Marija Paunović[*]
Jelena Doganjić[**]

UDK 005.334:368
343.533::004

DOI: 10.5937/MegRev2201053P
Pregledni naučni članak
Primljen 15.04.2021.
Odobren 20.04.2021.

SAJBER OSIGURANJE I AKTUARSKA ANALIZA

Abstrakt. *Digitalna revolucija utiče na sve. Sajber rizik je prirodna posledica razvoja digitalnih tehnologija, koje izazivaju nastanak novih faktora od uticaja na ranjivost kompanija u različitim sektorima delatnosti. Sa porastom sajber pretnji, ugovori o osiguranju se pojavljuju kao značajan alat za poboljšanje otpornosti na uticaj ovih rizika. Sajber osiguranje je najbrže rastuća linija poslovanja osiguravača u modernoj istoriji. Cilj ovog rada je da prikaže osnovne aktuarske analize prilikom razvoja proizvoda sajber osiguranja.*

Ključne reči: *sajber osiguranje, premija osiguranja, rizici u sajber osiguranju, sajber kriminal*

[*] PhD, Fakultet za hotelijerstvo i turizam u Vrnjačkoj banji, Univerziteta u Kragujevcu, Srbija; majap@rcub.bg.ac.rs

[**] PhD, Milenijum osiguranje a.d.o, Beograd, Srbija; doganjic.jelena75@gmail.com

1. Uvod

Četvrta industrijska revolucija donosi brojne promene uključujući i veštačku inteligenciju (AI), mašinsko učenje, robotiku, Internet stvari (IoT), nanotehnologiju, 3D štampu. Nove tehnologije čine ljude i kompanije efikasnijim, ali nažalost, donose i razvoj sajber kriminala.

Sajber kriminalci brzo usvajaju nove tehnologije. Povećana internet aktivnost od strane mobilnih platformi je često praćena sajber kriminalom. Čak se i neke tehnike veštačke inteligencije koriste u sajber kriminalu u cilju pronalaženja mete napada. Sajber rizik je složen, podložan stalnim promenama i stalnom razvoju, sa većim brojem skrivenih elemenata rizika. Međutim, dok tržište sajber osiguranja brzo raste, analiza rizika se suočava sa nedostatkom doslednih i pouzdanih statističkih podataka u kontekstu u kojem je iznos nastalih šteta posebno podložan nestabilnosti. Stoga je kvantifikovanje ovog rizika težak zadatak. Zbog heterogenosti sajber rizika, procena premije osiguranja i/ ili potrebnog iznosa rezervi predstavlja izazov za stručnjake.

Sajber osiguranje se s početka pojavilo kao osiguravajuće pokriće za zaštitu kompanija od hakovanja, ali se ubrzo proširilo se na osiguranje u slučaju prekida poslovanja, iznude, finansijske prevare, zakonske odgovornosti i kvarova sistema koji nastaju kao rezultat sajber napada. Nakon uvoda, u drugom delu rada dat je pregled sajber rizika. U trećem delu rada opisane su specifičnosti sajber osiguranja i obuhvat ovog osiguranja, kao i način određivanja premije sajber osiguranja. Na kraju, data su zaključna razmatranja ovog istraživanja.

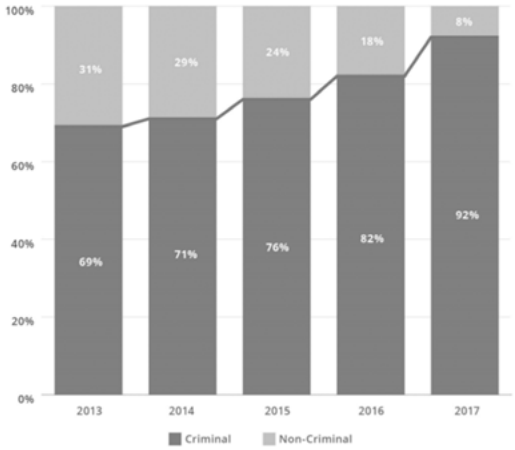
2. Sajber kriminal

Sajber kriminalna dela uključuju hakovanje, ransomware, malware / virus, phishing / BEC / socijalni inženjering, DDoS napade, ukradene uređaje, krađu novca putem bankovnog transfera i bankarske/ACH prevare i slične radnje. Drugi događaji, poput greški osoblja, nepravilnog rukovanja evidencijama u papiru, gubitka prenosnih računara, greški u programiranju, sistemskih greški i dr. se ne smatraju kriminalnim delima. Socijalni inženjering podrazumeva još složeniju proceduru, koja se postiže elektronskim resursima, kao i sastancima ili pozivima. Na primer, zahtevi kroz e-poštu, podržani telefonskim pozivom lažne službe pomoći, u cilju dobijanja pristupne kartice, šifre ili slično radi fizičkog unosa podataka.

