalne ranjivosti na temelju anomalija u ponašanju

korisnika i infrastrukture. Kontinuirano prikupljanje podataka o mrežnom saobraćaju, pristupima sistemima i promjenama konfiguracija omogućava dublje sagledavanje statusa kontrola koje štite integritet, poverljivost i dostupnost informacija. Tehnički aspekt ove metodologije temelji se na sinergiji između tehnologija enkripcije javnim/privatnim ključem (PKI sistemi), inteligentnog nadzora mrežnog saobraćaja kroz SIEM platforme te mašinskog učenja sposobnog da distinktivno identifikuje obrasce incidenata [5]. Kada takav ekosistem radi sinhronizovano, moguće je automatski detektovati kompromitovane naloge i računare ili netipičnu upotrebu privilegovanih naloga u samom trenutku kada prijetnja nastaje. Ovo skraćuje vrijeme reakcije i povećava vjerovatnoću uspješnog sprečavanja posljedica visokotehnoloških napada. Uprkos tome što nijedan sigurnosni okvir ne garantuje apsolutnu zaštitu od svih oblika sajber prijetnji, iskustvo iz ovih studija slučaja potvrđuje da kombinacija naprednih analitičkih metoda unutar AI-Driven Cyber Risk Assessment-a sa kontinuiranim praćenjem i procjenom može drastično smanjiti izloženost organizacija specifičnim napadima poput APT kampanja, MITM presretanja ili internih zloupotreba privilegovanih naloga [4]. Oslanjanje samo na statičke mehanizme odbrane postaje neadekvatno kada protivnici koriste prediktivne taktike za minimiziranje svog otiska dok djeluju unutar kompromitovanih sistema. [11] Iz tog razloga ova metodologija nosi dodatnu vrijednost jer primjenjuje iste analitičke principe predviđanja ponašanja – ali sada ih koristi u svrhu zaštite umjesto eksploatacije ranjivosti.[7]

V. INDUSTRIJSKI KONTEKST PRIMJENE METODOLOGIJE – STUDIJA SLUČAJA

Studija slučaja je zasnovana na primjeru četiri kompanije, koje dolaze iz različitih industrijskih grana. Zamoljeni smo da ne navodimo imena kompanija u radu. Podaci su dobiveni anketom u doktorskoj disertaciji jednog od autora.

A. Kompanija iz drvne industrije

Prva kompanija obuhvaćena studijom slučaja posluje u sektoru drvne industrije i zapošljava približno 120 zaposlenih. Informaciono-tehnološka infrastruktura ove kompanije je relativno jednostavna i sastoji se od ukupno 25 radnih stanica, uključujući pet industrijskih mašina koje u svom sastavu imaju ugrađene personalne računare, kao i jednog centralnog servera.

Kompanija ne posjeduje implementirano backup rješenje, što predstavlja značajan rizik u pogledu dostupnosti i integriteta podataka. IT okruženje je pretežno orijentisano na podršku proizvodnim procesima, sa ograničenim nivom automatizovanih sigurnosnih kontrola i bez formalizovanog sistema upravljanja informacionom sigurnošću. Ovakva infrastruktura čini ovu kompaniju pogodnom za analizu primjene savremenih AI-baziranih metodologija procjene i upravljanja sajber rizicima u okruženjima sa niskim stepenom digitalne zrelosti.

B. Kompanija iz industrije kože i galanterije

Druga kompanija uključena u studiju slučaja posluje u industriji kože i galanterije i zapošljava oko 300 radnika. Informaciona infrastruktura kompanije sastoji se od 20 radnih stanica, dvije industrijske mašine sa integrisanim računarima, kao i dva servera.

Za razliku od prethodnog slučaja, kompanija posjeduje lokalno backup rješenje, koje se realizuje putem drugog servera. Iako ovo predstavlja osnovni nivo zaštite podataka, takvo rješenje i dalje nosi određene rizike u pogledu otpornosti na incidente poput ransomware napada, hardverskih kvarova ili fizičkih prijetnji. Kompanija nema formalno uvedene međunarodne standarde upravljanja kvalitetom ili informacionom sigurnošću, što omogućava sagledavanje efekata primjene kontinuiranih AI-baziranih metodologija procjene rizika u industrijskom okruženju srednje složenosti.

