

Sajber osiguranje i izazovi digitalnog doba

Danijela Glušac, Pravni fakultet, Univerzitet u Kragujevcu

Sažetak — Rad se bavi sajber osiguranjem kao savremenim instrumentom zaštite od posledica digitalnih pretnji u uslovima sve izraženije digitalizacije poslovanja i upravljanja podacima. Polazi se od činjenice da sajber rizike odlikuju visoka neizvesnost, nedostatak stabilnih empirijskih podataka, međusobna povezanost informacionih sistema i mogućnost nastanka velikog broja istovremenih šteta, što otežava njihovu procenu i ugovorno oblikovanje osiguravajućeg pokrića. U radu se analiziraju osnovne kategorije sajber rizika, razlika između pokrića za direktne štete i odgovornosti prema trećim licima, kao i specifičnosti sajber osiguranja u pogledu obima pokrića, ugovornih isključenja i značaja pravilne procene rizika. U radu se razmatra i stanje u Republici Srbiji, gde je ponuda ovog proizvoda još uvek ograničena, ali se istovremeno ukazuje da postojeći domaći pravni okvir omogućava da se sajber osiguranje posmatra kao vrsta imovinskog osiguranja, bez potrebe za njegovim posebnim zakonskim regulisanjem.

Ključne riječi – sajber osiguranje, sajber rizik, imovinsko osiguranje, odgovornost prema trećim licima, procena rizika.

Abstract – This paper examines cyber insurance as a modern instrument for protection against the consequences of digital threats in the context of the increasingly intensive digitalisation of business operations and data management. It proceeds from the premise that cyber risks are characterised by a high degree of uncertainty, a lack of stable empirical data, the interconnectedness of information systems, and the possibility of a large number of simultaneous losses, all of which make their assessment and the contractual design of insurance coverage more complex. The paper analyses the main categories of cyber risk, the distinction between first-party coverage and third-party liability coverage, as well as the specific features of cyber insurance with regard to the scope of coverage, policy exclusions, and the importance of proper risk assessment. The paper also considers the situation in the Republic of Serbia, where the availability of this insurance product remains limited, while at the same time indicating that the existing domestic legal framework allows cyber insurance to be treated as a form of property insurance, without the need for separate statutory regulation.

Keywords – cyber insurance, cyber risk, property insurance, third-party liability, risk assessment

I. UVOD

Digitalizacija poslovanja, upravljanja podacima i komunikacije dovela je do toga da sajber rizici postanu jedno od ključnih pitanja savremene ekonomije i prava osiguranja. Sve veća zavisnost privrednih subjekata od informacionih sistema, cloud infrastrukture i digitalnih mreža povećava izloženost incidentima kao što su povreda podataka, prekid poslovanja, sajber iznuda i neovlašćen pristup sistemima, što istovremeno stvara potrebu za novim oblicima ugovorne i ekonomske zaštite. U literaturi se zato naglašava da je sajber-

osiguranje nastalo kao odgovor na ograničenja tradicionalnih polisa, koje često nisu bile prilagođene štetama nastalim usled sajber incidenata, kao i da ono danas predstavlja važan element šireg sistema upravljanja digitalnim rizicima [1], [2].

Posebnost sajber-osiguranja proizlazi iz same prirode sajber rizika. Za razliku od klasičnih osiguravajućih rizika, sajber rizike odlikuju visoka neizvesnost, nedostatak stabilnih i potpunih podataka, izražena međusobna povezanost sistema i mogućnost istovremenog nastanka velikog broja šteta, što otežava procenu rizika i održivo oblikovanje pokrića [1]. Organizacija za ekonomsku saradnju i razvoj (OECD) dodatno ukazuje da razvoj tržišta sajber-osiguranja zavisi od veće jasnoće obima pokrića, preciznijeg ugovornog jezika i boljeg razumevanja potreba osiguranika, budući da nejasne formulacije polisa povećavaju rizik sporova i slabe poverenje u ovaj proizvod [5]. Agencija Evropske unije za sajber bezbednost (ENISA) u tom smislu posebno naglašava da neujednačen jezik procene rizika i terminologije u sajber-osiguranju predstavlja jednu od prepreka njegovom daljem razvoju [3].