Prema statistikama, u sektoru telekomunikacija, 85% ukupnih troškova u periodu od 2013. do 2017. godine, činili su troškovi nastali radnjama zaposlenih koji su pristupili osetljivim podacima. Sektor finansijskih usluga je, zbog neodgovornih zaposlenih, takođe pretrpeo velike gubitke, kako zbog krađe novca, tako i zbog krađe podataka o klijentima. Zdravstveni sektor je takođe izložen ovoj vrsti

napada. Prema podacima kompanije IBM Securiti i Instituta Ponemon, najčešće mete napada su: zdravstveni i finansijski sektor koji poseduju veliki broj ličnih podataka. Tu spadaju lični podaci, brojevi kreditnih kartica, računi, zdravstvene evidencije, podaci o vozačkoj dozvoli i sve druge informacije povezane sa identitetom određene osobe ili njenim finansijskim i zdravstvenim statusom (podaci o e-mail adresama, brojevima telefona, poštanskim adresama, itd.). Zatim slede tehnološki i IT sektor, sektor energetike i životne sredine. Posebnu metu sajber napada čine kompanije sa visokim godišnjim prihodom.

U poslednje vreme se sajber napadi i incidenti povećavaju, a štete koje oni izazivaju kontinuirano rastu. Statistički podaci o štetama nastalim zbog sajber kriminala pokazuju značajne razlike, zbog različitih metodologija njihovog prikupljanja i obrade. Bilo koja procena šteta nastalih zbog sajber kriminala se suočava sa nekoliko problema. Najznačajnije ograničenje u proceni šteta nastalih zbog sajber kriminala je njihovo potcenjivanje. Problem nepostojanja, neadekvatnosti ili neuporedivosti podataka o sajber kriminalu, koji se javlja u nekim zemljama, je povezan sa propisima i izveštavanjem, koji se razlikuju među industrijskim sektorima, čine podatke nedostupnim ili neuporedivim. Prikupljanje podataka je dodatno otežano zbog oklevanja mnogih kompanija da prijave sajber napade zbog reputacije.



Slika 1. *Kriminalni i nekriminalni incidenti*

Izvor: Net Diligence 2018 Cyber Claims Study[1]

Stoga, prikupljanje podataka i dalje predstavlja problem, a procene po zemljama su i dalje neprecizne. Međutim, predstavljamo rezultate studije „Net Diligence" (slika 1) kako bi se sagledala veza između kriminalnih i nekriminalnih sajber incidenata, kao i povećanje aktivnosti u sajber kriminalu od 2013. do kraja 2017. godine.

[1] Net Diligence (2018). *Cyber Claims Study*, Net Diligence, https://netdiligence.com

3. Sajber osiguranje

S obzirom na povezanost rizika u sajber osiguranju, njihovu prirodu, dugačak rep i nesigurnost, sajber osiguranje je trenutno relativno skupo u poređenju sa drugim vrstama osiguranja, uz procene da ono može biti tri puta skuplje od osiguranja od opšte odgovornosti i šest puta skuplje od osiguranja imovine.[2]

U ovom delu istraživanja razmotriće se glavne specifičnosti sajber osiguranja.