C. Kompanija iz sektora prodaje i održavanja automobila

Treća kompanija obuhvaćena studijom slučaja bavi se prodajom i održavanjem novih automobila i zapošljava približno 75 zaposlenih. IT infrastruktura ove kompanije uključuje oko 50 radnih stanica, pet industrijskih računara, kao i četiri servera. Kompanija posjeduje lokalno backup rješenje koje se koristi za zaštitu poslovno kritičnih podataka.

Za razliku od prethodnih kompanija, ova organizacija je certifikovana prema standardu ISO 9001, što ukazuje na postojanje formalizovanih poslovnih procesa i sistema upravljanja kvalitetom. Ipak, ISO 9001 ne obuhvata direktno upravljanje informacionom sigurnošću, što ovu kompaniju čini interesantnom za analizu integracije novih AI-Driven metodologija procjene sajber rizika u već postojeće upravljačke i operativne procese.

D. Kompanija – sistem integrator

Četvrta kompanija uključena u studiju slučaja posluje kao sistem integrator i zapošljava oko 90 zaposlenih. IT infrastruktura ove kompanije je najkompleksnija među analiziranim slučajevima i obuhvata 120 radnih stanica (90 laptop računara i 30 desktop računara), šest fizičkih servera na kojima je implementirano oko 30 virtuelnih servera, centralni storage sistem, jedan NAS uređaj, kao i S3 immutable online storage rješenje.

Kompanija posjeduje certifikate ISO 9000 i ISO/IEC 27001, što ukazuje na visok stepen formalizacije procesa i zrelosti u upravljanju kvalitetom i informacionom sigurnošću. Ovakvo okruženje predstavlja pogodan primjer za primjenu naprednih AI-baziranih metodologija kao što su kontinuirana procjena rizika, kontinuirani monitoring kontrola, kao i upravljanje rizicima u lancu snabdijevanja i odnosima sa trećim stranama.

VI. ANALIZA I REZULTATI

Studija slučaja je zasnovana na primjeru četiri kompanije, koje dolaze iz različitih industrijskih grana. Zamoljeni smo da ne navodimo imena kompanija u radu. Podaci su dobiveni anketom u doktorskoj disertaciji jednog od autora.

U okviru AI-Driven Cyber Risk Assessment metodologije, sajber rizik se definiše kao dinamička funkcija vjerovatnoće, uticaja i kontekstualne izloženosti, pri čemu se vrijednosti procjenjuju pomoću AI modela treniranih nad sigurnosnim i operativnim podacima.

Osnovna definicija rizika data je izrazom:

$$R = P \times I \tag{1}$$

gdje je:

- R – sajber rizik
- P – vjerovatnoća realizacije prijetnje (AI-procjena)

- I – uticaj incidenta na poslovanje

Vjerovatnoća realizacije prijetnje modeluje se kao funkcija više varijabli:

$$P = f(V, T, H) \tag{2}$$

gdje su:

- V – nivo tehničkih ranjivosti (npr. CVE, konfiguracije)
- T – aktuelni threat intelligence
- H – istorijski sigurnosni incidenti

AI model (npr. logistička regresija ili neuronska mreža) aproksimira vjerovatnoću u opsegu:

$$P \in [0,1]$$

Modeliranje uticaja incidenta se definiše kao ponderisana suma poslovnih posljedica:

$$I = w_1 I_{fin} + w_2 I_{ops} + w_3 I_{rep} \tag{3}$$

gdje su:

- I_{fin} – finansijski uticaj
- I_{ops} – operativni uticaj
- I_{rep} – reputacioni uticaj
- $w_1 + w_2 + w_3 = 1$ – ponderi određeni AI analizom poslovnog konteksta

AI-Driven metodologija uvodi faktor izloženosti sistema(Attack Surface Factor):

$$E \in [0,1]$$

koji zavisi od:

- broja i tipa IT resursa
- povezanosti sistema
- dostupnosti sa interneta

Konačni AI-Driven model rizik za pojedinačnu prijetnju definiše se kao:

$$R_{AI} = P \times I \times E \tag{4}$$

Za cjelokupno okruženje, ukupni rizik je:

$$R_{AI}^{total} = \sum_{i=1}^{n} (P_j \times I_j \times E_j) \tag{5}$$

gdje je n broj identifikovanih prijetnji.

