

VEŠTAČKA INTELIGENCIJA – SAVEZNIK ILI PROTIVNIK U PROCESU OTKRIVANJA PREVARA?¹

Dragomir Dimitrijević

Univerzitet u Kragujevcu, Ekonomski fakultet, dimitrijevicd@kg.ac.rs,
ORCID: 0000-0001-8049-9451

Dragana Paunović

Ekonomsko-trgovinska škola Kraljevo, draganapaunovic14@gmail.com

Apstrakt: Pojava i primena veštačke inteligencije u savremenom poslovnom okruženju više nije novina, već je postala redovna i u nekim delatnostima i neophodna. I pored mnogobrojnih prednosti koje je sa sobom donela primena veštačke inteligencije u savremenom poslovanju ona je i stvorila ogroman „potencijal“ za nove vrste prevara. Ipak njena primena dovela je do stvaranja novih tehnika otkrivanja i sprečavanja prevara u poslovanju kompanija. Posebno važnu ulogu veštačka inteligencija ima u oblasti otkrivanja prevara, gde se koristi za analizu velikih količina podataka, identifikovanje sumnjivih obrazaca (takozvanih znakova upozorenja na postojanje prevara) i unapređenje efikasnosti istražnih postupaka. Cilj ovog rada jeste da se ispita da li veštačka inteligencija predstavlja saveznika ili potencijalnog protivnika u procesu otkrivanja prevara. U radu se analiziraju prednosti primene veštačke inteligencije, kao što su brzina obrade podataka, smanjenje ljudskih grešaka i unapređenje prediktivnih sposobnosti, ali i nove vrste prevara koje su nastale upotrebom veštačke inteligencije. Analiza u radu treba da ukaže na to da veštačka inteligencija, uz pravilnu i odgovornu primenu, može predstavljati snažnog saveznika u procesu otkrivanja i sprečavanja prevara, dok njena nekontrolisana upotreba može otvoriti nove oblike prevara i manipulacija.

Cljučne reči: veštačka inteligencija, prevare, proces otkrivanja prevara

Uvod

Celokupna privreda sveta u današnjem digitalnom dobu doživljava dramatične promene zbog potrebe za brzim prilagođavanjem novim društvenim i ekonomskim stvarnostima, kao i zbog brzine kojom se tehnologija razvija. Veštačka inteligencija koristi svoju sposobnost analize ogromnih količina podataka, prepoznavanja obrazaca i predviđanja prevarantskog ponašanja kako bi ponudila inovativna rešenja za ovaj rastući problem. Mašinsko učenje i napredna analitika predstavljaju ključne alate u borbi protiv prevara. Ove tehnologije omogućavaju analizu brojnih izvora podataka, uključujući finansijske transakcije, kadrovske evidencije, ponašanje potrošača i komunikacione sisteme. One otkrivaju

¹ Ovo istraživanje je finansijski podržano od strane Ministarstva nauke, tehnološkog razvoja i inovacija Republike Srbije (Ugovor br. 451-03-33/2026-03/200099).

skrивene veze i brzo prepoznaju sumnjivo ponašanje. Potrebna je proaktivna odbrana od prevara, jer sprečavanje razvoja novih prevarantskih šema postaje sve važnije. Svedoci smo da se veštačka inteligencija u poslednje vreme sve više koristi za ostvarivanje raznih oblika prevara, kako u svakodnevnom životu ljudi, tako i u poslovanju kompanija. Kao novi „alat“ za ostvarivanje prevara, veštačka inteligencija donosi sa sobom i niz novih oblika prevara protiv kojih sistemi kontrole se sve teže bore, posebno u procesu sprečavanja prevara. Mora se napomenuti da kontrolori koriste veštačku tehnologiju u procesu otkrivanja prevara, posebno finansijskih prevara u formiranju lažnih finansijskih izveštaja. Upravo zbog toga, cilj ovog rada je da se sagleda da li je veštačka tehnologija više saveznik ili novi protivnik u procesu otkrivanja i sprečavanja prevara u poslovanju kompanija.

