UDK: 005.334:368 ; 343.533::004
CERIF: S137, S144
ТИП РАДА: СТРУЧНИ РАД

***Стефан* ПЕТРОВИЋ**[*]
дипломирани правник – мастер

САЈБЕР ОСИГУРАЊЕ[1]

Сажетак

Делатност осигурања је изузетно значајна за привредни сектор као такав, а тржишни учесници, предузетници, а посебно правна лица, као субјекти знатно већих економских капацитета посебно су заинтересовани да ризике свог свакодневног пословања ублаже, односно изнивелишу једним таквим механизмом, какав делатност осигурања пружа. У ери у којој технологија представља неизостављни део како индивидуалног, тако и пословног живота, сајбер осигурање постаје једно од најзначајнијих типова осигурања за материјалну сигурност најразличитијих субјеката, почев од појединаца – физичких лица, преко правних лица већих економских капацитета, па на крају и самих држава. Комјутери, интернет и технолошки напредак уопште, весници су својеврсне глобалне дигиталзације друштва, која за своју последицу има појаву једне нове, савремене врсте ризика – сајбер ризика.

Кључне речи: *Сајбер осигурање. – Сајбер одговорност. – енгл. First party cyber insurance. – енгл. Third party cyber insurance. – Сајбер ризици. – Подаци о личности.– Сајбер изнуде. – Мрежне инфраструктуре. – Управљање ризиком.*

---

* Електронска адреса аутора: *stefan92@gmail.com*.

1 Чланак представља део мастер рада „Имовинско осигурање са посебним освртом на начело обештећења и сајбер осигурање“.

I Појам и врсте сајбер осигурања

У најширем смислу, сајбер осигурање се користи ради заштите пословања и индивидуа од интернет ризика. Свако чији је саставни део пословања примање или слање електронских докумената, чување истих и повезивање са интернетом, подложан је сајбер одговорности.[2] 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 енгл. *First party cyber insurance* и енгл. *Third party cyber insurance.*

Када говоримо о сајбер осигурању првенствено мислимо на *First party cyber insurance*, јер је то тип сајбер осигурања који је неопходан највећем броју корпорација које нису део ИТ сектора.[3] Оно обухвата ризике са директним утицајем на пословање осигураника, који могу, на пример, проузроковати прекиде на мрежним системима осигураника и мрежним системима његових повезаних лица, као и утицати на повећање трошкова повраћаја осигураникових података и података његових повезаних лица. Ризици обухваћени овом врстом сајбер осигурања могу проузроковати додатне и неочекиване трошкове, као што су трошкови поправке и замене дигиталне имовине, трошкови пословних прекида (као последице хакерских напада, пада ИТ инфраструктурне мреже или грешака оператора), додатни трошкови обављања пословних активности или губитак прихода. Примери потенцијалних штета су:

- Санирање повреде података;
- Прекиди на мрежној инфраструктури;
- Сајбер изнуде;
- Одговорност према личним подацима запослених.

Third party cyber insurance, са друге стране, је полиса намењена лицима која су одговорна за успостављање и одржавање нападнутих и хакованих ИТ система.[4] Дакле, овај тип сајбер осигурања намењен је превасходно лицима која се баве развојем софтвера, ИТ компанијама или другим лицима одговорним за успостављање и одржавање корпо-

2 James A. Johnson, *Cyber insurance*, State Bar of Michigan – Inter Alia – Spring 2018, 2018, 1.

3 Third-Party Vs First-Party Cyber Risk Insurance: Protect Your IT Firm Right, доступно на адреси: *https://www.techinsurance.com/blog/cyber-liability/third-party-vs-first-party-cyber-risk-insurance/*, 28. 3. 2019.

4 Third-Party Cyber Risk Insurance, доступно на адреси: *https://www.ctrp.org/2018/03/21/differentiating-between-first-party-and-third-party-cyber-risk-insurance/*, 28. 3. 2019.