Polazeći od toga, predmet ovog rada jeste analiza sajber-osiguranja kao pravnog instrumenta zaštite od posledica digitalnih pretnji, sa posebnim osvrtom na njegove osnovne karakteristike i izazove u savremenim uslovima. Posebna pažnja biće posvećena specifičnostima sajber rizika, složenosti ugovornih klauzula, pitanju pokrića i isključenja, kao i značaju pravilne procene rizika i predugovornih informacija koje osiguranik dostavlja osiguravaču. U tom okviru, sajber-osiguranje se posmatra ne samo kao sredstvo naknade štete, već i kao deo šireg mehanizma upravljanja rizicima i jačanja otpornosti poslovanja u digitalnom dobu [4], [2].

II. SAJBER RIZICI KAO NOVI IZAZOV SAVREMENOG DRUŠTVA

Iako je sajber rizik postao široko rasprostranjen termin, njegova definicija je i dalje predmet stalnog istraživanja i promena. U najširem smislu, sajber rizik se definiše kao rizik od obavljanja posla u sajber okruženju (*risk of doing business in the cyber environment*) [6]. Budući da je usko povezan sa primenom novih tehnologija, spada u grupu rizika na čije ostvarenje prevashodno utiče ljudski faktor.

U nastavku su predstavljeni najčešći sajber rizici, svrstani u različite kategorije.

1) Kategorija zaštite podataka i sajber odgovornosti

Ova kategorija namenjena je pokriću osiguranika, njegovih povezanih lica, zaposlenih i ostalih fizičkih lica koje osiguranik razumno smatra svojim zaposlenima. Ključni pokriveni rizici: tužbeni zahtevi trećih lica usled povrede poverljivih informacija (uključujući podatke o ličnosti) ili

bezbednosnog propusta kompjuterskog sistema osiguranika; tužbeni zahtevi trećih lica usled nepoštovanja merodavnih zakona o zaštiti podataka o ličnosti kao i drugih politika o zaštiti podataka o ličnosti i okolnosti koje mogu dati povoda podizanju tužbenih zahteva i istrazi organa javnih vlasti, kao i troškovi takvih postupaka takođe su pokriveni ako osiguranik odluči da izvesti osiguravača o istima [7].

2) Kategorija gubitka bezbednosti računarske mreže i podataka nakon unutrašnje greške-ovde dolazi do prekida poslovanja zbog tehničkog zastoja samog računarskog sistema kao nenemarnog sajber događaja, a nekad i zbog ljudskog promašaja [8]. Osiguranik može podneti zahtev za naknadu štete po osnovu pokrića iz ove kategorije sajber osiguranja najčešće samo u slučaju kada materijalni prekidi prelaze unapred određen broj sati (npr. prekid u trajanju većem od 12 sati) i u tom slučaju osiguranik ostvaruje pravo naknade iz osiguranja za celokupan period trajanja materijalnog prekida [7].

3) Kategorija upravljanja nastalim rizikom-jedna od obaveza kompanije koja se suoči sa sajber incidentom je i reagovanje na povredu privatnosti, odnosno obaveštavanje korisnika i upravljanje kriznom situacijom. No, te situacije ne prolaze bez daljih troškova angažovanja eksperata, bilo unutar ili van kompanije, kao i ulaganje u medijske objave i obaveštenja [9].

4) Kategorija sajber iznude-izmiruju se zahtevi za naknadu troškova proisteklih iz borbe protiv ucenjičavkog programa koji ograničava pristup računarskom sistemu ili pohranjenim podacima i traži otkupninu. Ključni pokriveni rizici: iznosi plaćeni radi sprečavanja i okončanja sajber iznude; troškovi angažovanja savetnika za rešavanje i otkrivanje uzroka sajber iznude; pretnje iznude, u zavisnosti od načina njihovog definisanja, koje pogađaju osiguranikove kompjuterske sisteme i koji mogu uzrokovati finansijsku i reputacionu štetu [8].