Pregled literature

Sprečavanje prevara je ključni izazov za finansijske institucije, kompanije i vlade širom sveta. Porast digitalnih transakcija i složenih finansijskih sistema doveo je do sve sofisticiranijih prevarnih aktivnosti. Veštačka inteligencija nudi inovativna rešenja za ovaj rastući problem, koristeći svoju sposobnost da analizira ogromne količine podataka, identifikuje obrasce i predviđa prevarno ponašanje sa visokom tačnošću (Bello & Olufemi, 2024). U trenutnom finansijskom okruženju, upravljanje rizicima i sprečavanje prevara su ključni, a veštačka inteligencija nosi ogromno obećanje za unapređenje ovih oblasti. Prevara je postala velika briga i globalna pojava. Postoji u svakoj zemlji i utiče na sve vrste organizacija, bez obzira na njihovu veličinu, industriju ili nivo profitabilnosti (Sowmiya et al., 2025). Finansijske prevare su se brzo proširile sa rastom digitalne ekonomije, evoluirajući od konvencionalnih transakcionih zloupotreba do složenijih oblika koji zahtevaju mnogo podataka. Tradicionalne metode otkrivanja zasnovane na pravilima su sve neadekvatnije za rešavanje problema obima, heterogenosti i dinamičnog ponašanja modernih prevara. U tom kontekstu, veštačka inteligencija je postala ključni alat u istraživanju otkrivanja finansijskih prevara (Yang et al., 2026). Otkrivanje finansijskih prevara je ključno područje primene mašinskog učenja, posebno imajući u vidu različite vrste prevara. Ove prevare mogu biti interne ili eksterne. Primeri internih napada uključuju finansijske izveštaje ili pranje novca, dok se eksterne prevare mogu desiti kod kreditnih kartica i osiguranja (Aros et al., 2024). Tehnike veštačke inteligencije poput mašinskog učenja i dubokog učenja revolucionisale su detekciju i prevenciju prevara. Algoritmi mašinskog učenja, posebno modeli poput stabala odluke i neuronskih mreža, široko se koriste za identifikaciju sumnjivih transakcija analizom istorijskih podataka. Ovi modeli mogu razlikovati legitimne, ali i lažne transakcije prepoznavanjem obrazaca. Integracija veštačke inteligencije u sprečavanje prevara donosi i izazove, uključujući zabrinutost u vezi sa privatnošću podataka, potrebu za visokokvalitetnim skupovima podataka i problem interpretabilnosti modela veštačke inteligencije. Ipak, prednosti daleko nadmašuju ove prepreke, jer veštačka inteligencija nastavlja da poboljšava tačnost i efikasnost u borbi protiv prevara

(Bello & Olufemi, 2024). Iako veštačka inteligencija pokazuje veliki potencijal u otkrivanju i sprečavanju prevara, njena implementacija se i dalje suočava sa složenim izazovima. Prevare u finansijskom sektoru nastavljaju da se razvijaju sa sve sofisticiranijim obrascima, koristeći nove tehnologije kako bi se izbeglo otkrivanje (Hutagalung, 2024). Međutim, tradicionalni sistemi za otkrivanje prevara imaju ograničenja u otkrivanju novih obrazaca prevara koji još uvek nisu prisutni u njihovim bazama podataka. Tu tehnologija veštačke inteligencije, sa svojim pristupom zasnovanim na mašinskom učenju, ima prednost u identifikovanju anomalija i složenih obrazaca prevara (Dawam, 2024). Veštačka inteligencija nudi niz tehnika koje značajno poboljšavaju mogućnosti otkrivanja prevara. Ove tehnike omogućavaju identifikaciju prevarnih aktivnosti sa većom tačnošću i efikasnošću u poređenju sa tradicionalnim metodama (Hasan et al., 2024; Yalamati, 2023).

Oblici prevara nastali korišćenjem veštačke inteligencije

Razvoj tehnologija zasnovanih na veštačkoj inteligenciji ima višedecenijsku istoriju, pri čemu su teorijski temelji ove oblasti postavljeni sredinom XX veka. Tokom pedesetih godina prošlog veka istraživači, među kojima se posebno isticao Alan Turing, formulisali su ključne koncepte za proučavanje inteligentnog ponašanja računarskih sistema. Jedan od najznačajnijih doprinosa iz tog perioda predstavlja Tjuringov test, osmišljen kao metod za procenu sposobnosti računara da simulira ljudsku komunikaciju i ponašanje. Ipak, značajniji praktični razvoj veštačke inteligencije ostvaren je tek u poslednjim decenijama, pre svega zahvaljujući eksponencijalnom rastu računarske snage, dostupnosti velikih skupova podataka i unapređenju algoritama mašinskog učenja i neuronskih mreža. Onlajn finansijske prevare i obmane nisu nove, ali ih je veštačka inteligencija učinila pametnijim i težim za otkrivanje. Kriminalci sada koriste lažne poruke i veb stranice, lažne profile poznatih ličnosti, pa čak i glasove ili video zapise koje generiše veštačka inteligencija, a koji izgledaju kao lični bankar, prijatelj ili član porodice, kako bi izvršili prevare. Često kontaktiraju ljude putem društvenih mreža, aplikacija za razmenu poruka, imejlova i neočekivanih poziva koji zvuče stvarno. Da bi se ljudi zaštitili od prevara putem veštačke inteligencije, trebali bi, pre svega, da vode računa o sledećim znakovima upozorenja (European Banking Authority, 2025):