ративних мрежних инфраструктура. Неки од случајева који могу бити покривени овом полисом су на пример:

- Пропуст да се предвиди или спречи пренос вируса на машине клијента услед безбедносног пропуста софтвера;
- Обелодањивање или крађа поверљивих информација клијента чуваних на недовољно обезбеђеној мрежној инфраструктури клијента.

Дакле, у складу са претходно реченим, *First party cyber insurance* покриће обухвата трошкове проузроковане директно осигуранику. На пример, оно обухвата трошкове везане за истраживање узрока повреде података о личности или сигурносног инцидента, трошкове везане за поновно успостављање нарушених мрежних инфраструктура, трошкове обавештавања погођених субјеката, кредитног мониторинга, трошкове изнуде и губитака повезаних са прекидом пословања, трошкова изнуда итд.[5] Паралелно, са друге стране, *Third party cyber insurance* покриће обухвата трошкове одбране проузроковане парничним поступцима, трошкове поравнања, пресуда и других одлука, као и казни и осталих накнада које проистичу из ових парница.[6]

II Правна природа и однос са традиционалним врстама осигурања

First party cyber insurance према својој врсти, зависно од ризика који се њиме могу обухватити, као и предмета осигурања која се њиме штите, можемо сврстати у, или осигурање ствари, или осигурање од одговорности, или оба у већој или мањој мери. У пракси, ово је последица тога да велики број корпорација већ има своје полисе осигурања од професионалне одговорности (било због обавезе које им намећу законски прописи,[7] било због подизања сопствене конкурентности на тржишту, јер оне саме по себи представљају један од индикатора озбиљног и сигурног пословног партнера), чиме у већој или мањој мери могу бити осигурани од појединих сајбер ризика.

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 професи-

5 Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones, *Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk*, 38 Pages Posted, 2017, 11.

6 S. Romanosky, L. Ablon, A. Kuehn, T. Jones, 12.

7 Вид. Закон о ревизији, *Службени ɪласник РС*, бр. 73/2019, чл. 18.

оналним 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. Управо је ово разлог због којег се, када причамо о *First party cyber insurance*, прво мисли на сајбер осигурање као осигурање ствари, пошто се очекује да је већина ризика која би потпала под сајбер осигурање од одговорности (тј. тужбених захтева упућених осигуранику услед остварења сајбер ризика), већ покривена полисама за професионално осигурање од одговорности. 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.

III Значај

Технологија, друштвени медији и интернет трансакције данас играју кључну улогу у начину на који већина организација послује и долази до својих потенцијалних клијената. Управо ови комуникациони медијуми представљају полазне тачке сајбер напада, било да они долазе од стране обичних хакера, криминалаца, инсајдера или чак понекад и држава.

Само су током 2017. године, као резултат великог сајбер напада проузрокованог вирусима *Petya*, *NotPetya* и *WannaCry*, укупни процењени осигурани губици износили 3.3 милијарде долара. Глобални конгломерати као *Merck* и *Maersk* претрпели су озбиљне прекиде у њиховим системима и пословању током напада. Фармацеутски гигант *Merck* највише је погођен овим нападом услед чега је по основу сајбер полисе добио 2 милијарде долара, док је са друге стране, корпорација за транспорт *Maersk* по истом основу добила накнаду од преко 300 милиона долара.[8] Ови подаци јасно говоре о значају сајбер осигурања и величини штета које услед сајбер ризика могу настати, које би се у случају сопственог сношења истих засигурно значајно одразиле на пословање оштећених, а неретко и резултирале њиховим банкротством.

8 The 1 minute dialogue, доступно на адреси: *https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/silent-cyber.html#_ftn1*, 27. 3. 2019.

IV Ризици покривени сајбер осигурањем

Сајбер ризици су такви да константно и веома брзо еволуирају како хакерски напади постају све софистицираније и далекосежнији. Управо због овакве своје природе, не постоји исцрпна листа сајбер ризика укључена у пакет сајбер осигурања. У наставку су представљени најчешћи сајбер ризици, сврстани у различите категорије.