U zavisnosti od toga da li se sajber osiguranje pribavlja sa ciljem zaštite sopstvene imovine i podataka od sajber rizika ili sa ciljem pokrivanja sopstvene odgovornosti za propuste koji su kod trećih lica doveli do sajber rizika, razlikujemo osiguranje od sajber odgovornosti za direktne štete (engl. *First party cyber insurance*) i osiguranje od sajber odgovornosti prema trećim licima (engl. *Third party cyber insurance*) [7].

Osiguranje od sajber odgovornosti može se podeliti na dva osnovna vida. Prvi se odnosi na direktne štete, odnosno na gubitke koje trpi sam osiguranik usled sajber incidenta. Drugi se odnosi na odgovornost prema trećim licima, kada zbog sajber događaja štetu pretrpe druga lica, pa osiguranje pokriva obavezu osiguranika prema njima.

Osiguranje za direktne štete obuhvata situacije kao što su krađa ili otkrivanje poverljivih podataka, zlonamerno ili slučajno uništenje podataka, otkaz IT sistema, sajber iznuda, kao i napadi virusima i zlonamernim softverom. Njegova svrha je da nadoknadi gubitke koji neposredno pogađaju samog osiguranika nakon sajber napada. U tu grupu spadaju, na primer, troškovi digitalne forenzike, prekida poslovanja, obnove podataka, gubici nastali sajber kriminalom, izdaci povodom sajber iznude, troškovi odnosa s javnošću radi

očuvanja reputacije, pravni troškovi, kao i troškovi obaveštavanja pogođenih lica, kol centra i kreditnog praćenja.

S druge strane, osiguranje od sajber odgovornosti prema trećim licima štiti osiguranika u slučajevima kada zbog povrede podataka ili bezbednosnog propusta štetu pretrpe druga lica. To je posebno značajno u poslovnim odnosima, jer u slučaju većih incidenata tužbom često budu obuhvaćene sve strane koje su na bilo koji način učestvovala u radu na kompromitovanom sistemu, uključujući i spoljne saradnike ili dobavljače. Ovo osiguranje, stoga, pokriva troškove sudske odbrane, iznose poravnjanja, presude i druge odluke, kao i kazne i naknade koje mogu proisteći iz takvih sporova.

III. SPECIFIČNOST SAJBER OSIGURANJA

Sudska praksa pokazuje da su sporna pitanja sajber-osiguranja najčešće vezana za tumačenje isključenja, obim pokrića i prirodu nastale štete. U predmetu *Merck & Co., Inc. v. ACE American Insurance Co.* sud je zauzeo stav da klasično isključenje za „*hostile or warlike action*“ ne isključuje automatski pokriće za štetu nastalu usled *NotPetty* sajber-napada, jer polisa nije dovoljno jasno predviđala primenu takvog isključenja na napad usmeren protiv civilnog privrednog subjekta [10]. Nasuprot tome, u predmetu *National Ink & Stitch, LLC v. State Auto Property & Casualty Insurance Co.* sud je prihvatio da *ransomware* napad može dovesti do „direktnog fizičkog gubitka ili oštećenja“ računarskog sistema, što je bilo od značaja za priznavanje pokrića po imovinskoj polisi subjekta [11]. Posebno je značajan i predmet *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, LLC*, u kome je utvrđeno da osiguravač ima obavezu da snosi troškove pravne odbrane osiguranika, jer je objavljivanje osetljivih medicinskih podataka na internetu potencijalno spadalo u pokriveni rizik po polisi odgovornosti subjekta [12]. Ovi sporovi pokazuju da je u sajber-osiguranju ishod često uslovljen preciznošću ugovornog jezika, a ne samo prirodom samog incidenta. Upravo zato sudska praksa sve jasnije potvrđuje da su jasno formulisana isključenja, definicije i uslovi za aktiviranje osiguravajućeg pokrića od presudnog značaja za pravnu sigurnost strana u ugovoru.

