Маст. Данијела Глушац, истраживач приправник
Правног факултета Универзитета у Крагујевцу

УДК: 159.923:004.738.5
DOI: 10.46793/UVP21.299G

ОСИГУРАЊЕ ОД САЈБЕР ОДГОВОРНОСТИ*

Резиме

У савременом свету осигурање је од посебног значаја због своје актуелности у позитивноправном смислу, у светлу савремених тенденција, постојања нових регулатива и извора права. На тржишту једне државе делатност осигурања спада у ред услужних делатности, тј. у ред оних делатности чије је главно обележје пружање услуга, где је услуга свака активност или корист коју једна страна може понудити другој. Осигурање од сајбер одговорности има за циљ покриће ризика који долазе са модерним технологијама. Предмет истраживања састоји се и у одговору на спорна питања у вези са појмом, врстом и ризицима осигурања од сајбер одговорности да се на тај начин осветле значајни сегменти ове теме као и решења у Републици Србији. У даљем тексту, имајући у виду комплексност теме, а ограниченост обима рада, биће учињен осврт на главне специфичности ове врсте осигурања.

***Кључне речи**: осигурање, сајбер осигурање, сајбер одговорност, ризик, одговорност.*

1. Увод

Реч „осигурање“ на разним језицима (*insurance, assurance, Versicherung...*) поред свог привредног, правног или техничког значења има и шире значење које означава појам сигурности, поверења у нешто, заштиту, обезбеђење, зајемчаност.[1] Према једној дефиницији осигурање представља институцију за накнаду штете настале остварењем стихијских и других ванредних догађаја, као и несрећних случајева, којима су изложени друштво или појединци и са тог аспекта улога осигурања посебно је важна за привреду, односно привредне

* Рад је написан у оквиру Програма истраживања Правног факултета Универзитета у Крагујевцу за 2021. годину који се финансира из средстава Министарства просвете, науке и технолошког развоја Републике Србије..

[1] Шулејић, П., *Право осигурања*, Београд, 2005, стр. 11.

организације.[2] Према другој дефиницији осигурање је институција која надоканађује штете настале у друштву, у његовој природи или код људи, услед дејства рушилачких сила и /или несрећних случајева и на тај начин оно пружа економску заштиту осигураницима (правним и физичким лицима) од штетних дејстава и економских поремећаја до којих долази када настане осигуран случај, односно када се оствари ризик у свим фазама друштвене репродукције, или у свакодневном животу људи.[3] У основи саме идеје осигурања лежи начело узајамности и солидарности. Идеја је врло стара и једноставна. Ако је један ризик расподели на више носитеља (атомизира), већа је сигурност да ће особа која је претрпела штету због ризика који им заједнички прети успети остварити одштету.[4] Протеклих година знатно су повећане штете од остварења сајбер ризика. Привредна друштва постају свеснија опасности са којима се суочавају и нужности управљања ризицима.[5] Исти је случај и са физичким лицима која су такође изложени бројним сајбер опасностима. Сајбер осигурање[6] је једна од могућности које стоје на располагању у циљу изградње безбедности и заштите од оваквих претњи, те способности брзог опоравка ако се она ипак догоде. Имајући у виду недовољну истраженост ове значајне проблематике у релеватној литератури из области права осигурања рад има за циљ да проучи сложеност правних односа и основне карактеристике исте.

2. Појам и врсте осигурања од сајбер одговорности

Последњих година расте интересовање за сајбер ризике и то се сматра једним од најизазовнијих питања за решавање јер сајбер ризици утичу на компаније и друштво. Ширење информационих технологија у пословању и у свакодневној стварности кроз експанзију друштвених мрежа, мобилних уређаја, бежичне технологије и услуга је довело до повећане рањивости компанија, које су почеле да траже методе којима би обезбедиле континуитет пословања у случају сајбер напада. Почевши од 1998. године осигурање од сајбер одговорности постаје све значајније на тржишту осигурања.[7] Начелно