- Hitan zahtev za novac ili lične podatke, uključujući i od nekoga ko se pretvara da je član porodice, prijatelj ili čak javna ličnost.
- Zahtev za preuzimanje kontrole nad vašim uređajem, preuzimanje aplikacije, skeniranje QR koda ili klik na link.
- Zahtev za lične podatke ili bankovne podatke (npr. lozinke, brojevi kreditnih kartica, akreditivi za internet bankarstvo ili bezbednosni kodovi).
- Zahtev za plaćanje putem metoda koje se ne mogu pratiti (npr. kriptovalute, poklon kartice, bankovni transferi ili prepaid debitne kartice).
- Sumnjiva ili netačna imejl adresa ili link (npr. pravopisne greške u URL-u ili neobične veb adrese).

- Prilog iz nepoznatog izvora, posebno .exe, .scr, .zip ili Office datoteka sa makroima (.docm, .xlsm).
- Loša gramatika ili formatiranje u dokumentu koji izgleda zvanično, iako veštačka inteligencija može omogućiti prevarantima da efikasnije prikriju ove nedostatke.
- Veb-sajt koji izgleda profesionalno, ali mu nedostaju verifikovani kontakt podaci ili podaci o registraciji kompanije.
- Video snimci gde glas može zvučati robotski ili previše glatko, pokreti usana i izrazi lica mogu biti neusklađeni sa govorom, ili pozadina, osvetljenje i senke mogu biti nedosledni. To su često video snimci generisani veštačkom inteligencijom (dipfejkovi).
- Biti oprezan sa neočekivanim i vremenski ograničenim investicionim prilikama: ako zvuči previše dobro da bi bilo istinito, verovatno jeste.

Prevare nastale upotrebom veštačke inteligencije se stalno „usavršavaju“ od strane počinioaca prevara, što samo znači da ubrzanim razvojem veštačke inteligencije ubrzano se razvijaju i tehnike prevara. Ipak neke od najčešćih prevara upotrebom veštačke inteligencije su sledeće:

1. **Prevvara lažnog predstavljanja i upotreba dubokog fejka** – obično se dešava da žrtva dobije neočekivani poziv od nekoga ko tvrdi da je banka, javni organ (npr. policija, poreska ili finansijska uprava itd.), distributer osiguranja, IT kompanija ili čak član porodice. Pozivalac traži da žrtva prevare prebaci sredstva kako bi se zaštitila, navodeći sumnjive aktivnosti na računu ili polisi osiguranja žrtve tražeći da otkrije svoje bankovne podatke. Prevaranti mogu koristiti veštačku inteligenciju da bi kreirali lažne video zapise, slike, ili zvuk koji imitiraju nečiji glas (npr. bankarskog službenika ili člana porodice), lice (npr. poznate ličnosti), ili pokrete. Ova prevara je poznata kao „Dipfejk“;
2. **Fišing** – žrtva prevare dobija mejl ili poruku koja izgleda kao da dolazi od banke ili finansijske kompanije, upozoravajući o „sumnjivim aktivnostima“ na njenom nalogu. Logo, raspored i jezik izgledaju profesionalno, a poruka podstiče da žrtva klikne na link da bi verifikovala svoj nalog ili resetovala lozinku. Link vodi do lažne veb stranice koja izgleda identično internet bankarstvu. Na ovaj način žrtva unosi svoje podatke na veb stranicu namenjenu da ukrade njene lične podatke. Prevaranti koriste veštačku inteligenciju da bi kreirali ubedljive fišing poruke analizirajući podatke društvenih medija kako bi identifikovali svoje žrtve i prilagodili sadržaj za svaku metu;
3. **Prevvara u vezi sa investicijama** – prevaranti postavljaju oglas na društvenim mrežama ili veb-sajt koji promoviše „vremenski ograničenu investicionu priliku sa niskim rizicima“ ili „vremenski ograničeni popust“ na osiguranje poznate kompanije. Oglas sadrži fotografiju poznate ličnosti i preporuke koje su često lažne. Klikom na link ili popunjavanjem obrasca, žrtva biva kontaktirana i preusmerena na platformu ili kanal za razmenu poruke gde dobija profesionalne savete da investira mali iznos, a zatim veće

sume. Prevaranti koriste alate veštačke inteligencije kako bi ove lažne predloge ili mejlove učinili veoma ubedljivim i teškim za otkrivanje. Takođe koriste botove društvenih mreža koje pokreće veštačka inteligencija da bi kreirali lažne naloge koji komuniciraju sa žrtvama;