U Republici Srbiji relativno mali broj osiguravača uopšte nudi ovaj proizvod osiguranja. Tradicionalne vrste osiguranja imovine ne pokrivaju ove vrste rizika, iako je moguće da se i po takvim polisama osiguranja pruža pokriće prilično ograničenog obima [13]. Sajber osiguranje je jedna od mogućnosti koje stoje na raspolaganju u cilju izgradnje bezbednosti i zaštite od ovakvih pretnji, te sposobnosti brzog oporavka ako se ona ipak dogode.

Uprkos specifičnostima sajber rizika, postojeće odredbe srpskog ugovornog prava osiguranja i dalje mogu primenjivati na sajber osiguranje. Posebno ukazuje na to da se u našem pravu pokazala korisnom opšta podela na osiguranje lica i osiguranje imovine iz Zakona o obligacionim odnosima iz 1978. godine, jer omogućava svrstavanje sajber osiguranja u već postojeći sistem. U literaturi se navodi da pristup srpskog

prava omogućava da se sajber osiguranje posmatra kao vrsta imovinskog osiguranja, pa zato nije potrebno posebno zakonski uređivati ugovor o sajber osiguranju. Drugim rečima, postojeći domaći pravni okvir je dovoljno širok da obuhvati i ovu novu vrstu rizika [14].

IV. ZAKLJUČAK

Sajber osiguranje predstavlja važan pravni i ekonomski instrument zaštite u uslovima intenzivne digitalizacije poslovanja, upravljanja podacima i komunikacije. Razvoj informacionih tehnologija, uz istovremeni porast učestalosti i složenosti sajber incidenata, pokazao je da tradicionalni modeli osiguranja često nisu dovoljni za adekvatno pokriće šteta koje nastaju u digitalnom okruženju. Zbog toga se sajber osiguranje sve jasnije izdvaja kao poseban odgovor tržišta osiguranja na savremene oblike rizika.

Analiza je pokazala da posebnost sajber osiguranja proizlazi pre svega iz prirode sajber rizika, koje odlikuju visoka neizvesnost, dinamičnost, međusobna povezanost sistema i mogućnost nastanka velikog broja istovremenih šteta. Upravo te karakteristike otežavaju procenu rizika, određivanje premije, kao i precizno ugovorno definisanje pokrića i isključenja. Istovremeno, praksa potvrđuje da su jasne ugovorne klauzule, precizan jezik polise i pravilna procena rizika od presudnog značaja za pravnu sigurnost ugovornih strana i efikasno ostvarivanje osiguravajuće zaštite.

Poseban značaj ima razlikovanje između pokrića za direktne štete i pokrića odgovornosti prema trećim licima. Dok prvo pruža zaštitu samom osiguraniku od posledica sajber incidenta, drugo obezbeđuje pokriće odgovornosti prema licima koja trpe štetu usled povrede podataka ili bezbednosnih propusta. Time sajber osiguranje potvrđuje svoju dvostruku funkciju: ono nije samo sredstvo naknade štete, već i mehanizam šireg upravljanja rizicima, očuvanja kontinuiteta poslovanja i zaštite reputacije privrednih subjekata.

Kada je reč o Republici Srbiji, može se zaključiti da je tržište sajber osiguranja još uvek nedovoljno razvijeno, budući da relativno mali broj osiguravača nudi ovu vrstu proizvoda. Ipak, uprkos ograničenoj ponudi i nedovoljnoj zastupljenosti u domaćoj praksi, postojeći pravni okvir omogućava da se sajber osiguranje sagleda kao vrsta imovinskog osiguranja, bez potrebe za njegovim posebnim zakonskim regulisanjem. To ukazuje da je dalji razvoj ove oblasti pre svega uslovljen razvojem tržišta, unapređenjem ugovornih uslova i jačanjem svesti o značaju zaštite od digitalnih pretnji.