[2] *Економска енциклопедија*, Књига II, Београд, 1984, стр. 286-287.
[3] Маровић, Б., *Осигурање*, Београд, 1993, стр. 13-14.
[4] Павић, Д., *Уговорно право осигурања - коментар законских одредаба*, Загреб, 2009, стр. 7.
[5] Жарковић, Н., Пузић, Г., Ђорђевић, Б., *Одрживост управљања ризицима у друштвима за осигурање*, Нови Сад, 2015, стр. 11.
[6] У литератури су у употреби оба термина и осигурање од сајбер одговорности (*cyber liabilty insurance*) и сајбер осигурање (*cyber insurance*), те ћемо оба користити у раду.
[7] Најраније познате полисе сајбер осигурања 1998. године су први пут увеле технолошке компаније у партнерству са осигуравајућим компанијама како би клијентима понудиле и технолошке услуге и осигурање. Будући да је то било ново и неистражено подручје, ове компаније су почеле са малим осигураним сумама (International Computer Security Association (ICSA) понудила је покриће од 250000

може се установити да су се на преласку у нови миленијум променили, односно, појавили многи чиниоци, неки од њих са убрзаним дејством, који су утицали, а утицаће свакако и даље на будућност сајбер осигурања. Осигурање од сајбер одговорности може у себи садржати пет елемената. Најпре, у питању су покриће сопствених штета (штета због прекида рада, штете због обнављања података), покриће насталих трошкова (трошкови информатичких трагача-форензичара у циљу установљавања штете; трошкови правног саветовања из области прекршајног, кривичног права, страних прописа, трошкови обавештавања власти и погођених појединаца), те покриће одговорности према трећим лицима (законска, уговорена одговорност). Оно што нарочито обележава сајбер осигурање је управљање насталом кризом. Засебност за осигураника је у томе да осигуравајућа заштита може бити покренута већ у тренутку претпостављеног, а не само у тренутку насталог сајбер напада, што се јасно уграђује у услове осигурања. Осигураник такође добија на располагање „број за хитне случајеве" који по правилу није везан за осигуравача, већ непосредно за рачунарско привредно друштво. И, коначно, истичемо да се у услуге сајбер осигурања, као пети чинилац још уграђују мере спречавања настанка штетних догађаја, што се може оценити сасвим примереним и пожељним приступом. Ради се о испитивању информатичке безбедности, прављењу пробних напада на рачунаре, школовању запослених, о новчаној подршци мерама које спроводе сами осигураници итд.[8]

У зависности од тога да ли се сајбер осигурање прибавља са циљем заштите сопствене имовине и података од сајбер ризика или са циљем покривања сопствене одговорности за пропусте који су код трећих лица довели до сајбер ризика, разликујемо осигурање од сајбер одговорности за директне штете (енгл. *First party cyber insurance)* и осигурање од сајбер одговорности према трећим лицима (енгл. *Third party cyber insurance).*[9] Осигурање од сајбер одговорности за директне штете покрива губитке самог осигураника, док осигурање од сајбер одговорности према трећим лицима покрива штету насталу трећим лицима као што и сам назив каже. Осигурање од сајбер одговорности за директне штете може обухватати крађу или обелодањивање заштићених информација, злонамерно уништавање података, случајно оштећење података, ИТ систем неуспех, сајбер изнуду, вирусе и злонамерни софтвер. Осигурање од сајбер одговорности за директне штете покрива од губитака који произилазе директно из сајбер напада. Покривени су: форензички трошкови ради утврђивања узрока и обима губитка података; трошкови прекида пословања; трошкови обнављања података; директни губици од сајбер криминала; претње сајбер изнуђивањем; трошкови односа са

долара). Више у: Majuca, R., Yurcik, W., Kesan, J., *The Evolution of Cyberinsurance*, Information Systems Frontier, 2006, p. 4.

[8] Жарковић, Н., Пузић, Г., *Сајбер осигурање као врста неживотних осигурања*, 2020, стр. 22.

[9] Петровић, С., *Сајбер осигурање,* Право и привреда, бр. 1/2020, стр. 207.