4. **„Romantična“ prevara** – žrtvu obično kontaktira neko koga je upoznala preko društvenih mreža, aplikacija za upoznavanje ili telefonom/porukom. Ova osoba vodi česte, lične i romantične razgovore, gradeći poverenje koristeći lažne profile. Vremenom, razgovor se pomera ka novcu ili finansijskim mogućnostima, kao što su kripto-investicije sa obećanjima visokog prinosa i niskog rizika. Prevarant traži da žrtva prebaci novac na račun ili je usmerava na otvaranje naloga i uplatu malog početnog depozita kako bi šema izgledala legitimno pre nego što je podstakne da više investira. Prevaranti koriste veštačku inteligenciju da bi generisali lažne profile, identifikovali svoje žrtve na društvenim mrežama/aplikacijama za upoznavanje koristeći podatke koje ste im dali na raspolaganje ili koriste četbotove za generisanje poruka;
5. **Prevara pri kupovini** – žrtva nailazi na atraktivnu ponudu za kupovinu na onlajn tržištu. Kompanija koja nudi ponudu zahteva plaćanje van zvanične platforme, tvrdeći da koristi „bezbedan sistem plaćanja“ i šalje link za završetak kupovine. Link žrtvu preusmerava na lažnu stranicu za autentifikaciju banke koja imitira zvaničnu veb stranicu banke i koristi njen logo i dizajn, sa ciljem da žrtva da svoje podatke o onlajn bankarstvu kako bi izvršila uplatu. Prevaranti koriste veštačku inteligenciju da bi kreirali veoma ubedljive lažne veb stranice banaka, potvrde porudžbina i fakture. Veštačka inteligencija im pomaže da imitiraju ton, brendiranje i stil pravih kompanija. U nekim slučajevima, koriste četbotove sa veštačkom inteligencijom da bi odgovorili na pitanja i učinili da ponuda izgleda verodostojnijom.

Upotreba veštačke inteligencije u procesu otkrivanja prevara

Veštačka inteligencija se pokazala kao neprocenjiv alat u borbi protiv prevara u različitim sektorima. Njena sposobnost da obrađuje i analizira ogromne količine podataka u realnom vremenu omogućava efikasnije otkrivanje i sprečavanje prevarnih aktivnosti (Jagatheesaperumal et. al., 2021). Istraživanja pokazuju da je 63,6% kontrolnih institucija koje koriste automatizovane metode sprečavanja prevara uspešno sprečilo prevare pre njihove pojave. Neke procene sugerišu da je 80% stručnjaka uvereno u smanjenje prevara korišćenjem platformi zasnovanih na veštačkoj inteligenciji. Sistemi veštačke inteligencije poboljšavaju otkrivanje prevara prepoznavanjem skrivenih obrazaca koje tradicionalni modeli ne uspevaju da uhvate. Istraživanja potvrđuju da veštačka inteligencija ne samo da poboljšava efikasnost otkrivanja prevara, već i smanjuje ljudske greške i kašnjenja u odgovoru. Najveće prednosti korišćenja veštačke inteligencije u procesu otkrivanja prevara u poslovanju kompanija su:

- Sistemi za otkrivanje prevara pomoću veštačke inteligencije koriste mašinsko učenje za analizu obrazaca transakcija i ponašanja korisnika,

označavajući anomalije koje bi mogle ukazivati na prevarne aktivnosti (kao što su neobični obrasci potrošnje ili pokušaji prijavljivanja).

- Prednosti korišćenja otkrivanja prevara pomoću veštačke inteligencije uključuju otkrivanje u realnom vremenu, smanjene troškove, povećanu tačnost i poboljšano poverenje kupaca.
- Efikasno sprečavanje prevara pomoću veštačke inteligencije kombinuje ove inteligentne algoritme za otkrivanje sa proaktivnim merama (kao što su višefaktorska autentifikacija i edukacija korisnika), osnažujući organizacije da u realnom vremenu reaguju na pretnje i efikasnije zaštite imovinu i informacije nego samo ručnim praćenjem.