Radi poređenja između različitih organizacija, rizik (indeks rizika) se normalizuje na skalu 0–100:

$$R_{index} = \frac{R_{AI}^{total}}{R_{AI}^{max}} \times 100 \tag{6}$$

gdje je:

R_{AI}^{max} – maksimalna teorijska vrijednost rizika u analiziranom skupu

A. Skup podataka i treniranje AI modela

AI modeli korišteni u istraživanju trenirani su nad empirijskim podacima prikupljenim putem strukturisane ankete sprovedene u okviru doktorske disertacije jednog od autora, kao i nad dodatnim tehničkim podacima dobijenim analizom IT infrastrukture uključenih organizacija.

Ukupan skup podataka obuhvatao je:

- 4 organizacije iz različitih industrijskih sektora
- 68 identifikovanih sigurnosnih kontrola (tehničkih i organizacionih)
- 42 tipa prijetnji mapiranih prema MITRE ATT&CK i ENISA klasifikacijama
- tri godine istorijskih podataka o incidentima (2023–2025)
- 120+ identifikovanih tehničkih ranjivosti (CVE klasifikacija)

Podaci su uključivali:

- Rezultate procjene ranjivosti (V)
- Evidentirane sigurnosne incidente (H)
- Procjenu poslovnog uticaja (finansijski, operativni i reputacioni)
- Parametre izloženosti sistema (broj javno dostupnih servisa, segmentacija mreže, backup arhitektura, postojanje SOC nadzora i sl.)

B. Model (AI) vještačke inteligencije

Za procjenu vjerovatnoće realizacije prijetnje korištena su dva modela:

- logistička regresija (baseline model)
- višeslojna neuronska mreža (MLP - Multi-Layer Perceptron sa jednim skrivenim slojem)

Ulazne varijable modela bile su:

X = {V, T, H, broj endpointa, broj javnih servisa, tip backup rješenja, segmentacija mreže, postojanje ISO standarda}

Model je treniran na 80% skupa podataka, dok je 20% korišteno za validaciju. Prosječna tačnost klasifikacije realizacije incidenta iznosila je 84%, dok je AUC (Area Under the Curve) vrijednost iznosila 0,87.

Ponderi w_1, w_2 i w_3 u izrazu (3) određeni su optimizacijom funkcije gubitka modela, čime je omogućeno prilagođavanje težinskih faktora specifičnom poslovnom kontekstu organizacije.

C. Definicija scenarija prije i poslije primjene AI metodologije

Vrijednosti indeksa rizika prije i poslije ne predstavljaju promjenu samog modela, već promjenu stanja sigurnosnih kontrola u organizaciji.

1) Prije primjene AI metodologije

Vrijednost prije odnosi se na početno stanje organizacije, karakterisano:

- nedostatkom formalizovane procjene rizika

- nepostojanjem kontinuiranog monitoringa prijetnji
- ograničenim ili nepostojećim backup rješenjima
- slabom segmentacijom mreže
- nepostojanjem centralizovanog log menadžmenta
- reaktivnim pristupom incidentima

Rizik je izračunat na osnovu realnog stanja infrastrukture u trenutku inicijalne analize.

2) Poslije primjene AI-Driven metodologije

Vrijednost poslije predstavlja simulirano stanje organizacije nakon implementacije preporuka generisanih AI modelom, koje su uključivale:

- uvođenje strukturisane procjene rizika
- implementaciju 3-2-1 backup strategije
- segmentaciju mreže i izolaciju kritičnih sistema
- uvođenje MFA autentifikacije
- implementaciju EDR nadzora
- kontinuirani monitoring prijetnji
- definisanje formalnog incident response procesa

Indeks rizika poslije izračunat je primjenom istog matematičkog modela (4) i (5), ali sa ažuriranim parametrima P, I i E koji reflektuju unaprijeđeno stanje sigurnosnih kontrola.