Na osnovu svega navedenog, može se zaključiti da će značaj sajber osiguranja u budućnosti nesumnjivo rasti. Sa razvojem digitalne ekonomije raste i potreba za efikasnim, jasnim i pravno sigurnim modelima osiguravajuće zaštite.

Upravo zato sajber osiguranje treba posmatrati kao neizostavan deo savremenog sistema upravljanja rizicima i kao oblast koja će u narednom periodu zahtevati dodatno teorijsko, zakonodavno i praktično usavršavanje.

LITERATURA

- [1] C. Biener, M. Eling, J.H. Wirfs, "Insurability of cyber risk: An empirical analysis," *The Geneva Papers on Risk and Insurance – Issues and Practice*, vol. 40 (1), pp. 131-158, 2015.
- [2] OECD (2017). Enhancing the role of insurance in cyber risk management. OECD Publishing. Preuzeto sa https://www.oecd.org/en/publications/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en.html
- [3] ENISA. (2017). Commonality of risk assessment language in cyber insurance. European Union Agency for Cybersecurity. Preuzeto sa <https://www.enisa.europa.eu/sites/default/files/publications/WP2017%2000-3-3-2%201%20Recommendations%20on%20Cyber%20Insurance.pdf>
- [4] International Association of Insurance Supervisors (IAIS). (2020). Cyber risk underwriting: Identified challenges and supervisory considerations for sustainable market development. Preuzeto sa <https://www.iais.org/uploads/2022/01/201229-Cyber-Risk-Underwriting-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf>
- [5] OECD. (2020). Encouraging clarity in cyber insurance coverage. OECD Publishing. Preuzeto sa https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/02/encouraging-clarity-in-cyber-insurance-coverage_c2dea16f/40beab07-en.pdf
- [6] Cyber Resilience – The cyber risk challenge and the role of insurance, Cro Forum, 2014.
- [7] S. Petrović, „Sajber osiguranje,” *Pravo i privreda*, vol. 58 (1), str. 206-217, 2020.
- [8] N. Žarković, G. Puzić, *Sajber osiguranje kao vrsta neživotnih osiguranja*, Novi Sad: Institut za energetiku, održivi razvoj i zaštitu životne sredine, 2020.
- [9] VIB-posredovanje u osiguranju. Sajber osiguranje. Preuzeto sa <https://vib.rs/sajber-osiguranje/>
- [10] Merck & Co., Inc., et al. vs. Ace American Insurance Company, et al., Docket Numbers: A-1879-21, A-1882-21, May 1, 2023. <https://law.justia.com/cases/new-jersey/appellate-division-published/2023/a-1879-21.html>
- [11] National Ink And Stitch, LLC v. State Auto Insurance Companies, Docket Number: 1:2018cv02138, January 23, 2020. <https://law.justia.com/cases/federal/district-courts/maryland/mddce/1:2018cv02138/427038/39/>
- [12] The Travelers Indemnity Company of America v. Portal Healthcare Solutions, LLC, Docket Number: 1:2013cv00917, August 7, 2014. <https://law.justia.com/cases/federal/district-courts/virginia/vaedce/1:2013cv00917/297932/33/>
- [13] D. Glušac, „Osiguranje od sajber odgovornosti,” *Usluge i vladavina prava: zbornik referata sa Međunarodnog naučnog skupa održanog 28. maja 2021. godine, na Pravnom fakultetu u Kragujevcu, Kragujevac: Pravni fakultet, Institut za pravne i društvene nauke, 2021, str. 299-306.*
- [14] M. Glintić, „Sajber osiguranje kao nova vrsta osiguranja - postoji li potreba za novom klasifikacijom osiguranja,” *Zbornik radova „Međunarodni pravni odnosi i pravda“ Kopaoničke škole prirodnog prava - Slobodan Perović, Beograd: Kopaonička škola prirodnog prava – Slobodan Perović, 2023, str. 465-482.*