1. **Identifikacija rizika**. Ovo je nova vrsta osiguranja, tako da osiguravajuća društva još nemaju potrebno iskustvo i uspostavljene standardizovane procedure za identifikaciju sajber rizika. ITC sistemi se brzo razvijaju, sa čestom promenom same organizacije sistema, što utiče na promenu i rast sajber rizika. Pored tih rizika, postoji i grupa rizika koja se u literaturi često naziva „neafirmativnim" ili „tihim" rizicima, koji su rezultat šteta pokrivenih drugim polisama osiguranja, a koje su izazvane sajber događajem.
2. **Utvrđivanje verovatnoće**. Jedna od glavnih karakteristika ovog osiguranja je informaciona asimetrija. Osiguravači se suočavaju sa brojnim preprekama u postupku pribavljanja pouzdanih informacija o izloženosti osiguranika sajber riziku. Pored toga, neophodno je znati da se ova izloženost može menjati tokom čitavog perioda pokrića. Primenjene metode zaštite i softver koji osiguranik koristi su često su poverljivi a, s druge strane, postavlja se pitanje, ako se zaštitni softver primenjuje, da li će zaista obezbediti zaštitu i u kojoj meri. Jer, bezbednost je proces, a ne proizvod.
   Utvrđivanje izloženosti riziku se zasniva na parametru stope pojavljivanja (učestalosti), koji je vrlo teško odrediti za sajber rizike, a otežan je dinamičnim promenama napada, njihovom nepredvidljivošću i brzom prilagođavanju novim okolnostima. Poseban problem predstavlja nedostatak informacija ili znanja o efikasnosti bezbednosnih mera i standarda ili koliko one utiču na nivo rizika, pa stoga otežava utvrđivanje bilo kakvog smanjenja premije osiguranja. Sigurnost jednog sistema nije nezavisna, može uticati na sigurnost drugog povezanog sistema. Zato bi gotovo sve što je pokriveno neživotnim osiguranjem moglo na kraju biti izloženo „tihim" rizicima. Pogodne metode za procenu izloženosti potencijalnih osiguranika sajber rizicima su metode ispitivanja scenarija i upotreba stres testova. Ipak, kao što je navedeno, nedostatak podataka i pouzdanih statistika dodatno otežava utvrđivanje verovatnoća.
3. **Uticaj incidenata**. Osnovni parametar kvantifikacije rizika je, pored učestalosti, uticaj. Postavlja se pitanje kako unapred proceniti moguće gubitke, na primer, zbog krađe intelektualne svojine, ulaganja u ekspertizu, krađe ili

[2] PwC (2015). *Insurance 2020 & beyond: Reaping the dividends of cyber resilience*, PwC; and Z/YEN GROUP (2015). *Promoting UK Cyber Prosperity: Public-Private Cyber- Catastrophe Reinsurance, Long Finance.*

gubitka privatnih podataka o identitetu, troškove reputacije itd. Jedan od načina za merenje gubitaka je putem konkurentskih proizvoda, kojima je preuzet tržišni udeo od zakonitih vlasnika, kao i putem procene negativnog uticaja na cene akcija kompanija izloženih sajber napadima. Razvoj metodologije za procenu je od izuzetne važnosti jer, primera radi, krađa intelektualne svojine čini najmanje četvrtinu troškova sajber kriminala i, kada uključuje vojnu tehnologiju, stvara rizike i po nacionalnu bezbednost[3].
Trenutno, čini se potpuno nemogućim proveriti tačnost uticaja ovih rizika.[4]

4. **Obim osiguravajućeg pokrića**. U situaciji dinamičnih, brzo promenljivih sajber pretnji, sa svim poteškoćama u njihovoj identifikaciji, teško je utvrditi osiguravajuće pokriće klijenata. Stoga uslovi sajber osiguranja sadrže puno isključenja iz pokrića ali i ograničenja (limita) pokriću, koja su niska, posebno posmatrajući iz ugla velikih kompanija. To može uticati na stepen spremnosti klijenata da kupe takvo osiguravajuće pokriće.
5. **Premija osiguranja**. U slučaju procene premije osiguranja, treba uzeti u obzir korelaciju rizika, geografsku sličnost (uticaj na diverzifikaciju rizika), monokulturu (slični operativni sistemi), lako izvođenje (napadi su laki i jeftini za izvođenje) itd. Više o određivanju premije biće reči u odeljku 3.2.
6. **Uslovi osiguranja**. Imperativ je jasno definisati uslove, ali je ugovorni jezik za sajber osiguranje i dalje nejasan i neprecizan, a teško je tačno definisati šta je osiguranjem pokriveno, a šta nije. Još jedna poteškoća je preklapanje sa postojećim, tradicionalnim vrstama osiguranja. Kada se dogodi sajber incident, neophodno je utvrditi odgovornost za štetu, identifikovati vlasnike sistema, proizvođače softvera itd.
7. **Utvrđivanje visine štete**. U ovoj vrsti osiguranja, utvrđivanje visine štete je otežano činjenicom da se mnogi sajber napadi mogu otkriti tek protekom puno vremena nakon incidenta. Takođe, sajber napadi mogu trajati duži vremenski period. Da bi se utvrdio trošak, često je potrebno angažovati stručnjake i pravilno istražiti nastale konsekvence, pa stoga incident više nije poverljiv, a zahtev osiguranika je često da događaj bude strogo poverljiv.