Detekcija prevara pomoću veštačke inteligencije funkcioniše implementacijom algoritama mašinskog učenja koji analiziraju ponašanja i otkrivaju prevarne anomalije. Potrebno je prvo uspostaviti osnovnu liniju normalnih obrazaca transakcija i ponašanja korisnika. Sistem zatim kontinuirano prati podatke, tražeći odstupanja od ove norme. Kako nailazi na nove i raznovrsne podatke, model veštačke inteligencije fino podešava svoje parametre, efikasnije razlikujući legitimne i sumnjive aktivnosti. Mehanizmi za otkrivanje prevara pomoću veštačke inteligencije uključuju:

- **Prikupljanje podataka:** Agregiranje ogromnih količina podataka iz različitih izvora. Ovo uključuje detalje o transakcijama, lokaciju korisnika, potrošnju korisnika, informacije o uređajima, prijave na naloge i istorijsko ponašanje. Pristup velikim količinama podataka omogućava sistemu veštačke inteligencije da dobije osnovnu liniju ponašanja korisnika i preciznije identifikuje prevarne aktivnosti tokom vremena.
- **Inženjering karakteristika:** Identifikovanje i odabir relevantnih atributa podataka ili karakteristika koje ukazuju na potencijalno prevarno ponašanje. Na primer, u okviru potrošačkog bankarstva, softver za otkrivanje prevara pomoću veštačke inteligencije analizira velike transakcije kako bi otkrio fišing prevare.
- **Obuka modela:** Korišćenje istorijskih podataka za obuku modela mašinskog učenja da prepoznaju obrasce prevara.
- **Detekcija anomalija:** Primena statističkih tehnika (npr. k-najbližeg suseda, faktor lokalnih anomalija, izolacione šume) za identifikaciju anomalija koje odstupaju od standardnih obrazaca.
- **Kontinuirano učenje:** Ažuriranje modela novoidentifikovanim prevarama i tipovima prevara osigurava da se sistem razvija kao odgovor na promenljive taktike.
- **Upozoravanje i izveštavanje:** Označavanje sumnjivih aktivnosti i pružanje detaljnih izveštaja za dalju stručnu istragu.

Veštačka inteligencija se pojavila kao moćno oruđe u borbi protiv prevara, nudeći sofisticirane tehnike i aplikacije koje poboljšavaju napore u otkrivanju i sprečavanju prevara. Tehnike kao što su mašinsko učenje, duboko učenje i obrada prirodnog jezika su ključne u otkrivanju i sprečavanju prevara u različitim

sektorima, od otkrivanja prevara kreditnim karticama do pretnji po sajber bezbednost. Proaktivne strategije za sprečavanje prevara, kao što su prediktivna analitika i sistemi za praćenje u realnom vremenu, su neophodne za prevarante. Predviđanjem potencijalnih žarišta prevara i sprovođenjem preventivnih mera, kompanije mogu smanjiti rizik od pojave prevara. Implementacija strategija za sprečavanje prevara zasnovanih na veštačkoj inteligenciji dolazi sa izazovima, uključujući zabrinutost za privatnost podataka, kvalitet skupova podataka i interpretabilnost modela. Rešavanje ovih izazova je ključno za obezbeđivanje etičke upotrebe i efikasnosti veštačke inteligencije u sprečavanju prevara.

Primer kako veštačka inteligencija može da pomogne u otkrivanju prevara može se videti na primeru fišinga kao jednom od najrasprostranjenijeg oblika prevara. Fišing je oblik onlajn prevare gde napadači pokušavaju da obmanu pojedince da dostave osetljive informacije, kao što su podaci za prijavu ili finansijski detalji. Sistemi zasnovani na veštačkoj inteligenciji mogu da analiziraju imejllove, poruke i veb stranice kako bi otkrili pokušaje fišinga identifikovanjem zlonamernih linkova, sumnjivih adresa pošiljalaca i obmanjujućeg sadržaja. Tehnike obrade prirodnog jezika omogućavaju veštačkoj inteligenciji da razume i tumači kontekst komunikacije, omogućavajući identifikaciju pokušaja fišinga sa visokom tačnošću. Integracijom veštačke inteligencije sa protokolima za bezbednost imejllova i veb filterima, organizacije mogu značajno smanjiti rizik od postajanja žrtvom fišing napada. Implementacijom bezbednosnih rešenja zasnovanih na veštačkoj inteligenciji, organizacije mogu automatizovati otkrivanje i reagovanje na pretnje, smanjujući vreme potrebno za identifikaciju i ublažavanje sajber pretnji. Ovaj proaktivni pristup sajber bezbednosti pomaže u sprečavanju kršenja podataka, zaštiti osetljivih informacija i održavanju integriteta IT sistema.