јавношћу за поправљање репутације; правни трошкови; трошкови обавештавања, трошкови кол центра и трошкови кредитног праћења.[10] Осигурање од сајбер одговорности према трећим лицима штити пословање када дође до крађе података на мрежи или системима треће стране. Када велике компаније подносе тужбе због крађе података, обично именују све стране које су радиле на компромитованом систему, укључујући независне добављаче. Чак и ако је неко био малог дела пројекта може бити обухваћен парницом. Ова врста осигурања обухвата трошкове одбране проузроковане парничним поступцима, трошкове поравнања, пресуда и других одлука, као и казни и осталих накнада које проистичу из ових парница.[11]

Сајбер осигурање као осигурање од одговорности, генерално је у највећем броју случајева покривено полисама осигурања од професионалне одговорности, све докле год су сајбер ризици у вези са професионалним услугама које осигураник пружа својим клијентима. Другим речима, ова врста сајбер осигурања обухвата тужбене захтеве трећих лица који су резултат одговорности осигураника насталих поводом неовлашћеног коришћења или откривања података трећих лица током уговорног ангажмана са клијентом. Тужбени захтеви ове природе могу проузроковати трошкове правне заштите, поравнања и казни. Трошкови одбране и накнаде штете које произилазе из тужбених захтева трећих лица у највећем броју случајева су покривени полисама осигурања од професионалне одговорности, све докле год су исти у вези са осигураниковом професионалном делатношћу.[12]

3. Ризици покривени осигурањем од сајбер одговорности

Иако је сајбер ризик постао широко распрострањен термин, његова дефиниција је и даље предмет сталног истраживања и промена. У најширем смислу, сајбер ризик се дефинише као ризик од обављања посла у сајбер окружењу (*risk of doing business in the cyber environment*).[13] Будући да је уско повезан са применом нових технологија, спада у групу ризика на чије остварење превасходно утиче људски фактор.

У наставку су представљени најчешћи сајбер ризици, сврстани у различите категорије.

1) Категорија заштите података и сајбер одговорности

[10] *First Party Cyber Insurance Coverage* преузето 25.4.2021. године са https://insuretrust.com/first-party-cyber-insurance-coverage/

[11] *First-party vs. third-party cyber liability insurance* преузето 25.4.2021. године са https://www.techinsurance.com/resources/first-party-vs-third-party-cyber-liability-insurance

[12] Петровић, С., *нав. чланак*, стр. 208-209.

[13] *Cyber Resilience – The cyber risk challenge and the role of insurance*, Cro Forum , 2014, p. 5.

Ова категорија намењена је покрићу осигураника, његових повезаних лица, запослених и осталих физичких лица које осигураник разумно сматра својим запосленима. Кључни покривени ризици: тужбени захтеви трећих лица услед повреде поверљивих информација (укључујући податке о личности) или безбедносног пропуста компјутерског система осигураника; тужбени захтеви трећих лица услед непоштовања меродавних закона о заштити података о личности као и других политика о заштити података о личности и околности које могу дати повода подизању тужбених захтева и истрази органа јавних власти, као и трошкови таквих поступака такође су покривени ако осигураник одлучи да извести осигуравача о истима.[14]

2) Категорија губитка безбедности рачунарске мреже и података након унутрашње грешке-овде долази до прекида пословања због техничког застоја самог рачунарског система као ненамерног сајбер догађаја, а некад и због људског промашаја.[15] Осигураник може поднети захтев за накнаду штете по основу покрића из ове категорије сајбер осигурања најчешће само у случају када материјални прекиди прелазе унапред одређен број сати (нпр. прекид у трајању већем од 12 сати) и у том случају осигураник остварује право накнаде из осигурања за целокупан период трајања материјалног прекида.[16]

3) Категорија управљања насталим ризиком-једна од обавеза компаније која се суочи са сајбер инцидентом је и реаговање на повреду приватности, односно обавештавање корисника и управљање кризном ситуацијом. Но, те ситуације не пролазе без даљих трошкова ангажовања експерата, било унутар или ван компаније, као и улагање у медијске објаве и обавештења.[17]