3.1 Pokriće sajber osiguranja

Sajber osiguranje može biti nezavisan proizvod i ugovoreno kao dodatno osiguranje i može obuhvatati pokriće za štete koje je pretrpeo osiguranik i štete koje je pretrpelo treće lice (odgovornost osiguranika)[5]. Zbog prirode ovog osiguranja, ono je najčešće prilagođeno određenom klijentu.

[3] Expenses for extortion or from an act of terrorism, war, or a military action are covered in rare cases, but mostly noted as exclusions.

[4] Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley.

[5] Fisrt party Loss i Third Party Loss

Uopšteno posmatrano, postoje tri ključne komponente sajber bezbednosti. Prvo, osiguranje nadoknađuje troškove koje kompanija plaća da bi odgovorila na sajber incident (zaštita pogođenih pojedinaca, plaćanje troškova za oporavak oštećenih ili uništenih podataka, ili čak plaćanje potraživanja zbog iznude). Drugo, sajber osiguranje pokriva naknade i štete koje kompanija može platiti u sudskom postupku koji je nastao kao rezultat sajber incidenta. Treće, sajber osiguranje nadoknađuje izgubljeni prihod ili troškove nastale usled poremećaja poslovanja povezanih sa sajber incidentom.

Obuhvat klasifikacije osiguranja varira u različitim studijama i autori preporučuju prilagođenu klasifikaciju koju je dala ENISA[6].

Većina osiguravajućih društava pokriva direktnu štetu nastalu gubitkom poslovnog prihoda usled sajber incidenta, prekida poslovanja, sajber iznude, kao i oporavka podataka. Preduzeću su potrebni podaci u realnom vremenu. Svaki prekid procesnog lanca - čak i na minut - mogao bi prouzrokovati ozbiljne prekide poslovanja, što bi uticalo na bilanse preduzeća.

Sa novom regulativom, kao i prilagođavanjem potrebama kupaca, sektor osiguranja se suočava sa novim izazovima u pogledu sajber osiguranja. Bolje razumevanje sajber rizika, kako od strane kupca osiguranja, tako i od strane osiguravača, je jedan od osnovnih zahteva, ne samo u pogledu procene pokrivenosti više rizika sajber osiguranjem, već i u pogledu razumevanja sopstvenih potreba od strane klijenta. Do sada su proizvodi više bili orijentisani ka privrednim subjektima, ali sa rastom i razvojem IoT-a, fizička lica su sve više izložena ovim rizicima.

3.2. Određivanje premije sajber osiguranja

Određivanje premije osiguranja u ovoj vrsti osiguranja se, zbog nedostatka relevantne statistike, zasniva pretežno na kvalitativnim modelima, ali ipak uz oslanjanje na kvantitativne modele. Kvalitativne metode za određivanje premije osiguranja koriste alate zasnovane na pretpostavkama izloženosti riziku, nivelisanju rizika prema unapred određenoj skali zasnovanoj na upitnicima, kao i pristupu specijalizovanoj bazi podataka. Kvalitativne metode procene rizika zasnivaju se na stručnoj proceni različitih faktora koji mogu biti više ili manje subjektivni. Lingvistička promenljiva, npr. „veoma visok rizik", sadrži subjektivnost stručnjaka. Za iste podatke stručnjaci mogu pružiti različite jezičke vrednosti koje su svojstvene različitoj percepciji stručnjaka na osnovu njihovog odnosa prema riziku, iskustvu itd. Suprotno tome, u nekim slučajevima je stručno mišljenje lako dostupno i može biti još vrednije i pružiti tačnije informacije u odnosu na istorijske podatke. Međutim, metode procene rizika, koje se oslanjaju na procenu stručnjaka, potrebno je unaprediti, formalizovati i

[6] European Union Agency for Network and Information Security (2016). *Cyber Insurance: Recent Advances, Good Practices and Challenges*. ENISA.

konačno, stručno znanje iskazano lingvističkim vrednostima transformisati u numeričke vrednosti.[7]

Kvantitativne metode koriste aktuarske tehnike i razne modele koji su se pokazali primenljivim u drugim, sličnim problemima. Ti modeli obično pokrivaju različite parametre i zasnivaju se na raznim tradicionalnim matematičkim modelima, ali takođe i na tehnikama fazi matematike, veštačke inteligencije, teorije igara i dr. Glavna razlika između modela je vrsta i broj promenljivih koje ovi modeli mogu uključiti u evaluaciju i kojima se mogu baviti.