Sistemi za otkrivanje prevara pomoću veštačke inteligencije nude niz prednosti za preduzeća koja žele da zaštite svoje poslovanje od stalno promenljivih pretnji:

- **Otkrivanje i sprečavanje u realnom vremenu:** Sumnjive aktivnosti se odmah identifikuju putem 24/7 praćenja pomoću sistema za otkrivanje prevara pomoću veštačke inteligencije, što podstiče bržu akciju.
- **Smanjenje troškova:** Otkrivanje prevara pomoću veštačke inteligencije pomaže u sprečavanju finansijskih gubitaka za vlasnike računa i organizacije. Takođe, automatizuje vremenski intenzivan proces identifikacije prevarnih aktivnosti, smanjujući potrebu za budžetiranjem ručnih pregleda.
- **Povećana tačnost:** Sistemi veštačke inteligencije analiziraju i identifikuju podatke znatno brže od ljudi. Ljudi su skloni umoru i pristrasnosti potvrde i mogu da obavljaju samo ograničenu količinu analiza tokom dužeg perioda. Naravno, redovan nadzor, ručni pregled i revizije su potrebni za bilo koju vrstu sistema veštačke inteligencije kako bi se održala tačnost.

Otkrivanje prevara pomoću veštačke inteligencije je tačno koliko i podaci koji se koriste za obuku algoritma i modela. Kompanije koje koriste otkrivanje

prevara moraju se oslanjati na potpune, čiste i tačne podatke kako bi smanjile broj lažno pozitivnih rezultata u svojim tokovima rada za otkrivanje prevara pomoću veštačke inteligencije. Iako je tehnologija veoma vešta u prepoznavanju obrazaca velikih razmera i otkrivanju anomalija, mora da uključi tokove rada za redovne ručne preglede i revizije kako bi se osigurala ukupna tačnost. Iako sistemi za otkrivanje prevara pomoću veštačke inteligencije nude značajne prednosti, oni takođe, dolaze sa nizom izazova sa kojima se preduzeća moraju nositi:

- **Kvalitet i dostupnost podataka:** Sistemi veštačke inteligencije zahtevaju visokokvalitetne, relevantne podatke da bi efikasno otkrili prevaru. Međutim, podaci su često nepotpuni, zastareli ili netačni, što može ometati performanse algoritama veštačke inteligencije i rezultirati nepotpunim skupovima podataka.
- **Postojeća sistemska integracija:** Nisu svi softveri veštačke inteligencije integrisani sa zastarelim sistemima i infrastrukturuom data centra. Mora se proceniti trenutna postavka softvera da bi procenila njegova efikasnost i bezbednost.
- **Lažno pozitivni rezultati:** Veštačka inteligencija automatizuje veliki deo procesa otkrivanja prevara, ali nije savršena i ponekad proizvodi lažna upozorenja, koja dolaze iz preširokih ili loše definisanih pravila. Kontinuirana obuka modela veštačke inteligencije, implementacija softvera i ažuriranja pravila su ključni za minimiziranje pojave lažno pozitivnih rezultata i obezbeđivanje zadovoljstva kupaca.
- **Evolucija prevara:** Tehnike prevara se brzo razvijaju kao odgovor na najnoviji softver za otkrivanje veštačke inteligencije, što zahteva posvećenost stalnim ažuriranjima koja uključuju najnovije podatke o prevarnim aktivnostima.
- **Usklađenost sa propisima i etika:** Osigurati da je korišćenje sistema veštačke inteligencije u skladu sa zakonima o privatnosti i zaštiti podataka potrošača. Pored toga, veštačka inteligencija za procese donošenja odluka pokreće etička pitanja, kao što je mogućnost pristrasnosti u algoritmima, što može dovesti do nepravednog tretmana određenih segmenata kupaca.

Nesporna je efikasnost upotrebe alata veštačke inteligencije u procesu otkrivanja prevara. Ipak, današnji uslovi poslovanja kompanija, neverovatno brzo napredovanje tehnologije zasnovane na veštačkoj inteligenciji, ulaganje velike količine novca u razvoj ove tehnologije, otvaraju mnoga pitanja u kom pravcu će ići proces izvršenja prevara, ali i proces otkrivanja i sprečavanja prevara korišćenjem VI. Danas svako može koristiti veštačku inteligenciju da ostvari prevaru. Pristup njenim alatima je sve lakši i jednostavniji. To umnogome stvara velike probleme kontrolorima, jer ako je sve lakše ostvariti prevaru putem VI, postavlja se pitanje kako sprečiti na vreme sve te nove oblike prevara. Da li razni oblici kontrole (interna i eksterna revizija, forenzičke računovođe, državni kontrolni organi) imaju dovoljno resursa, vremena i znanja da prate ovakav brz razvoj novih oblika prevara putem veštačke inteligencije? Praksa je pokazala da

nažalost nemaju, niti će skorije imati. Problem je što su kontrolni organi znatno „sporiji“ u procesu prilagođavanja i korišćenja veštačke inteligencije, ograničeni zakonskim rešenjima koje ne prepoznaju upotrebu veštačke inteligencije pa samim tim sprečavaju kontrolne organe da brzo i efikasno reaguju na pojavu novih oblika prevara.