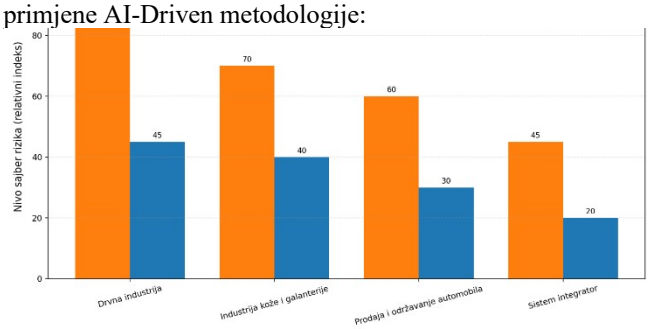
3) Rezultati primjene AI metodologije

Na osnovu primjene navedenog modela, dobijeni su sljedeći indeksi rizika prikazani u Tabeli I

TABLA I. – Prikaz rezultata AI-Driven model rizika

Kompanija	Indeks rizika prije primjene AI metodologije	Indeks rizik poslije primjene AI metodologije
Drvna industrija	85	45
Industrija kože i galanterije	70	40
Prodaja i održavanje automobila	60	30
Sistem integrator	45	20

Grarfički prikazani su rezultati na Slici 1 prije i poslije primjene AI-Driven metodologije:



Slika 1 – Prikaz rezultata prije i nakon primjene AI-Driven metodologije procjene rizika

Primjena AI-Driven Cyber Risk Assessment metodologije pokazala je značajan uticaj na redukciju sajber rizika u različitim industrijskim sektorima. Na osnovu uporednih vrijednosti prije i poslije implementacije, evidentno je da je došlo do značajnog smanjenja rizika u svim posmatranim kategorijama.

Drvna industrija bilježi pad sa 85 na 45, što predstavlja apsolutno smanjenje od 40 indeksnih poena, odnosno relativno smanjenje indeksa rizika od približno 47,1%. Ovaj rezultat ukazuje na gotovo prepolovljen nivo rizika, što je indikativno za visoku efikasnost primijenjene metodologije u sektoru sa tradicionalnim procesima.

Industrija kože i galanterije ostvarila je redukciju sa 70 na 40, što je smanjenje od 30 poena ili oko 42,9%. Iako je procentualno smanjenje nešto manje u odnosu na drvnu industriju, rezultat i dalje potvrđuje značajan napredak u mitigaciji sajber prijetnji.

Kompanija koja se bavi prodaja i održavanje automobila pokazuje pad sa 60 na 30, što je apsolutno smanjenje od 30 poena, odnosno 50%. Ovaj podatak sugeriše da je sektor automobilske industrije posebno osjetljiv na optimizaciju kroz AI-Driven pristupe, vjerovatno zbog kompleksnosti digitalnih servisa i povezanih sistema.

Kompanija sistem integrator bilježi najveći relativni napredak, sa smanjenjem sa 45 na 20, što predstavlja redukciju od 25 poena ili približno 55,6%. Ovaj rezultat ukazuje na izuzetnu efikasnost metodologije u okruženju koje se bavi integracijom različitih tehnoloških rješenja, gdje je kontrola rizika ključna.

VII. ZAKLJUČAK

U okviru ovog istraživanja analizirana je primjena AI-Driven Cyber Risk Assessment metodologije kroz studiju slučaja četiri kompanije iz različitih industrijskih sektora u Bosni i Hercegovini. Metodologija se pokazala kao efikasan alat za kvantitativnu i objektivniju procjenu sajber rizika, zasnovanu na analizi velikih količina podataka, prediktivnom modeliranju prijetnji i kontekstualnoj evaluaciji izloženosti informacionih sistema. Za razliku od tradicionalnih pristupa, AI-Driven Cyber Risk Assessment metodologija omogućava dinamičku procjenu rizika i bržu identifikaciju kritičnih tačaka u IT okruženju.

Rezultati dobijeni primjenom predloženog modela ukazuju da sve analizirane kompanije ostvaruju značajno smanjenje nivoa sajber rizika nakon uvođenja AI-Driven procjene. Uočen je pad indeksa sajber rizika u rasponu od približno 42,9% do 55,6%, što jasno potvrđuje visok potencijal ove metodologije u unapređenju sajber sigurnosti. Najveći relativni efekat zabilježen je kod kompanije koja posluje kao sistem integrator, što se može povezati sa već postojećim stepenom digitalne zrelosti i mogućnošću efikasnije integracije AI-baziranih sigurnosnih mehanizama. Istovremeno, kompanije iz drvne industrije i sektora prodaje i održavanja automobila također bilježe značajna poboljšanja, uprkos nižem početnom nivou sigurnosne zrelosti.