4) Категорија сајбер изнуде-измирују се захтеви за накнаду трошкова проистеклих из борбе против уцењивачког програма који ограничава приступ рачунарском систему или похрањеним подацима и тражи откупнину. [18] Кључни покривени ризици: износи плаћени ради спречавања и окончања сајбер изнуде; трошкови ангажовања саветника за решавање и откривање узрока сајбер изнуде; претње изнуде, у зависности од начина њиховог дефинисања, које погађају осигураникове компјутерске системе и који могу узроковати финансијску и репутациону штету.[19]

[14] Петровић, С., *нав. чланак,* стр. 210.
[15] Жарковић, Н., Пузић, Г., *нав. дело*, стр. 23.
[16] Петровић, С., *нав. чланак,* стр. 211.
[17] *Сајбер осигурање*, преузето 25.4.2021. године са https://vib.rs/sajber-osiguranje/
[18] Жарковић, Н., Пузић, Г., *нав. дело*, стр. 24.
[19] Петровић, С., *нав. чланак,* стр. 213.

4. Осигурање од сајбер одговорности у Републици Србији

За разлику од високоразвијених држава, где је тржиште одговорило на претње понудом конкретних производа који се међусобно разликују, домаћа друштва још увек немају у понуди ову врсту осигурања која би одговарала садржини услова осигурања страних осигуравача.[20] Традиционалне врсте осигурања имовине не покривају ове врсте ризика, иако је могуће да се и по таквим полисама осигурања пружа покриће прилично ограниченог обима. Тако, на пример, традиционално осигурање имовине пружало би осигуравајуће покриће у случају да сајбер напад доведе до настанка неког од осигураних ризика као што су пожар или експлозија, који проузрокују материјалну штету на осигураним стварима. Домаћа друштва за осигурање продају „Комбиновано осигурање електронских рачунара, процесора и сличних уређаја", које пружа покриће само од тзв. пожарних ризика и крађе, својствених осигурању имовине.[21] До дана приступања Републике Европској унији, код страног друштва за осигурање могу се осигурати ризици за које се у Републици не врши осигурање, као и други ризици за које то пропише Влада Републике Србије.[22] Из наведене одредбе Закона о осигурању закључујемо да се може директно купити полиса сајбер осигурања код страног осигуравајућег друштва.

Због могућег преклапања осигураних ризика, између полисе за осигурање од професионалне одговорности и полисе за сајбер осигурање, осигураник би пре њене куповине свакако требало да спроведе детаљан *due diligence* како би избегао потенцијално дуплирање осигураних ризика.[23]

5. Закључак

Сајбер осигурање је област која се брзо развија и која привлачи све више пажње практичара и истраживача. Осигурање, алтернативни начин за решавање преосталих ризика, тек је недавно примењено на сајбер свет. Незрело тржиште сајбер осигурања суочава се са низом јединствених изазова на путу свог развоја. Сајбер осигурање је основни алат за пренос финансијских ризика повезаних с ИТ-ом са осигураника на осигуравача. Ускоро ће постати незамисливо да компанија у својој понуди осигурања нема сајбер полису.

Свако захваћен сајбер нападом који је проузроковао неку врсту новчаног губитка желеће одговарајуће обештећење. Та раван заштите ће вероватно бити сматрана доњом границом. Међутим, многима ће бити потребна додатна

[20] Јовановић, С., *Осигурање од информатичких ризика*, Теме, бр. 3/2017, стр. 824.
[21] Голијанин Стајшић, Н., *Осигурање као начин управљања сајбер ризицима*, Зборник радова Факултета техничких наука у Новом Саду, бр. 10/2020, стр. 1788.
[22] Ч. 274 ст. 2 Закона о осигурању (Сл. гласник РС, бр. 139/2014)
[23] Петровић, С., *нав. чланак*, стр. 209.

