SorS

35. susret
osiguravača i
reosiguravača
Sarajevo

**SVETLANA STANISAVLJEVIĆ, dr. sc.***

# SUVREMENI ALATI OBRADE ŠTETA U SEKTORU OSIGURANJA

*CONTEMPORARY CLAIMS PROCESSING TOOLS IN THE INSURANCE SECTOR*

## Sažetak

Osiguravajuća društva kao specifične financijske institucije pružaju ekonomsku zaštitu od rizika koji mogu pogoditi pojedince ili imovinu. Osim sklapanja ugovora o osiguranju i likvidacije šteta koje su nastale, važni su institucionalni investitori koji ulažu značajna sredstva na financijskom tržištu. Stoga svi prihodi i rashodi koji nastaju takvim aktivnostima utiču na njihov stupanj uspješnosti poslovanja.

U osiguranju digitalizacija predstavlja proces koji uvodi nove elemente i mogućnosti za proširenje portfelja usluga osiguranja, a time i nove mogućnosti za povećanje profitabilnosti.

Dakle, upotreba suvremenih tehnologija vodi ka transformiranju u poslovni model, koji je u potpunosti usmjeren potrebama korisnika/osiguranika. Tu su i mogućnost trajnog prisustva na tržištu, što služi za prepoznavanje i realizaciju poslovnih prilika.

Prateći razvoj umjetne inteligencije (AI) i ulaganja u informacione tehnologije (IT), te sve brojniju ponudu mobilnih usluga, osiguravatelji na domaćem tržištu nastoje da prate globalne trendove i zahtjeve osiguranika.

Police se danas kupuju putem mobilnih aplikacija, osiguravatelji prikupljaju podatke o potencijalnim klijentima preko društvenih mreža, a uz napredne analize koje su moguće putem AI, može se predvidjeti želje i potrebe sadašnjih i potencijalnih klijenata, ponuditi proizvod koji im najviše odgovara u određenom momentu i to jednostavno i efikasno.

Velike svjetske osiguravajuće kompanije prepoznale su nove mogućnosti AI – od povećanja prodaje do prostora za uštede u poslovanju. Dok su ranije osiguravatelji bili usmjereni na zaključivanje što većeg broja ugovora o osiguranju tj. pridobiti što veći broj osiguranika, sada je naglašena potreba da se obrati pažnja na već postojeće klijente i njihove zahtjeve.

* Evropski pokret Banja Luka, Slavka Rodića 2b, 78000 Banja Luka

AI i IT sistem omogućava osiguravajućim društvima da smanje operativne troškove, zadrže klijente i povećaju efikasnost procesa. AI i IT rješenje pruža optimizaciju procesa, poboljšanje – personalizaciju usluge, jačanje distribucije i platformu za razvoj novih proizvoda.

Digitalni trendovi ukazuju da IT sistem jednog društva za osiguranje treba da uključi i sistem za upravljanje odnosima sa klijentima (CRM), sistem poslovnog izvještavanja (BI), te sisteme za predviđanje trendova, naprednu analitiku i sl.

**Ključne riječi:** umjetna inteligencija, digitalizacija, obrada šteta, sistem za upravljanje odnosima s klijentima (CRM), sistem poslovnog izvještavanja (BI).

## Abstract

Insurance companies as specific financial institutions provide economic protection against risks that may affect individuals or property. In addition to concluding insurance contracts and liquidating damages, institutional investors who invest significant funds in the financial market are important. Therefore, all income and expenses arising from such activities affect their level of business success.

In insurance, digitalization represents a process that introduces new elements and opportunities for expanding the portfolio of insurance services, and thus new opportunities for increasing profitability.

Therefore, the use of modern technologies leads to a transformation into a business model, which is completely focused on the needs of beneficiaries/insureds. There is also the possibility of a permanent presence on the market, which serves to recognize and realize business opportunities.

Following the development of artificial intelligence (AI) and investments in information technology (IT), as well as the increasingly high supply of mobile services, insurers on the domestic market strive to follow global trends and the demands of policyholders.

Today, policies are purchased through mobile applications, insurers collect data on potential clients through social networks, and with advanced analyses that are possible through AI, it is possible to predict the wishes and needs of current and potential clients, offer the product that best suits them at a certain moment and simple and effective.

Large global insurance companies have recognized the new possibilities of AI – from increasing sales to generating savings in business. While earlier insurers were focused on concluding as many insurance contracts as possible, i.e. the greater the number of insured persons the better, the need to pay attention to existing clients and their requests is now emphasized.

The AI and IT system enables insurance companies to reduce operating costs, retain customers and increase process efficiency. AI and IT solutions provide process optimization, improvement – personalization of service, strengthening of distribution and platform for development of new products.

Digital trends indicate that the IT system of an insurance company should include a customer relationship management system (CRM), a business reporting system (BI), and systems for forecasting trends, advanced analytics, etc.

**Keywords:** artificial intelligence, digitalization, claims processing, customer relationship management system (CRM), business reporting system (BI).

## Uvod

Kako u posljednjih pet godina digitalizacija i automatizacija u sektoru osiguranja uzimaju zamah, s eksponencijalnim povećanjem u 2020. godini, javila se nova vrsta klijenata; osiguranici koji su digitalno osviješteni i naviknuti na brojne pogodnosti, brzinu i permanentnu dostupnost alata digitalnog svijeta. Radi se o osiguranicima koji uslugu traže sada 24/7/365, koji su konstantno na mreži ili *online*, bilo kada, bilo gdje i imaju pristup svom osiguravatelju i proizvodu osiguranja.

Tako iz istraživanja Deloittea iz lipnja 2022. Cybersecurity in Insurance – Thematic Research Global Data (globaldata.com) proizlazi da 95% osiguravatelja konstatira da su usredsređeni na ubrzavanje svojih inicijativa za digitalnu transformaciju. Taj fokus je uglavnom na upravljanju štetama koje će, prema Deloitteu, biti novo područje za transformaciju, diferencijaciju i, glavni segment, za automatizaciju. Uzimajući u obzir da su tipične stope direktne obrade manje od 10%, u potpunosti je razumljivo da osiguravatelji moraju koristiti tehnologije koje mogu značajno povećati točnost podataka i pomoći u postavljanju tzv. čistih potraživanja.