1. Категорија заштите података и сајбер одговорности

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[9]) или безбедносног пропуста[10] компјутерског система осигураника;[11]
- тужбени захтеви трећих лица услед непоштовања меродавних закона о заштити података о личности као и других политика о заштити података о личности;
- казне и поравнања са органима јавних власти настали услед кршења одредаба меродавног закона о заштити података о личности;
- трошкови *PCI-DSS* процене[12] настале услед повреде или сумње настанка повреде поверљивих информација;

9 Осигураник се појављује у улози обрађивача података у односу на личне податке својих клијената, који се појављује у улози руковаоца подацима. Руковалац одређује обим и сврху обраде података о личности и у случају обраде у обиму или за сврху која није уговорена, осигураник је као обрађивач података у прекршају. Вид. Закон о заштити података о личности, *Сл. гласник РС*, бр. 97/2008, 104/2009 – др. закон, 68/2012 – одлука УС и 107/2012.

10 Широко дефинисан у смислу да обухвата упаде, неовлашћен приступ и коришћење, губитак података и сл.

11 Широко дефинисано у смислу да обухвата хардвер, софтвер, персоналне рачунаре запослених за које имају дозволу коришћења у пословне сврхе, *cloud* и друге рачунарски управљане сервисе од осигураникових добављача.

12 Сваки писани захтев који је осигураник примио, од стране банке или друге платне установе која врши услуге новчаних трансакција, ради потраживања новчаног износа (укључујући пенале и уговорне казне) због непоштовања генерално прихваћених и објављених Стандарда безбедности података приликом коришћења платних картица, што је резултирало повредом или наводном повредом поверљивих информација.

- 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.

2. Категорија прекида функционисања мрежне инфраструктуре

Ова категорија намењена је покрићу осигураника и његових повезаних лица. Прекид функционисања мрежне инфраструктуре мора бити материјалан, што подразумева:

- делимичан или тоталан прекид, суспензију и погоршање услуга осигураника услед безбедносних пропуста[13] његовог компјутерског система;
- немогућност осигураника да приступи, поврати, користи, пренесе или сачува податке, услед тога што су подаци избрисани, оштећени, корумпирани, промењени или изгубљени услед безбедносног пропуста.

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. Ово због тога, како би се из покрића искључили планирани прекиди проузроковани редовним активностима одржавања осигураникове мрежне ИТ инфраструктуре.

Кључни покривени ризици:

- губитак прихода и додатни трошкови настали ради обезбеђивања поновног нормалног функционисања мрежне инфраструктуре, трошкови настали приликом свођења настале штете на минимум и додатни трошкови (укључујући поправку и замену хардвера);
- трошкови настали материјалним прекидима осигураниковог добављача услуга приликом одржавања његових ИТ инфраструктурних мрежа (укључујући и провајдере *cloud* услуга), када такви прекиди имају утицаја на осигураника.

13 Безбедносни пропусти су широка категорија и могу обухватати *DDOS* нападе, пријеме и преносе штетних кодова, софтвера и вируса, мењање, оштећење, уништење података, активности шпијунирања, крађе шифри и приступних кодова и сл.

3. Категорија управљања насталим ризиком

Ова категорија намењена је покрићу осигураника и његових повезаних лица. Настанак, односно наводни настанак сајбер ризика који погађа осигураникове компјутерске системе повлачи са собом и специфичне трошкове управљања новонасталим ризиком, који најчешће подразумева ангажовање тима специјалиста са задатком управљања читавим процесом који следи након настанка, односно наводног настанка сајбер ризика.