помоћ. Разумљиво је да ће то подразумевати различите видове техничке подршке, правне помоћи, даљинске обуке за повећање сопствене безбедности, па можда и психолошког саветовања. Оваква допуна услуга не само што ће унапредити ниво покрића, већ ће такође осликавати додатну вредност коју осигураницима дају сајбер полисе.

Закључујемо да производи сајбер осигурања чине Интернет сигурнијим окружењем јер сајбер осигуравачи захтевају од компаније да минимизирају губитке користећи економске подстицаје и појединци/организације све више виде сајбер осигурање у сопственом интересу. Постоји потенцијал за већи развој тржишта при чему велику улогу има освештавање и информисање потрошача о изложеностима разним облицима сајбер криминала те могућим губицима којима их излажу потенцијални сајбер напади. Управљање пословним ризицима је битан елемент корпоративног управљања, а сајбер осигурање недвосмислено треба да постане део пословне стратегије сваког већег пословног субјекта. Свакако да је потребно разграничити ову врсту осигурања у односу на постојеће врсте осигурања, али је нужно развити интердисциплинарни однос, пошто је неопходно покрити и сопствене штете и штете нанесене другима.

Тренутно у Републици Србији није понуђено осигурање од сајбер одговорности као самостални облик заштите. С друге стране у условима других врста осигурања као нпр. осигурање од одговорности из делатности и из осигурања од одговорности за производе искључује штета настала због сајбер одговорности и из делатности обезбеђивача Интернета. Но, то не значи да применом члана 274 Закона о осигурању се не може купити полиса директно у страном осигуравајућом друштву.

Danijela Glušac, LL.M., Junior Researcher
Faculty of Law, University of Kragujevac

CYBER INSURANCE

Summary

In the modern world, insurance is of special importance due to its relevance in a positive legal sense, in the light of modern tendencies, the existence of new regulations and sources of law. On the market of one country, the insurance business belongs to the service activities, ie. among those activities whose main feature is the provision of services, where the service is any activity or benefit that one party can offer to the other. Cyber insurance

aims to cover the risks that come with modern technologies. The subject of the research also consists in answering to the disputable questions regarding to the concept, type and risks of cyber insurance in order to to put a light on significant segments of this topic as well as solutions in the Republic of Serbia. In the following text, having in mind the complexity of the topic, and the limited scope of work, a review will be made of the main specifics of this type of insurance.

Key words: *Insurance, cyber insurance, cyber liability, risk, liability.*

Литература

Голијанин Стајшић, Н., *Осигурање као начин управљања сајбер ризицима*, Зборник радова Факултета техничких наука у Новом Саду, бр. 10/2020.

Економска енциклопедија, Књ. II, Београд, 1984.

Жарковић, Н., Пузић, Г., Ђорђевић, Б., *Одрживост управљања ризицима у друштвима за осигурање*, Нови Сад, 2015.

Жарковић, Н., Пузић, Г., *Сајбер осигурање као врста неживотних осигурања*, 2020.

Јовановић, С., *Осигурање од информатичких ризика*, Теме, бр. 3/2017.

Majuca, R., Yurcik, W., Kesan, J., *The Evolution of Cyberinsurance*, Information Systems Frontier, 2006.

Маровић, Б., *Осигурање*, Београд, 1993.

Павић, Д., *Уговорно право осигурања - коментар законских одредаба*, Загреб, 2009.

Петровић, С., *Сајбер осигурање*, Право и привреда, бр. 1/2020.

Сајбер осигурање, преузето са https://vib.rs/sajber-osiguranje/

First Party Cyber Insurance Coverage преузето са https://insuretrust.com/first-party-cyber-insurance-coverage/

First-party vs. third-party cyber liability insurance преузето са https://www.techinsurance.com/resources/first-party-vs-third-party-cyber-liability-insurance

Cyber Resilience – The cyber risk challenge and the role of insurance, Cro Forum , 2014.

Шулејић, П., *Право осигурања*, Београд, 2005.

Прописи

Закон о осигурању („Сл. гласник РС“, бр. 139/2014);