## Umjetna inteligencija

Umjetna inteligencija (engl. Artificial Intelligence, AI) nije samo novi tehnološki trend, već predstavlja revoluciju koja temeljito mijenja prirodu poslovanja. Od malih startup poduzeća do globalnih korporacija, AI transformira svaki segment industrije, omogućavajući kompanijama automatizaciju kompleksnih procesa, povećanje efikasnosti i otkrivanje novih mogućnosti za rast. Uz sposobnost analize ogromne količine podataka brže i preciznije od ljudi, umjetna inteligencija otvara vrata inovacijama koje su prije bile nezamislive. Organizacije sada mogu predvidjeti tržišne trendove, personalizirati korisničko iskustvo na temelju stvarnog ponašanja potrošača i donositi informirane odluke u stvarnom vremenu. Umjetna inteligencija danas nije samo alat za

poboljšanje poslovnih procesa, ona je ključni pokretač koji nanovo definira način poslovanja, donošenja odluka i komunikacije s korisnicima.

Umjetna inteligencija obuhvaća veliki broj područja djelovanja, svako s posebnim fokusom i primjenama. Jedno od njih je prediktivna analitika, prirodna evolucija pametne analitike nad podacima, koja organizacijama omogućava da iz sakupljenih ranijih podataka imaju uvide i predviđanja za buduće odluke. AI postavlja nove standarde u donošenju informiranih odluka. Obrada prirodnog jezika (NLP) poboljšava način na koji računala interpretiraju i razumiju ljudski jezik, omogućujući automatizaciju korisničke službe i analizu velikih količina tekstualnih podataka. Obrada govora, uključujući tehnologije sinteze govora (engl. Text-to-Speech, TTS) i transkripcije govora (engl. Speech-to-Text, STT), omogućava fluidnu govornu komunikaciju između ljudi i računala, proširujući granice interakcije u audio sferu. Računalni vid (engl. computer vision), s druge strane, daje računalima sposobnost vida, omogućavajući im da kroz procese detekcije i klasifikacije objekata analiziraju i identificiraju objekte, slike i scene u stvarnom svijetu.

## Prediktivna analitika

Kao jedan od važnih segmenata umjetne inteligencije, prediktivna analitika predstavlja osnov za informirano donošenje odluka unutar svakog poslovnog modela. Putem naprednih algoritama i strojnim učenjem, prediktivna analitika analizira historijske i trenutne podatke s ciljem uočavanja uzorka i predviđanja budućih događaja i trendova. Ovom karakteristikom transformira se način na koji kompanije pristupaju planiranju, od marketinga do upravljanja rizicima.

U financijskom sektoru, prediktivna analitika omogućuje bankama, osiguravateljima i drugim financijskim institucijama da procjenjuju kreditni rizik, optimiziraju portfelje i predviđaju tržišne pokrete, čime se povećava profitabilnost i smanjuje izloženost riziku. U području osiguranja, koristi se za personalizaciju ponuda i premija, predviđanje vjerojatnosti i troškova šteta te za unaprjeđenje strategija upravljanja rizicima.

Osim toga, prediktivna analitika nalazi primjenu u operativnom planiranju i lancima opskrbe, gdje pomaže u optimizaciji zaliha i predviđanju potražnje, omogućavajući tvrtkama smanjenje troškova i povećanje efikasnosti. U marketingu se koristi za segmentaciju korisnika, personalizaciju komunikacije i optimizaciju kampanja, što dovodi do povećanja konverzija i zadovoljstva klijenata.

Kroz primjenu prediktivne analitike, organizacije ne samo da mogu bolje razumjeti i predvidjeti tržišne uvjete i ponašanje korisnika, već i proaktivno djelovati, prilagođavajući svoje strategije za ostvarivanje konkurentske prednosti. Prediktivna analitika služi kao most između podataka i strateškog donošenja odluka, čineći je nezamjenjivim alatom u poslovanju svake uspješne kompanije.

## Obrada prirodnog jezika

Obrada prirodnog jezika (engl. *Natural Language Processing*, NLP) područje je umjetne inteligencije koje strojevima omogućava razumijevanje, interpretaciju i generiranje ljudskih jezika. Uz pomoć tehnika strojnog i dubokog učenja, NLP povezuje ljudsku komunikaciju s računalnom interpretacijom, čime se računalima omogućuje da analiziraju tekst te razumiju značenje i kontekst, premošćujući tako razliku između ljudskog jezika i digitalnog procesiranja informacija.

Poslovne primjene obrade prirodnog jezika vrlo su široke. U korisničkim službama NLP se koristi za izradnju chatbotova, odnosno virtualnih asistenata, koji vode smislene razgovore s korisnicima, rješavajući upite i pružajući podršku bez potrebe za ljudskom intervencijom, uz stalnu dostupnost i konzistentnost. Obrada prirodnog jezika znatno olakšava i analizu velikih količina dokumenata, identificirajući relevantne informacije i trendove koji bi ručno zahtijevali stotine sati rada. Na nedavno održanim Hrvatskim danima osiguranja u Opatiji istaknute su složene i brze promjene u svim segmentima industrije osiguranja, a predstavnik jednog osiguravatelja je naznačio da oni već koriste Chat GPT u podršci korisnicima.

U marketingu ovaj alat se koristi za analizu sentimenta i raspoloženja korisnika koji imaju profile na društvenim mrežama, portalima i drugim platformama, pružajući kompanijama dragocjene uvide u percepciju brenda i potrošačko ponašanje, prije ili nakon plasiranja proizvoda ili usluge na tržište. Osim toga, NLP olakšava automatsko sažimanje i prevođenje teksta te generiranje izvještaja, omogućavajući brzu analizu i distribuciju informacija unutar organizacija. Prednosti ovakvih poslovnih primjena pogotovo su izražene u današnje vrijeme generativnog AI-ja.