U svakom slučaju, pri utvrđivanju premije, polazna osnova je registar rizika koji treba da se zasniva na kombinaciji kvalitativnih i kvantitativnih metoda kako bi se iskoristile njihove prednosti i izbegli nedostaci i podstaklo korišćenje kvantitativne metode tamo gde je to moguće. Agregacija informacija zauzima značajno mesto u mnogim sistemima zasnovanim na znanju, gde je agregiranje podataka ili vrednosti potrebno. Uopšteno, može se reći da se pomoću agregacije simultano koriste različiti delovi informacija iz različitih izvora, u cilju donošenja zaključka ili odluke.[8]

U praksi se najčešće koristi paušalni pristup utvrđivanja premije sajber osiguranja, dok ostali pristupi koriste veći broj faktora korektivnog uticaja. Pri utvrđivanju premije osiguranja važno je da se slični faktori rizika kombinuju u jasno odredive grupe da bi se izbegli komplikovana primena tarife premija, komplikovani upitnik za pribavu osiguranja i teškoće u obradi osiguranja[9]. Faktori uticaja sa njihovim podelementima podeljeni su u nekoliko grupa.

1. Prva grupa faktora sastoji se od elemenata koji se odnose na aktivnost i detalje poslovanja preduzeća, veličinu preduzeća, imovinu ili prihod. Ovo je uobičajeni način određivanja stopa za mnoge vrste osiguranja.

Važan skup elemenata čine podaci o aktivnosti osiguranika, kao važan pokazatelj izloženosti riziku. Uobičajeni elementi pored gore navedenog su:

1) Povereni poslovi (autsorsing)
2) Zavisnosti od IT infrastrukture
3) Korišćenje, čuvanje ili deljenje podataka
   - Obim podataka

---

7 Milutinović, O., Kerkez, M., & Mladenović - Vojinović, B. (2018). Fuzzy logic inference system model for risk assessment in information technology and services environment, In: *Economic and Social Development*, 30th International Scientific Conference on Economic and Social Development, 249-255.

8 Paunović, M., Ralević, N., Gajović, V. (2020). Application of the C-Credibility Measure. *Tehnički vjesnik*, 27 (1), pp. 237-242. (ISSN: 1330-3651) https://doi.org/10.17559/TV-20200113093742

9 Jelena Doganjić, Živorad Ristić, „Diferenciranje premija kao preduslov za zaštitu od premijske nestabilnosti i negativne selekcije rizika“, Tokovi osiguranja 4/2011, 2011, str. 27-31

- osetljivost podataka (npr. lični podaci, zdravstveno stanje, intelektualna svojina)
- Posredna odgovornost

4) Korporativno prisustvo na društvenim mrežama

U ovu grupu se mogu svrstati i indikatori koji se odnose na izloženost osiguranika ili tržišta drugim jurisdikcijama.

2. Druga grupa faktora povezana je sa uobičajenim aktuarskim tehnikama, limitom osiguranja, odbitnom premijom, kao i dostupnim podacima o gubicima i incidentima u prethodnom periodu.

3. Najsloženiju grupu faktora čine elementi koji se odnose na IT procenu i njenu sigurnost. Identifikacija ovih elemenata utvrđuje se putem upitnika, razgovora sa specijalistima na terenu, IT revizijama itd.

Prema istraživanju autora, učestalost osiguranja od sajber napada je oko 0,20%, sa prosečnim gubitkom od 43.500 eur. Za osiguranje od mrežne sigurnosti, učestalost je oko 0,17%, uz veći prosečni gubitak od 75.300 eur. Međutim, u industrijama koje su više izložene tim rizicima, učestalost dostiže 0,60%, dok je prosečni gubitak blizu 150.000 eur. Treba napomenuti da na visinu štete utiču i visoki troškovi stručnjaka procenitelja, oko 30%. Prosečna premija osiguranja za osiguranje kompjuterskih napada (Computer Attack) iznosi 124 eur, dok je premija za Odgovornost za mrežnu bezbednost 183 eur. Sastavni deo ovog ugovora je ograničenje osiguranja i učešće u šteti.