Jedno je sigurno, kompanije u svom poslovanju moraju sve više da koriste veštačku inteligenciju iz razloga što donosi veliku uštedu troškova na raznim nivoima poslovanja. Za sada su to najčešće inovativna rešenja koja pomažu u donošenju odluka, brzom obradi velike količine podataka, ali i postepenoj zameni ljudi u izvršenju pojedinih poslova. Trenutno velike kompanije rade na razvoju takozvane „svesne“ veštačke inteligencije koja će moći da donosi samostalne odluke u poslovanju. S obzirom da trenutni nivo razvoja veštačke inteligencije donosi mnogo prostora za ostvarivanje sve većeg broja novih oblika prevara, sa razlogom se postavlja pitanje šta će razvoj ove tehnologije tek doneti na polju prevara. Takođe, opasnost može predstavljati i činjenica da kompanije koje rade na razvoju veštačke inteligencije nemaju jasan cilj čemu će ona sve služiti u budućnosti, tj. dokle je granica njenog razvoja. Samim tim, ako ne postoji tačan cilj njenog razvoja, postoji i opasnost da će počinioци prevara umnogome iskoristiti „mogućnosti“ koje će njen razvoj doneti na polju ostvarivanja prevara.

Zaključak

Sistemi za otkrivanje prevara zasnovani na veštačkoj inteligenciji koriste mašinsko učenje, obradu prirodnog jezika i prediktivnu analitiku kako bi identifikovali sumnjive obrasce, anomalije i lažne transakcije u realnom vremenu. Ove tehnologije poboljšavaju tradicionalne mehanizme za otkrivanje prevara, tako što kontinuirano uče iz novih podataka i poboljšavaju tačnost. Veštačka inteligencija može da analizira velike količine finansijskih podataka kako bi otkrila sumnjiva ponašanja koja mogu ukazivati na pranje novca ili finansijske prevare. Jedna od ključnih prednosti u sprečavanju prevara je njena sposobnost da se prilagodi novim i novonastalim pretnjama. Uprkos svojim prednostima, postoje i izazovi, kao što su etička razmatranja, zabrinutost za privatnost podataka i potencijalne pristrasnosti u donošenju odluka. Obezbeđivanje transparentnosti i odgovornosti u sistemima za otkrivanje prevara vođenim veštačkom inteligencijom je ključno za održavanje poverenja u ove sisteme. Integracija veštačke inteligencije u sprečavanje prevara predstavlja izazove, ali koristi daleko nadmašuju ove prepreke, jer ovaj oblik tehnologije nastavlja da poboljšava tačnost i efikasnost procesa za sprečavanje prevara. Kako se ovi oblici tehnologije razvijaju, njihova uloga u zaštiti finansijskih sistema i smanjenju gubitaka od prevara će samo rasti, naglašavajući važnost kontinuiranih inovacija i istraživanja u ovoj oblasti.

Tehnologije veštačke inteligencije moraju da se razvijaju kako bi otkrile i sprečile nove oblike prevara. Ulaganjem u istraživanje i razvoj, organizacije mogu osigurati da njihovi sistemi ostanu efikasni i prilagodljivi novim pretnjama. Budućnost u sprečavanju prevara izgleda obećavajuće, sa napretkom u mašinskom učenju, dubokom učenju i integraciji sa novim tehnologijama. Očekuje se da će

veštačka inteligencija igrati sve važniju ulogu u sprečavanju prevara u različitim sektorima, šireći se izvan finansijskih usluga na oblasti kao što su zdravstvo, maloprodaja i telekomunikacije. Suština je da počinioci prevara sve lakše koriste ovaj oblik tehnologije, koji strašno brzo napreduje, za razvoj novih oblika prevara. Veštačka inteligencija je pristupnija, brzo se prilagođava, uči, napreduje, a sa njom i počinioci prevara. U svojoj toj situaciji kontrolni organi nemaju ni resursa ni zakonskih ovlašćenja da tako brzo prate razvoj tehnologije i da pokušaju da istu tu tehnologiju koriste u procesu otkrivanja i sprečavanja prevara. To u startu daje veliku prednost počiniocima prevara, posebno u delu finansijskih prevara, kako ljudi, tako i kompanija. Kompanije moraju da ulažu u sisteme zaštite, da edukuju svoje kontrolne organe i da u saradnji sa državnim organima iniciraju donošenje zakonskih rešenja koje će sprečiti nove oblike prevara. To sve košta, za ove procese je potrebno dosta vremena, a počinioci prevara ne čekaju, brzo uče i primenjuju svoje znanje u ostvarivanju prevara. Iz tih razloga, trenutno je veštačka inteligencija veći saveznik počiniocima prevara nego kontrolnim organima.