Kroz svoje sposobnosti, NLP ne samo da poboljšava efikasnost i smanjuje troškove poslovanja već također omogućava stvaranje novih proizvoda i usluga koje poboljšavaju korisničko iskustvo i zadovoljstvo. U eri digitalizacije, gdje se količina podataka neprestano i rapidno povećava, NLP predstavlja ključni alat za pretvaranje neobrađenog teksta u vrijedne uvide, čineći ga nezamjenjivim dijelom poslovne strategije.

AI kao alat za poboljšanje efikasnosti ili redukciju troškova, predstavlja i osnovu za kreiranje budućnosti poslovanja, pruža donošenje boljih odluka, shvaćanje potreba korisnika i u tom smislu generiranje usluga. Bez obzira što donosi brojne izazove, AI pruža i mnoge prilike za rast i razvoj.

Povećana preciznost i točnost izračuna premije putem umjetne inteligencije smanjuje rizik, što dovodi do potencijalnog smanjenja troškova za osiguravajuća društva i samim tim i osiguranike kroz nižu cijenu usluge osiguranja.

Ovo je značajno jer osiguravatelji mogu pojednostaviti poslovanje i prenijeti ove uštede na klijente kroz niže premije. Preciznost analiza umjetne

inteligencije dramatično umanjuje vjerojatnost rizika od pretjerane ili preniske cijene. Osiguranici tada plaćaju stopu koja odgovara stvarnoj razini rizika.

Primjena AI utiče i na segmentaciju kupaca, stvarajući personalizirane proizvode osiguranja prilagođene individualnim potrebama. Ova se personalizacija događa analizom detaljnih podatkovnih točaka, što osiguravateljima pruža razumijevanje različitih grupa klijenata i ponudu proizvoda koji točnije odgovaraju različitim stilovima života i profilima rizika.

Dolazi do automatizacije rutinskih zadatka i analiza, npr. unosa podataka i obrade zahtjeva, čime se utiče na ekspeditivnije obavljanje operacija i smanjuje mogućnost ljudske pogreške. Rezultat je brža usluga i pouzdanije pokriće osiguranja jer umjetna inteligencija pomaže tvrtkama u upravljanju policama i potraživanjima vrlo precizno i učinkovito.

## Kibernetička sigurnost tržišta osiguranja

Globalni prihod od kibernetičke sigurnosti u sektoru osiguranja iznosio je 6,4 milijarde USD u 2020. godini. Očekuje se da će tržište rasti uz složenu godišnju stopu rasta (CAGR) više od 10% od 2020. do 2025. godine. Brza digitalna transformacija sektora utiče na ovaj rast.

COVID-19 doveo je do toga da više klijenata digitalno pristupa svojim računima, a osiguravatelji prodaju putem digitalnih kanala, povećavajući kibernetički rizik sektora. Porast složenih *ransomware* napada, postojanost hibridnih radnih modela, stalne prijetnje opskrbnom lancu i rat između Rusije i Ukrajine ubrzali su potrebu za snažnom kibernetičko-sigurnosnom obranom u svim sektorima.

## Kibernetička sigurnost u osiguranju

Današnji korisnici osiguranja, od kojih su mnogi pripadnici generacije Z, navikli su svojim osiguravateljima pristupati putem digitalnih kanala. To povećava prostor za kibernetičke napade, slično digitalizaciji koju je iznudila pandemija COVID-19 koja je zahvatila i ostavila posljedice na brojne industrije i poslovanja kompanija. Povećani rizik od kibernetičkog napada i isplata za vlasnika police kibernetičkog osiguranja obeshrabruju osiguravatelje da ponude kibernetičke police. Štoviše, ekonomska šteta od pandemije i stalna kriza troškova života dodatno su smanjili mogućnosti poduzeća i potrošača da si priušte sve skuplje *cyber* osiguranje.

Pandemija COVID-19 ubrzala je digitalnu transformaciju poduzeća, zahtijevajući da više zaposlenika radi na daljinu i da se više transakcija obavlja online. Uz sve više klijenata koji digitalno pristupaju svojim računima i osiguravatelja koji prodaju putem digitalnih kanala više nego prije, *cyber* rizik s kojim se osiguravatelji suočavaju raste. Ovo je posebno važno za tradicionalne

osiguravatelje, koji obično imaju manje digitalnog iskustva i stručnosti od osiguravatelja specijaliziranih za visoko tehnološke rizike.

Digitalni izazovi u industriji osiguranja u početku su bili naročito prisutni u osobnim linijama, dok su druga područja osiguranja ostala nepromijenjena. To je sada drugačije, a na većinu proizvoda osiguranja utjecali su izazovi u nastajanju koji su ubrzali digitalnu transformaciju u sektoru. Ova brza digitalna transformacija, međutim, riskira da ostanu praznine u razvoju aplikacija. Uz zaštitu svog ugleda i izbjegavanje velikih kazni, osiguravatelji bi trebali ulagati u rješenja za kibernetičku sigurnost kako bi spriječili narušavanje sigurnosti podataka.

Porast kibernetičkih aktivnosti i napada (sponzoriranih od strane države) predstavlja ozbiljnu prijetnju kibernetičkoj sigurnosti na globalnoj razini. Postoji vrlo realna opasnost da se mogućnosti koje nudi Gen AI i LLM iskoriste, osobito u području dezinformacija i informacijskog rata za potkopavanje demokracije. Potencijalni društveni, ekonomski i geopolitički učinak mogao bi biti golem, jer granice između fizičkog i virtualnog svijeta, te između istine i laži, postaju sve manje i nejasnije.

Glavni fokus zlonamjernih napada vjerojatno će biti ometanje izbora na propagandistički i manipulativan način, te bacanje sumnje na njihov integritet. Glavni izbori 2024. bit će predsjednički izbori u SAD-u. Međutim, više od 40 drugih država raspisaće izbore, što znači više od 4 milijarde birača s pravom glasa diljem svijeta, uključujući EU, Indiju, Južnu Koreju, Indoneziju i Meksiko. Suprotstavljanje dezinformacijama i razotkrivanje lažnog sadržaja predstavlja izazov za svaku demokraciju, kao i zaštita izbornog procesa sa svim njegovim digitalnim komponentama.