Drugi metod određivanja premijskih stopa zasniva se na imovini, godišnjem prihodu ili broju zaposlenih klijenta. Ovaj faktor ima najveći uticaj. Tako utvrđena osnovna premija prilagođava se različitim faktorima uticaja, koji se mogu podeliti u dve grupe.

Prvu grupu čine elementi standardnog osiguranja, poput limita i odbitka, zatim bonusi, popusti za višegodišnje osiguranje i drugo. Korektivni faktori koji se odnose na limit osiguranja prikazani su u sledećoj tabeli:

Limit	**Faktor**
$500,000	0.809
$1,000,000	1.000
$2,000,000	1.132
$3,000,000	1.245
$4,000,000	1.371
$5,000,000	1.405

Druga grupa faktora uključuje dodatno osiguranje. Najčešći oblik je osiguranje u slučaju prekida poslovanja, gde stopa zavisi od vremena prekida i sektora industrije u kome je osiguranik. Prekidi u poslovanju su obično od 8 do 24 sata. Tako, za fakultete ovaj doplatak iznosi 5%, dok je za telekomunikacione kompa-

nije, za 8-satni prekid. doplatak od 15% i 18%. Klasifikacija industrijskih sektora vrši se prema izloženosti riziku. Najjednostavnija podela je prema nivou rizika, npr. nizak, srednji i visok rizik, kao i prema vrsti i obimu ličnih podataka o klijentima. Takođe, postavlja se pitanje, da li su kompanije neprofitne ili profitne, sa posebnim naglaskom na sektore finansijskih usluga, maloprodaju, zdravstvo itd.

Prema NIS Direktivi ključni sektori[10] koji su značajno izloženi sajber kriminalu su:

- Energetika (električna energija, nafta, gas)
- Transport (vazdušni, železnički, vodeni, drumski)
- Bankarstvo
- Infrastrukture finansijskog tržišta
- Zdravstveni sektor (uključujući bolnice i privatne klinike)
- Snabdevanje i distribucija vode za piće
- Digitalna infrastruktura
- Digitalne usluge: mrežni marketing, mrežni pretraživači i usluga računarstva u oblaku

Sa razvojem tehnologija, procene rizika u ITS okruženju postaju sve složenije. Nedostatak informacija o brojnim parametrima rizika utiče na pouzdanost procene rizika i procesa informacione sigurnosti. Procesi u sistemu su izloženi mnogim rizicima koji mogu nastati usled nepovoljnih scenarija i posledica koje mogu biti prouzrokovani različitim događajima. Informaciona tehnologija ima značajan uticaj na bezbednosne sisteme. Često postoje značajne neodređenosti povezane sa njihovom složenošću, pouzdanošću informacija i procenom istorijskih podataka.

Procena premije dovoljne za pokriće šteta nastalih usled realizacije sajber rizika je posebno teška zbog troškova sekundarnih efekata. Na primer, trošak informacionog sistema može biti lako definisan, ali to nije slučaj sa indirektnim troškovima, kao što su vrednost informacija, gubitak proizvodne aktivnosti i troškovi oporavka. U informacionim sistemima procene se zasnivaju na formuli:

$$Rizik = Verovatnoća \cdot Uticaj$$

Alternativna formula koja se koristi je

$$Rizik = Pretnja \cdot Ranjivost \cdot Uticaj.$$

u slučaju da postoji dovoljno istorijskih podataka, tako da se vrednosti mogu dodeliti čestim incidentima (kao što su malver, neželjena pošta, greške pri unosu podataka itd.). Standard ISO27005[11] predlaže, ali i potkrepljuje postupak mode-

[10] point (4) of Article 4 of NIS Directive.

[11] ISO. BS ISO/IEC 27005:2011

liranja rizika pružajući najbolje prakse za upravljanje rizicima koji se odnose na informacionu sigurnost. S obzirom na činjenicu da podaci o elementima rizika često nisu dostupni ili dovoljno pouzdani, za procenu vrednosti parametara pri unosu u model koriste se iskustvo, intuicija i stručno znanje o elementima i njihovom uticaju i klasifikaciji u posmatranom procesu.[12]

Na taj način se mogu uzeti u obzir faktori koji nisu obuhvaćeni upotrebom standardnih alata. Ali, kompanije za sajber osiguranje različito procenjuju rizik klijenta i većina njih ne prihvata jednoobrazno sertifikat kao potvrdu nivoa sigurnosti osiguranika. U cilju angažovanja na uspostavljanju uobičajene prakse poslovanja u ovom segmentu i višeg stepena doslednosti na tržištu, i samim tim razvoju tržišta, osiguravajuća društva su počela da ostvaruju saradnju[13].