Reference

- Aros, L. H., Molano, L. X. B., Gutierrez-Portela, F., Hernandez, J. J. M., & Barrero, M. S. R. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications*, 11, Article number: 1130. Preuzeto sa: <https://www.nature.com/articles/s41599-024-03606-0> (02.05.2026).
- Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, 5(6), 1505-1520.
- Dawam, A., & Adwim Rifqy El-Hisan, M. (2024). Peran artificial intelligence dalam mengurangi perilaku koruptif (perspektif pendidikan islam). *syaikhona : Jurnal Magister Pendidikan Agama Islam*. Preuzeto sa: <https://jurnal.stainidaeladabi.ac.id/index.php/syaikhona/article/view/231/119> (02.04.2026).
- European Banking Authority (2025). *Online financial frauds and scams in an Artificial Intelligence world*. Preuzeto sa: <https://www.eba.europa.eu/sites/default/files/2025-12/fa63af9a-bafd-4821-baee-48c7c8fb6490/AI%20and%20online%20financial%20fraud%20and%20scams%20factsheet.pdf> (02.04.2026).
- Jagatheesaperumal, S. K., Rahouti, M., Ahmad, K., Al-Fuqaha, A., & Guizani, M. (2021). The duo of artificial intelligence and big data for industry 4.0: Applications, techniques, challenges, and future research directions. *IEEE Internet of Things Journal*, 9(15), 12861-12885.
- Hasan, M. R., Gazi, M. S., & Gurung, N. (2024). Explainable AI in credit card fraud detection: interpretable models and transparent decision-making for enhanced trust and compliance in the USA. *Journal of Computer Science and Technology Studies*, 6(2), 1-12.

- Hutagalung, E. (2024). Potensi, Tantangan, dan Implementasi Blockchain untuk Pengembangan Aplikasi dalam Era Digital Modern. *Jurnal Multidisiplin Saintek*, 5(3), 1-23.
- Nuraziza, S., Febri, W., & Sudirman, R. (2024). Studi Literatur: Integrasi Artificial Intelligence (AI) dalam Manajemen Keuangan (Tantangan dan Kepatuhan Regulasi) 1, 2(1), 47.
- Sowmiya, B., Ida Seraphim, B., Fancy. C., Abirami, R., & Hussain, A. (2025). Harnessing artificial intelligence in financial fraud detection and prevention systems. *International Journal of Innovative Research and Scientific Studies*, 8(3), 1449-1459.
- Yalamati, S. (2023). Identify fraud detection in corporate tax using Artificial Intelligence advancements. *International Journal of Machine Learning for Sustainable Development*, 5(2), 1-15.
- Yang, H., Shukur, Z., & Sahran, S. (2026). A Review of Artificial Intelligence for Financial Fraud Detection. *Applied Sciences*, 16(4), 1931.

ARTIFICIAL INTELLIGENCE – ALLY OR OPPONENT IN THE PROCESS OF FRAUD DETECTION?

Abstract: *The emergence and application of artificial intelligence in the modern business environment are no longer a novelty; rather, they have become routine and, in some sectors, indispensable. Despite the numerous advantages that artificial intelligence has brought to contemporary business practices, it has also created significant “potential” for new types of fraud. Nevertheless, its application has led to the development of new techniques for detecting and preventing fraud in corporate operations. Artificial intelligence plays a particularly important role in the field of detecting fraud, where it is used to analyze large volumes of data, identify suspicious patterns (so-called red flags indicating potential fraud), and enhance the efficiency of investigative procedures. The aim of this paper is to examine whether artificial intelligence represents an ally or a potential adversary in the process of fraud detection. The paper analyzes the advantages of applying artificial intelligence, such as data processing speed, reduction of human error, and improved predictive capabilities, as well as new types of fraud that have emerged through its use. The analysis seeks to demonstrate that artificial intelligence, when applied properly and responsibly, can serve as a powerful ally in the detection and prevention of fraud, while its uncontrolled use may give rise to new forms of fraud and manipulation.*

Keywords: *artificial intelligence, fraud, fraud detection process*