Uz dezinformacije (namjerno stvaranje lažnog sadržaja ili manipulacije), zlonamjerne informacije (namjerno objavljivanje štetnih podataka ili privatnih informacija) postat će skupa prijetnja vlasnicima rizika: do 2028. godine korporativna potrošnja na suzbijanje zloćudnih informacija premašit će 30 milijardi USD, što će potrošiti 10 % proračuna za kibernetičku sigurnost i marketing kako to pojašnjava istraživački tim kompanije Gartner.

Aktivnosti država vjerojatno će se proširiti izvan sofisticiranih dezinformacija i utjecaja na izbore te obuhvatiti gospodarsku, vojnu i političku špijunažu. U nekim slučajevima vlasti država aktivno podupiru ili barem toleriraju kibernetičke kriminalce. Arsenali država rastu i sada obično uključuju kao standard destruktivne wiper napade dizajnirane za trajno brisanje ili oštećenje podataka na sustavima.

Zbog sve većeg globalnog natjecanja i velikog oslanjanja na svemirsku, satelitsku i komunikacijsku sigurnost, ovaj će sektor biti ključni čimbenik u svim razmatranjima kibernetičke sigurnosti – i za države i za velike komercijalne satelitske operatere. Ne iznenađuje da se 95% donositelja odluka u obrani i zrakoplovstvu slaže da je tekuća digitalizacija dovela do dinamičnijeg i složenijeg bojnog polja (BAE Systems).

## Glavni uzročnici gubitaka u kibernetičkom osiguranju

Kao primjer mogu poslužiti podaci i iskustvo tvrtke Munich Re o gubicima koji daju jasnu sliku kibernetičkih rizika i njihovog utjecaja na kibernetičko osiguranje. To posebno vrijedi za ransomware, kompromitaciju poslovne e-pošte i kompromitaciju poslovne komunikacije, povrede podataka i ranjivosti lanca opskrbe.

### *Ransomware*

Smatra se da će ransomware i dalje biti dominantan pokretač rizika i gubitaka za cyber osiguranje. Napredak u primijenjenom tehnološkom napretku i taktikama ukazuje na složenije i štetnije okruženje ransomwarea, gdje će sve više i jače grupe ransomwarea skratiti svoje vrijeme zadržavanja, uključujući korištenjem taktike brzog ubacivanja.

Modeli Ransomware-as-a-Service (RaaS) postat će još konkurentniji na tržištima dark weba, dijelom zato što ih AI može pokretati ili poboljšati. AI će potaknuti visok stupanj automatizacije u procesima hakiranja i dovesti do snažne individualizacije napada – s prilagođenim phishingom ili iznuđivanjem e-pošte koje AI može lako prevesti na više jezika u visokoj kvaliteti i tako skalirati u mnogim regijama istovremeno.

Stručnjaci Munich Re također očekuju daljnju diverzifikaciju metoda iznude izvan enkripcije, nastavljajući već uočeni pomak s fokusa na podatke za iznudu prema podacima koji se mogu iskoristiti za prodaju, potencijalno ciljajući na zaposlenike, dobavljače, klijente i druge zainteresirane strane.

Tim za analizu cyber podataka Munich Re primijetio je da je ransomware daleko vodeći uzrok gubitaka u cyber osiguranju. Proizvodnja je identificirana kao industrija s najvećim brojem zahtjeva za ransomware.

### *Kompromitiranje poslovne e-pošte (BEC) i kompromitiranje poslovne komunikacije (BCC)*

Od 2024. godine i narednih, stručnjaci Munich Rea predviđaju nagli porast BCC i BEC napada. Oni će prevariti ljude unutar tvrtki i navesti ih da izvrše štetne radnje, kao što su neovlaštena plaćanja ili dijeljenje osjetljivih podataka prema onima izvan kompanije. Budući da prevaranti nastoje postići svoj cilj na relativno lak način, BEC ostaje glavni vektor napada, posebno zato što ga je lako izvesti i ne zahtijeva praktički nikakvo tehničko znanje, a ima vrlo visoke rezultate. Ne koristi se samo e-pošta kao pristupnik, već i sve komunikacijske platforme i kanali društvenih medija. BEC i BCC napadi pored velikih financijskih gubitaka, dovode i do erozije povjerenja i štete ugledu tvrtki.

Primjeri uključuju napade pod krinkom izvršnih direktora, gdje se hakeri predstavljaju kao rukovoditelji i daju upute zaposlenicima da prebace novac. Budući da su alati umjetne inteligencije i tehnologije *deepfake* postali dio alata

*mainstream* kriminalaca, uvjerljivi lažni telefonski pozivi ili digitalni sastanci, kao i videozapisi, široko su i ekonomično dostupni za prijevare.

Početkom 2024. godine zaposlenik multinacionalne tvrtke sa sjedištem u Hong Kongu prebacio je gotovo 26 milijuna dolara prevarantima nakon što je prisustvovao videopozivu s *deepfakeovima* svojih suradnika, uključujući financijskog direktora tvrtke. Zaposlenik je bio jedino ljudsko biće koje je prisustvovalo video pozivu, dok su lažne sudionike oponašali pomoću tehnologije vođene umjetnom inteligencijom.

### *Povrede podataka*

Do kraja 2024. godine propisi o privatnosti pokrivat će tri četvrtine potrošačkih podataka u cijelom svijetu, ali 60% svih reguliranih globalnih subjekata borit će se uskladiti sa sve intenzivnijim propisima o zaštiti podataka i zahtjevima za privatnošću, s obzirom na visoke stope rasta podataka potaknute tehnologija. 5G će i dalje biti pokretačka snaga rasta mobilnih podataka: do 2029. godine udio 5G u mobilnom podatkovnom prometu porast će na 76%. Videopromet činit će većinu mobilnih podataka, eskalirajući s trenutno malo iznad 70% ukupnog mobilnog podatkovnog prometa na 80% do 2029. godine (Ericsson).