Poteškoće kvantitativnog merenja sigurnosti koje postoje u kontekstu kvantifikacije rizika razmatrane su u Verendel, 2009[14]. Podaci vezani za IT rizik uvek su povezani sa subjektivnom stručnom procenom. Složene kvantitativne metode uglavnom koriste ograničene skupove podataka. To obično dovodi do nepotpune slike o rizicima, ali s druge strane, pojednostavljene metode takođe mogu dovesti do nepouzdanih očekivanja o riziku.

Kvantitativne i kvalitativne tehnike imaju neke prednosti i nedostatke. Tačnost procene stručnjaka i kvalitet rezultata mogu se poboljšati primenom kombinovanih modela. Na primer, modeli za procenu rizika predstavljeni u radu Gajović, Kerkez i Kočović[15] sa početnom idejom da se modelira ukupan rizik procesa na osnovu procene značaja različitih elemenata rizika, njihovom međusobnom odnosu i njihovom uticaju na ukupan rizik. U radu je razvijen model fazi logike zasnovan na modelima Analitički hijerarhijski proces (AHP) i Fazi analitički hijerarhijski proces (FAHP). Model je dizajniran da bude praktičan, razumljiv i lak za primenu i održavanje. U literaturi se razmatraju i predlažu i drugi modeli za pomoć u upravljanju sajber rizikom zasnovani na teoriji korisnosti, teoriji ekstremnih vrednosti[16], teoriji igara i dr. Neke od novih teorija i mera, kao što je na primer mera c-kredibiliteta[17] , mogu naći svoju primenu u rešavanju navedenih problema u razvoju proizvoda sajber osiguranja.

[12] Paunović, M., Ralević, N., Gajović, B., Mladenović-Vojinović, B., & Milutinović, O. (2018). Two-Stage Fuzzy Logic Model for Cloud Service Supplier Selection and Evaluation, *Mathematical Problems in Engineering*, MATH PROBL ENG, 11pages.

[13] Cambridge Centre for Risk Studies (2016). *Cyber Insurance Exposure Data Schema V1.0.*

[14] Verendel, V. (2009). Quantified security is a weak hypothesis: a critical survey of results and assumptions, in *Proc. of the 2009 workshop on new security paradigms workshop.* ACM, Oxford, 37–50.

[15] Gajović, V., Kerkez, M., & Kočović, J. (2018). Modeling and simulation of logistic processes: risk assessment with a fuzzy logic technique. *Simulation: Transactions of the Society for Modeling and Simulation International*, 94(6), 507–518.

[16] Martin, E., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research,* 272, 1109–1119.

[17] Ralević N., Paunović M. (2019). c-Credibility Measure. *Filomat*, Vol 33, No 9, pp. 2571-2582.

4. Zaključna razmatranja

U bliskoj budućnosti se očekuje da će potražnja za sajber osiguranjem neprestano rasti, usled uvođenja novih propisa, kao i povećane svesti o rizicima, ali i sve veće učestalosti sajber događaja. Potrebno je da kompanije sistematizuju rizike i donesu odluku o rizicima koje će izbeći, prihvatiti, kontrolisati ili preneti u osiguranje. Tržište sajber osiguranja će se i dalje razvijati.

Nedostatak obrazovanih stručnjaka sa iskustvom, statističkih podataka, standarda i kvantitativnih alata su ključni nedostaci za osiguranje i adekvatno pokriće. Obrazovanje, kako u smislu razumevanja izloženosti kompanije ovim rizicima, tako i znanja iz osiguranja, treba poboljšati. Generalno, sistemi se razvijaju usled dinamike samog sistema i evolucije tehnologije. Sama dinamika sistema podrazumeva promene unutar sistema. Nagli razvoj tehnologije zajedno sa njenom primenom predstavljaju problem za osiguranje.