Dobijeni nalazi ukazuju da je integracija naprednih tehnika vještačke inteligencije u procese upravljanja sajber rizikom strateški opravdana i da donosi mjerljive i uporedive koristi u različitim industrijskim domenima. Na osnovu rezultata istraživanja može se zaključiti da AI-Driven Cyber Risk Assessment predstavlja održiv i skalabilan pristup koji može značajno doprinijeti unapređenju otpornosti informacionih sistema i ukupnog nivoa sajber sigurnosti u savremenim poslovnim okruženjima.

LITERATURA

[1] M. Stojanović, J. Marković-Petović, Dinamička procena bezbednosnog rizika u industrijskim IoT sistemima, Novembar 2021. https://doi.org/10.37528/ftte/9788673954455/postel.2021.020.

[2] O. Matthew Ijiga, I. Peter Idoko, G. Isenyo Ebiega, F. Itunu Olajide, T. Isaiah Olatunde, and C. Ukaegbu, Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention, Open Access Research Journal of Science and Technology, vol. 11, no. 1, pp. 001–004, May 2024, https://doi.org/10.53022/oarjst.2024.11.1.0060.

[3] P. Ukić, Pravni okvir zaštite od visokotehnološkog kriminala u Bosni i Hercegovini – analiza strateških ciljeva i mogućnost usklaivanja sa evropskom strategijom sajber bezbednosti, 45RKKP, tom 61, izd. 2, str. 45–67, August. 2023, https://doi.org/10.47152/rkkp.61.2.3.

[4] К. Јонев, Х. Бериша, А. Ћираковић, Информациона безбедност Руске федерације, str. 100, 2018, https://doi.org/10.5937/vojdelo1802100J.

[5] Z. Vujić, V. Rajs, Sajber bezbednost u automobilskoj industriji, Zbornik radova Fakulteta tehničkih nauka, Novi Sad, Februar 2019., https://doi.org/10.24867/29IH02Vujic

[6] Ž. Milojević, L. Dulović, Velike baze podataka – Big Data, primena u vojno-bezbednosnom sistemu, str. 236, Mart 2018, https://doi.org/10.5937/vojdelo1803236M.

[7] C. Ratnawat and C. Prakash, Sarcouncil Journal of Multidisciplinary under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 (CC BY-NC- ND 4.0) International License Revolutionizing Cyber Insurance: AI-Driven Risk Scorecards for SMEs, July 2025, https://doi.org/10.5281/zenodo.15793533.

[8] Y. Agzayal and M. Bouhorma, AI-Driven Cyber Risk Management Framework, , pp. 571–584, Jan. 2024, https://doi.org/10.1007/978-3-031-53824-7_51.

[9] W. Stallings, Cryptography and network security : principles and practice. Hoboken, New Jersey: Pearson Education, Inc, 2020.

[10] M. Nikolić, M. Petrović, Analiza konteksta, rizika i prilika u procesu upravljanja medicinskim otpadom na teritoriji Autonomne pokrajine Vojvodine, Zbornik radova Fakulteta tehničkih nauka, Novi Sad, Mart 2024. https://doi.org/10.24867/24HZ03Nikolic.

[11] G. Sam, E. R Kaburuan, AI-Driven Cyber Risk Assessment: Protecting against Cyberthreats Determined with Machine Learning." Journal of Wireless Networks and Communication Systems, 2025, https://jwncs.melangepublications.com/index.php/jwncs/article/view/9

[12] Уредба-о-мјерама-информационе-безбједности-РС, https://cert.aikt.rs/ova_doc/uredba-o-mjerama-informacione-bezbjednosti-rs/.

ABSTRACT

This paper presents and provides a detailed explanation of a new type of methodology, AI-Driven Cyber Risk Assessment, applied through a case study involving four companies from Bosnia and Herzegovina. Contemporary approaches to information security are increasingly based on dynamic and adaptive risk assessment models, which go beyond static, periodic evaluations and enable continuous monitoring of system security posture. AI-Driven Cyber Risk Assessment represents one of the emerging methodologies in information security, focusing on the analysis and mitigation of cyber risks.

Keywords - information security; dynamic threat assessment; AI-Driven Cyber Risk Assessment; case study;

ARTIFICIAL INTELLIGENCE-DRIVEN CYBER RISK ASSESSMENT IN MODERN BUSINESS INFORMATION SYSTEMS

Gradimirka Popovic, Alen Kamis, Aleksandar Zakic, Bogdan Ignjatovic, Dejan Milic, Djordje Sarcevic