Usred svih tehnoloških razvoja, jedan čimbenik ne treba zaboraviti kada se raspravlja o povredama podataka ili drugim kibernetičkim incidentima: vrijednost i kritičnost podataka, zajedno s regulacijom podataka i temeljnim pitanjima u vezi s odgovornošću, dodatno će potaknuti pojavu više grupa koje nude hakiranje – usluge iznajmljivanja i krađe podataka.

Unatoč tome, čak i najnaprednije povrede podataka s phishingom poboljšanim AI i dalje će uključivati ljudski element u približno 90% slučajeva (Forrester). Višestrani napori za stvaranje svijesti i provedbu odgovarajuće obrane koja nadilazi tehnologiju jesu i bit će nužni.

### *Ranjivosti lanca opskrbe*

Ovisnost o lancima opskrbe softvera i hardvera te digitalnim uslugama nastavit će se i biće u velikom porastu u narednom razdoblju. Kao očigledna slabost većine organizacija, opskrbni lanac ima za posljedicu da konstantno privlači napadače. Eksperti Munich Re očekuju da će se hakiranja preko mreža dobavljača, proizvođača i pružatelja usluga unutar digitalnih opskrbnih lanaca (IT/OT/IoT) dodatno povećati. Organizacije će također svjedočiti većem broju „napada na lanac opskrbe kao usluge“, otvarajući ovo polje drugim hakerskim grupama manje upućenim u tehnologiju.

Prema studiji Svjetskog ekonomskog foruma (WEF 2024.), 41% anketiranih tvrtki bilo je pogođeno cyber incidentom treće strane. Male i srednje velike dobavljače sve više napadaju s ciljem kasnijeg hakiranja sustava njihovih većih kupaca. Procjenjuje se da će očekivani porast troškova poduzeća na globalnoj

razini zbog napada na lanac opskrbe softverom porasti sa 46 milijardi USD 2023. godine na 60 milijardi USD 2025. godine (Juniper Research).

## Temelji cyber osiguranja

U razdoblju od jednog desetljeća, cyber osiguranje postalo je ključna i važna komponenta upravljanja cyber rizicima za organizacije i kućanstva. U ekstremno dinamičnom krajoliku prijetnji, gdje geopolitički i tehnološki faktori stresa postavljaju nove prioritete, suočavanje s izazovima osiguranja i upravljanje akumulacijskim rizikom ključni su za dugoročnu održivost i funkcionalnost tržišta koje i dalje sazrijeva. Osiguravatelji i upravljači rizika nastavljaju istraživati granice i mogućnosti osiguranja. Nužan je razborit daljnji razvoj tržišta, s očekivanom budućom globalnom potražnjom koja zahtijeva dovoljan kapacitet osiguranja i alternativnih tržišta kapitala.

Cyber rizikom mora se pravilno i zajednički upravljati. To također vrijedi za one rizike kojima privatni sektor ne može upravljati, ili barem ne u potpunosti.

Osiguravatelji danas ulažu u inicijative i resurse koji produbljuju svoje vlastito i industrijsko razumijevanje ukupne cyber izloženosti i dodatno unapređuju modeliranje rizika. Potreba za robusnim modeliranjem akumulacije prožima sve aktivnosti preuzimanja rizika i upravljanja rizicima.

Tako glavni preuzimač cyber rizika u jednom europskom osiguranju, Jürgen Reinhart, smatra djelovanje u tom smjeru važnom misijom koja je ključna za uspješno gospodarstvo: raditi s klijentima, partnerima i brokerima kako bi se pružila učinkovita rješenja za cyber osiguranje koja štite digitalno okruženje i čine ga otpornijim. Osiguravanje primjerenih modela cyber akumulacije potrebnih za profitabilno, održivo tržište cyber osiguranja ključni je izazov za industriju osiguranja. Svi učesnici na tržištu nastavljaju težiti izvrsnosti u vlastitom modeliranju i poduprijeti inicijative koje unapređuju modeliranje u cijeloj industriji.

Oni aktivno surađuju s dionicima u industriji o različitim aspektima u vezi s modeliranjem akumulacije, s ciljem pomirenja razlika u percepciji rizika i osiguravanja sve bolje pouzdanosti modela na cijelom tržištu. Na primjer, njihovi stručnjaci surađuju s pružateljima podataka trećih strana, pružateljima usluga i dobavljačima modela kako bi poboljšali kvalitetu i kvantitetu podataka, bolje razumjeli rizike, razvili kvantifikaciju rizika i dodatno unaprijedili modeliranje.

Sofisticirani modeli kibernetičke akumulacije koji odgovaraju svrsi ključni su za osiguravanje profitabilnog, održivog tržišta kibernetičkog osiguranja, što je izazov s kojim se suočava cijela industrija. Jasnoća u vezi s granicama osiguranja preduvjet je za pouzdanost modela. Ako se želi osigurati dugoročna održivost tržišta kibernetičkog osiguranja, tada moraju postojati nužna isključenja, posebno u pogledu kibernetičkog rata.

Cyber osiguranje je nedvojbeno umnogome pomoglo u izgradnji učinkovitog sloja otpornosti. Međutim, sposobnost industrije osiguranja za nošenje

rizika ima prirodna ograničenja. Šteta od katastrofalnih sustavnih događaja poput cyber rata ili ispada kritične infrastrukture daleko bi premašila kapacitet industrije. Takvi scenariji predstavljaju prijetnju makroekonomskoj stabilnosti zbog čega je društvima potrebna uključenost vlada u upravljanju ovim potencijalno katastrofalnim kibernetičkim rizicima. Osiguravatelji i reosiguravatelji mogu i žele podržati razvoj rješenja i jasno se zalažu za provedbu ekonomske kibernetičke zaštite kao posljednje mjere opreza. Dijalozi i pregovori o takozvanim „državnim potporama" već se odvijaju.

Rizici koje predstavlja digitalizacija su izazov za društvo u cjelini. Industrija osiguranja igra svoju ulogu u ublažavanju tih rizika. Međutim, najteže sistemske kibernetičke rizike, poput kvara kritične infrastrukture ili štete od kibernetičkog ratovanja, ne može snositi privatni sektor. Osiguravatelji nastoje pomoći vladama da zajednički upravljaju ovim potencijalno katastrofalnim, sistemskim rizicima za društva, tražeći alternativna rješenja.