Pored problema povezanih sa negativnom selekcijom, javlja se i problem moralnog hazarda. Osiguravač mora biti siguran da su pretpostavke postavljene na početku ugovora, u vezi sa sigurnošću sistema, tačne i tokom ugovora o osiguranju. Problem procene gubitaka od sajber kriminala leži u činjenici što je veliki deo njegovih uticaja nematerijalan. Prećutana izloženost ovim rizicima od strane kompanija, identifikovana je kao ključna prepreka u pogledu tačne procene akumulacije rizika. Modeli koji se češće koriste u proceni rizika zasnovani su na kvalitativnoj osnovi, između ostalih problema, uglavnom zbog nedostatka relevantnih podataka. Takvo ograničenje može prouzrokovati pogrešnu procenu cene rizika. Hibridni modeli koji koriste obe tehnike mogu dati bolje rezultate. Kvantitativni modeli zasnovani na fazi teoriji i teoriji neodređenosti, više odgovaraju prirodi problema sajber osiguranja.

Literatura

- Paunović, M., Ralević, N., Gajović, B., Mladenović-Vojinović, B., & Milutinović, O. (2018). Two-Stage Fuzzy Logic Model for Cloud Service Supplier Selection and Evaluation, *Mathematical Problems in Engineering*, MATH PROBL ENG, 11 pages, Hindawi Publishing Corporation.
- Cambridge Centre for Risk Studies (2016). Cyber Insurance Exposure Data Schema V1.0.
- Verendel, V. (2009). Quantified security is a weak hypothesis: a critical survey of results and assumptions, in Proc. of the 2009 workshop on new security paradigms workshop. ACM, Oxford, 37–50.
- Gajović, V., Kerkez, M., & Kočović, J. (2018). Modeling and simulation of logistic processes: risk assessment with a fuzzy logic technique. *Simulation: Transactions of the Society for Modeling and Simulation International*, 94(6), 507–518.

- Martin E., & Wirfs. J., (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272, 1109–1119.
- Milutinović, O., Kerkez, M., & Mladenović - Vojinović, B. (2018). Fuzzy logic inference system model for risk assessment in information technology and services environment, In: Economic and Social Development, 30th International Scientific Conference on Economic and Social Development, 249-255.
- Net Diligence (2018). Cyber Claims Study, Net Diligence, https://netdiligence.com
- McAfee Report (2018). Economic Impact of Cybercrime— No Slowing Down, february 2018.
- PwC (2015). Insurance 2020 & beyond: Reaping the dividends of cyber resilience, PwC.
- Z/YEN GROUP (2015). Promoting UK Cyber Prosperity: Public-Private Cyber- Catastrophe Reinsurance, Long Finance.
- Jaquith, A. (2007). Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley.
- Marsh (2015). UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk. HM Government, Marsh Ltd.
- European Union Agency for Network and Information Security (2016). Cyber Insurance: Recent Advances, Good Practices and Challenges. ENISA.
- Ralević N., Paunović M. (2019). c-Credibility Measure. *Filomat*, Vol 33, No 9, pp. 2571-2582. https://doi.org/10.2298/FIL1909571R
- Ponemon Institute (2016). 2016 Cost of Data Breach Study: Global Analysis. http://ibm.co/1tz141c
- European Commission – Press Release (2016). Joint Statement on the final adoption of the new EU rules for personal data protection. European Commission.
- European Council – Council of the European Union (2016). EU-wide cyber security rules adopted by the Council.
- Paunović, M., Ralević, N., Gajović, V. (2020). Application of the C-Credibility Measure. *Tehnički vjesnik*, 27 (1), pp. 237-242. (ISSN: 1330-3651) https://doi.org/10.17559/TV-20200113093742
- Jelena Doganjić, Živorad Ristić, „Diferenciranje premija kao preduslov za zaštitu od premijske nestabilnosti i negativne selekcije rizika“, Tokovi osiguranja 4/2011, 2011, str. 27-31

Marija Paunović
Jelena Doganjić

UDC 005.334:368
343.533::004

DOI: 10.5937/MegRev2201053P
Review scientific article
Received 15.04.2021.
Approved 20.04.2021.

CYBER INSURANCE AND ACTUARY ANALYSIS

Abstract: *The digital revolution is affecting everyone. Cyber risk is a natural consequence of digital transformation. The development of digital technologies is causing the emergence of new factors that affect the vulnerability of companies in different sectors of activity. With the rise of cyber threats, insurance contracts are emerging as basic tools to improve society's resilience to the impacts of these risks. Cyber Insurance is the fastest growing line of business in modern history. The aim of this paper is to present basic actuarial analyzes during the development of cyber insurance products.*

Keywords: *cyber insurance, insurance premium, risks in cyber insurance, cyber criminal*