## Trendovi tržišta cyber osiguranja

Globalno tržište cyber osiguranja doseglo je veličinu od 14 milijardi USD u 2023. godini, a Munich Re procjenjuje da će se povećati na oko 29 milijardi USD do 2027. godine. S obzirom na trend rasta, na tržištu je primjetan sve veći broj i sve veća složenost cyber napada. To povlači određene financijske reperkusije i striktnije zahtjeve regulatora. Npr. Direktiva o mrežnoj i informacijskoj sigurnosti (NIS2) koja stupa na snagu u posljednjem kvartalu ove godine.

Cilj NIS2 je jačanje europske kibernetičke sigurnosti i otpornosti. Kako su za dalji rast neophodni i stalna digitalna transformacija, a tako i tehnološki napredak u svim sektorima, postoje specifični zahtjevi koje moraju ispuniti poslovni partneri koji se nalaze u okviru lanca opskrbe. Sve gore navedeno upućuje koliko je kibernetičko osiguranje bitno kao i komponente upravljanja rizikom kibernetičke sigurnosti.

Prema jednoj grupi autora samo posljednjih pet godina tržište cyber osiguranja bilježi gotovo trostruki rast. To može značiti da postoji veliki interes reosiguratelja kao i interes na tržištima kapitala za kibernetičke rizike uopće. Ostaje činjenica da je trenutačno osiguran samo dio rizika. Velika poduzeća i dalje drže većinu premija, dok mala i srednja poduzeća veliki dio kibernetičkih rizika preuzimaju na sebe.

Pred osiguravateljima je glavni izazov da ne postoji ogroman nesklad između ekonomskih i osiguranih gubitaka. S obzirom na vrlo dinamičan rast rizika u digitaliziranom gospodarstvu, najveći je cilj veći prodor osiguranja za cyber rizike. Pomažući u zaštiti digitalnog svijeta, osiguravatelji će još jednom pokazati važnost industrije za otpornost gospodarstva i društva. Industrija osiguranja nudi niz atraktivnih rješenja koja su djelotvorna u pridobijanju

neosiguranih i sklapanju novih ugovora. U isto vrijeme, fokus je na uvjeravanju da je osiguranje dostatno i da se bazira na održivoj mjeri.

## Ključni lanci vrijednosti kibernetičke sigurnosti

Lanci vrijednosti u smislu kibernetičke sigurnosti odnose se na tri segmenta: *hardware*, *software*, i usluge.

### *Hardware*

Sa čipovima koji se sada koriste u serverima koji su bitni u aplikacijama kritičnim za sigurnost, zaštita čipova od sajber napada postaje sve važnija i skuplja. Kompanije koje nude te sisteme kao što su npr. Apple i Amazon sve više dizajniraju svoje čipove umjesto da kupuju komercijalno razvijene uređaje i intelektualno vlasništvo (IP) koje su kreirali programeri trećih strana.

### *Software*

Softverski element lanca vrijednosti kibernetičke sigurnosti sastoji se od sljedećih područja: upravljanje identitetom, sigurnost mreže, sigurnost krajnjih tačaka, otkrivanje prijetnji i odgovor, cloud sigurnost, sigurnost podataka, sigurnost e-pošte, sigurnost aplikacija, objedinjeno upravljanje prijetnjama i upravljanje ranjivostima.

### *Usluge*

Element usluga lanca vrijednosti kibernetičke sigurnosti sastoji se od područja: upravljane sigurnosne usluge, usluge odgovora nakon kršenja i usluge rizika i usklađenosti. Usluge se obično povjeravaju vanjskim izvršiteljima zbog složenosti rješavanja pitanja vezanih za sajber sigurnost, kao što je praćenje ranjivosti, prepoznavanje i reagiranje na prijetnje i ispunjavanje zahtjeva za usklađenost.

Vodeće kompanije u oblasti cyber sigurnosti su: AIG, Allianz, Aon, Chubb, Hiscox, Marsh, Munich Re, Ping An, Swiss Re, and Zurich Insurance.

Dok su specijalizirani dobavljači sajber sigurnosti na tržištu osiguranja: Blackberry, CyberCube, FireEye, Portnox, and SecurityScorecard.

**Tabela 1. Pregled tržišta**

| **Veličina tržišta (2020. godina)** | **6,4 milijarde USD** |
|---|---|
| Složena godišnja stopa rasta CAGR (2022. – 2025. godine) | >10% |
| Ključni lanci vrijednosti | Hardware, software, usluge |
| Vodeći osiguravatelji | AIG, Allianz, Aon, Chubb, Hiscox, Marsh, Munich Re, Ping An, Swiss Re i Zurich Insurance |
| Specijalizirani dobavljači kibernetičke sigurnosti | Blackberry, CyberCube, FireEye, Portnox i SecurityScorecard |

Uz povećanu digitalizaciju, sve osiguravajuće tvrtke sada moraju dati prioritet kibernetičkoj sigurnosti.

COVID-19 prisilio je tvrtke na brzu digitalizaciju, ostavljajući više otvorenog prostora za kibernetičke napade.

U 2019. godini globalni prihodi od sigurnosti u industriji osiguranja iznosili su 5 milijardi dolara. Do 2024. godine ta će brojka dosegnuti 6,4 milijarde USD.

Pozicioniranje za uspjeh pretpostavlja razumijevanje kako kibernetička sigurnost – jednu od najvećih tema desetljeća – treba primijeniti unutar sektora osiguranja za ublažavanje izazova brze digitalizacije.

Već postoje vodeći i specijalizirani dobavljači tehnologija kibernetičke sigurnosti za sektor osiguranja. Potrebno je brzo reagirati i identificirati atraktivne portfelje ulaganja u industriji osiguranja tako što će se pratiti informacije koje će kompanije najvjerojatnije biti pobjednici u budućnosti na temelju tzv. tematskih tablica rezultata.

Konkurentska prednost u industriji osiguranja se postiže razumijevanjem vrijednosti kibernetičko-sigurnosnih rješenja za svaki segment vrijednosnog lanca osiguranja.

## Podaci i upotreba novih izvora informacija za preoblikovanje pojma rizika

Podaci mogu transformirati industriju osiguranja na dva načina: mogu pružiti nove izvore uvida za pojednostavljenje i pojednostavljenje postojećeg osiguranja, i mogu poboljšati razumijevanje rizika kako bi omogućili preciznije kategorizacije rizika.

Mnoge kompanije započele su svoje programe za inovacije automatizacijom postojećih skupova pravila kako bi donijele manje složene politike. Zatim su prešli na inkorporiranje eksternih izvora podataka, od kojih se neki danas široko koriste. Na primjer, anamneza na recept se sada koristi kao input za osiguranje za više od 90 posto polica životnog osiguranja. U SAD-u rezultati osiguranja zasnovani na kreditu pokazali su se kao dobri za predviđanje mortaliteta i propusta u policama, a nekoliko kompanija za reosiguranje su u partnerstvu sa kreditnim agencijama da riješe pitanje bodovanja. TransUnion, u tom smislu, nudi TrueRisk rezultat, koji je potvrdila Reinsurance Group of America.

Novi podaci također su omogućili preciznije razumijevanje rizika. Tako se izgledi smrtnosti mogu smisleno formirati putem faktora kao što su dobrotvorne akcije, vlasništvo kućnih ljubimaca, fitnes protokoli i niz drugih pokazatelja ponašanja. Gledajući unaprijed, osiguravatelji bi mogli razmotriti brojne obećavajuće nove digitalne izvore zdravstvenih podataka, u rasponu od elektroničkih medicinskih zapisa (sve češći unos za osiguranje) do novih i

inovativnih izvora poput telemedicine, koji se koriste za obavljanje razgovora i vizualno mjerenje tjelesne mase (BMI) podnositelja zahtjeva.

Osim korištenja novih izvora podataka, osiguravatelji imaju priliku ponovno osmisliti paradigmu koja je u osnovi današnjeg procesa preuzimanja rizika. Sadašnji proces prevodi informacije o dobi, spolu i korištenju duhana u relativno uzak skup kategorija ocjenjivanja—standard, standardni plus, preferirani i preferirani plus. Za podnositelje zahtjeva s akutnijim čimbenicima rizika, osiguravatelji vrše prilagodbe tablice za te kategorije, što može povećati premije za 300 posto ili više. Dok tvrtke kritički ispituju svoje osiguranje, mnogi su primijetili da da načelo 80/20 vrijedi: potrebno je mnogo manje informacija da bi se kandidati svrstali u trenutne kategorije ocjenjivanja, posebno kada se koriste novi podaci i analitičke tehnike. Ipak, industrija se nastavlja pridržavati statusa quo.

Neke su tvrtke zauzele čist pristup kako bi pojednostavile procjenu rizika, uključile nove izvore podataka i povećale primjenu tehnika vođenih umjetnom inteligencijom. To je dovelo do puno jednostavnijih obrazaca za prijavu (na primjer, skupovi pitanja smanjeni su za više od 70 posto), uklanjanja invazivnih zahtjeva za veći dio populacije i razlika u cijenama koje su niže od onih za potpuno osigurane proizvode.

Kako bi bili uspješni, osiguravatelji će morati prevladati napetosti između tradicionalnih aktuarskih modela i novijih tehnika znanosti o podacima. Ponekad se čini da su odluke mehaničkog učenja u suprotnosti s rezultatima tradicionalnih mehanizama za pravila. Neke su tvrtke izgradile jake analitičke modele, ali samo ih je nekoliko prešlo iz laboratorija na teren i prebacilo značajnu moć donošenja odluka na te modele. Kako bi prevladali ovaj izazov, aktuari i znanstvenici koji se bave podacima moraju se usuglasiti za koje je segmente model dovoljno jak da bi se pokrenuo. U isto vrijeme, tvrtke moraju prihvatiti određeni stupanj rizika i neizvjesnosti pri prelasku na novije modele.

Algoritamsko preuzimanje rizika sve će više biti preduvjet za ostanak i zadržavanje trenutnih pozicija na tržištu. A budući da je pandemija COVID-19 dodatno utjecala kao otežavajući faktor na zaključivanje ugovora o životnom osiguranju, mnogi osiguravatelji sve više shvaćaju da je transformacija osiguranja još hitnija. Ta činjenica predstavlja samo početak. Mnogi trenutni napori da se modernizira osiguranje digitalno omogućuju klasične proizvode. Današnji potrošači imaju drugačije sklonosti i potrebe nego što su imali prije nekoliko desetljeća, iako sadržaj polica životnog osiguranja ostaje uglavnom isti.

Pojednostavljeno osiguranje postavlja platformu za buduće inovacije u industriji. Omogućit će poboljšanje tehnika prikupljanja, uz pomoć nove tehnologije za prikupljanje i analizu biometrijskih podataka. Prodaja osiguravajućih proizvoda pomaknut će se s jednokratnih transakcija s malim angažmanom na trajni odnos između korisnika i osiguravatelja; ovaj će angažman biti definiran kontinuiranim preuzimanjem rizika i većim fokusom na zdravlje i

dobrobit. Segmentacija tržišta će sve više dosezati razinu pojedinaca, uz bolje razumijevanje svake osobe u skupini rizika. Potpomognuto ovim inovacijama, pojednostavljeno preuzimanje rizika prvi je temeljni korak koji će dovesti do šireg ponovnog otkrivanja koje industrija treba.

## Zaključak

Do sada je industrija osiguranja implementirala mnoge projekte koji se zasnivaju na upotrebi umjetne inteligencije. Primjena AI u osiguranju utiče na rast operativne izvrsnosti i efikasnost poslovanja. Uvođenjem AI postiže se brže i preciznije preuzimanje rizika i adekvatnije upravljanje odštetnim zahtjevima. Isto tako, AI pozitivno utiče na ispunjavanje obaveza predviđeno regulativnom, zakonskim i podzakonskim aktima, odnosno uvjetima koje postavlja regulator. Značajno je što je osiguranicima, u svakom momentu, na raspolaganju podrška.

U Srbiji Udruženje osiguravatelja koristi softver FROPS za strojno učenje u osiguranju. Sistem za detekciju prevara u osiguranju (FROPS) je korisnička platforma čija je namjena povezivanje sa svim vertikalnim izvorima informatičke infrastrukture i ostvarivanje objedinjenog pristupa, prikaza i obrade podataka. Sa tehnološkog pogleda platforma predstavlja organizacijski nivo informacija gdje se pohranjuje unifikacija svih struktura podataka kojima sustav raspolaže.

Funkcionalno platforma pruža efikasno pretraživanje, razumijevanje, ovladavanje i analizu velikih količina podataka. FROPS je osnova rješenjima kao što je eng. Advance Police Investigation Suite (APIS) čija je namjena istraga, koja uključuje sve postojeće izvore. Upotrebom ove platforma postiže se brz i efikasan pristup izvorima za potrebe istrage provođene, zasnovane na IBM L2 rješenju.

Izvori te informatičke infrastrukture su:

- baze podataka,
- *file* sustavi
- interna IT rješenja

Osnovni element sustava je zapravo entitet, dok objedinjeni pristup znači povezivanja i prikaz svih entiteta iz raspoloživih podataka koji se prikupljaju u sklopu Informacionog sistema Udruženja.

Jedan osiguravatelj u Hrvatskoj primjenjuje digitalno osiguranje LAQO i SPEKTAR program paketa za kućanstvo sa prvim automatiziranim 360° sustavom za procjenu šteta na motornim vozilima temeljen na umjetnoj inteligenciji. To je o složeni digitalni sustav koji povezuje rad rotacione 360° view mehaničke platforme, video opreme i kalkulacijskog sustava za detekciju oštećenja i kalkulaciju popravka. Ovaj sustav procjenu štete na vozilu obavlja za kratko vrijeme (oko tri minute) i bez popunjavanja papirologije.

Pored prednosti koje metode, tehnike i primjena AI omogućava industriji osiguranja, postoje i određena otvorena pitanja i izazovi. Koliko će sektor osiguranja uvoditi inovacije iz oblasti AI zavisi i spremnost upravljačkih struktura na optimizaciju i modernizaciju samog načina poslovanja pojedinih društava. Trenutna razina razvoja AI, i njenih sustava koji su dostupni odnosi se na vrlo specijalizirane vrste poslova i aktivnosti. Dakle, primjenjivih na ograničenu grupu zadaća npr. uparivanje složenih sustava mehaničke platforme, video opreme i softwarea za detekciju oštećenja te testiranje sustava u različitim uvjetima.

Budućnost umjetne inteligencije u obradi šteta ogleda se u razvoju rješenja za *remote* procjenu i detekciju oštećenja uz korištenje pametnih telefona ili srodnih uređaja te u dodatnom usavršavanju programa za prepoznavanje oštećenja i izradu kalkulacija popravka kod procjene i obrade šteta na motornim vozilima.

Biće potrebno nekoliko desetljeća da se razvije generalni sistem AI koji bi mogao imati različite uloge i aktivno rješavati brojne zadaće. Ono što predstoji osiguravateljima u tom smislu je da pažljivo prate razvoj novih tehnologija i postepeno vrše prilagodbe radnih procesa i IS-a kako bi se pripremili za kreiranje i uvođenje sveobuhvatnih virtuelnih sustava u dogledno vrijeme koji će voditi sve poslove u društvima za osiguranje.

Da bi transformacija bila učinkovita i uspješna neophodno je, pored uvođenja suvremenog IT sustava i alata AI, imati adekvatan model poslovanja koji uveliko nadilazi klasične forme.

AI je tehnologija koja preuzima pojedine sfere poslovanja u osiguranju i koja će promijeniti osnovne funkcije osiguranja i poduzeća.

Navedeni zahtjevi u oblastima transformacije poslovanja pokazuju da su podaci glavno pitanje i izazov u smislu inovacija. Podaci su bitni, a osiguravatelji imaju obavezu da izvrše odgovarajuću pripremu podataka koje će koristiti za svoje potrebe kao i potrebe regulatora i voditi se načelom usklađenosti u pogledu operativnih, reputacijskih, strateških i regulatornih rizika. Dobro izbalansirano rukovanje prilikama i rizicima preko operativnih modela zasnovanih na riziku će omogućiti da osiguravatelji posluju.

## Literatura


1. Chesbrough, H. W. (2007). Open innovation: the new imperative for creating and profiting from technology. Boston (Mass.): Harvard Business School Press.
2. Chesbrough, H. W. (2011). Everything You Need to Know About Open Innovation, http://www.forbes.com/sites/henrychesbrough/2011/03/21/everything-you-need-toknow-about-open-innovation/ [Accessed 25 March 2024]
3. Jednak, J. (2007) *Finansijska tržišta*. Beograd, Beogradska Poslovna Škola.
4. Lee, S., Park, G., Yoon, B., Park, J. (2010). Open innovation in SMEs — An intermediated network model. Research Policy, (39), str. 290–300.
5. Lukić, R. (2009) *Računovodstvo osiguravajućih kompanija*. Beograd, Centar za izdavačku delatnost Ekonomskog fakulteta.
6. Ostojić, S. (2007) *Osiguranje i upravljanje rizicima*. Beograd, Data Status.
7. Cybersecurity in Insurance – Thematic Research (globaldata.com) GlobalData. June 28, 2022. https://www.globaldata.com/store/report/cybersecurity-in-insurance-theme-analysis/
8. Cyber insurance for companies | Munich Re
9. Gartner: Three top trends in cyber security for 2024 | Computer Weekly
10. World Economic Forum 2018: New Physics of Financial Services
11. www.cea.eu
12. www.dani-osiguranja.huo.hr
13. www.insuranceeurope.eu
14. www.svijetosiguranja.eu
15. www.swissre.com