Кључни покривени ризици:

- правне услуге које генерално подразумевају саветодавне услуге свођења штете осигураног случаја на минимум, управљање одштетним захтевима физичких лица упућеним осигуранику, а чији су подаци о личности остварењем сајбер ризика повређени, као и координисање и давање инструкција ИТ стручњацима и/или консултантима за управљање ризиком о правним и регулаторним обавезама обавештавања физичких лица чији су подаци о личности повређени, трећих лица и јавних надлежних органа, а у вези са насталим осигураним случајем и сл.;
- ИТ услуге које подразумевају установљење узрока настанка сајбер ризика, идентификовање повреда поверљивих информација као и обима у којем су оне компромитоване, отклањање узрока настанка осигураног случаја, као и давање препорука у погледу заштите и унапређивања осигураникових компјутерских система у циљу избегавања будућих сајбер инцидената;
- рестаурација података и хардвера која подразумева утврђивање да ли се подаци које осигураник чува могу или не могу заменити, повратити или реинсталирати, као и приступање таквим радњама уколико су оне могуће, затим замене, поправке оштећених и уништених хардверских делова осигураниковог компјутерског система погођених вирусима и другим штетним софтверима и сл.;
- услуге репутационе заштите које подразумевају услуге савета и подршке консултаната за управљање ризиком и ПР агенција са циљем ублажавања и превенирања даље репутационе штете, као и њен накнадни опоравак;
- трошкови обавештења, који подразумевају прикупљање информација, успостављање посебних „*call*“ центара ради обавештења и њиховог достављања физичким лицима чији су подаци повређени, као и трећим лицима и надлежним јавним органима;

- кредитни и идентификациони надзор подразумева све накнаде и трошкове које је осигураник претрпео у случају крађе идентитета (нпр. трошкови крађе, заштите и враћања идентитета, укључујући и трошкове блокирања кредита и сл.).

4. Категорија сајбер изнуде

Ова категорија намењена је покрићу осигураника и његових повезаних лица.

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.

Обим осигураниковог покрића у многоме зависи од начина дефинисања претње изнуде. Претња изнуде се најчешће дефинише као:

- свака претња везана за наводни или стварни безбедносни пропуст осигураникових компјутерских система који проузрокују или могу проузроковати финансијску или репутациону штету осигуранику, укључујући сваку претњу везану за:
  - откривање, дељење, корумпирање, енкриптовање, уништење или коришћење података стечених неовлашћеним приступом или коришћењем осигураникових компјутерских система;
  - уношење штетних кодова на осигураникове компјутерске системе или коришћења осигураникових компјутерских система као средства за преношење штетних кодова;
  - корумпирање, енкриптовање, наношење штете или уништење осигураникових компјутерских система;
  - електронско комуницирање са осигураниковим клијентима или потенцијалним клијентима са којима је осигураник био или је и даље у неком уговорном ангажману, лажно се представљајући као осигураник са циљем прибављања новца, личних или корпоративних неоткривених информација клијента (енгл. *phishing*, *pharming*);
  - ограничавање или отежавање приступа осигураниковим компјутерским системима;

- откривање електронских поверљивих информација као и поверљивих информација у другим формама;
- извршење напада ограничења приступа осигураниковим компјутерским системима (енгл. *DDoS attack*).

или

- било каква претња:
  - намерног напада на осигураникове компјутерске системе;
  - незаконитог коришћења или јавног објављивања проневерених поверљивих информација осигураника, а све у циљу захтевања новца, хартија од вредности или друге опипљиве и неопипљиве имовинске вредности осигураника.

Претња изнуде такође обухвата било какву делимично извршену претњу или серију таквих повезаних претњи упућених осигуранику.

V Сајбер осигурање у Србији

Српски позитивноправни прописи одређују да послове осигурања/реосигурања не може обављати нико изузев друштава за осигурање/реосигурање са седиштем у Републици Србији која су у регистар надлежног органа уписана на основу дозволе Народне банке Србије за обављање послова осигурања/реосигурања.[14]

Изузеци од овог правила су ретки и када је то случај, ови изузеци су изричито прописани. Тако је нпр. прописано да друштво за осигурање може целокупан ризик осигурања имовине од елементарних непогода (град, мраз и друге опасности и/или природне непогоде какве су земљотрес, поплава и суша), као и осигурања финансијских губитака због лошег времена, да реосигура у Републици, односно у иностранству.[15] Такође, Влада Републике Србије је 2015. године донела Уредбу, којом је детаљније дефинисала ризике које домаћа правна и физичка лица могу осигурати, односно реосигурати код страног друштва за осигурање, односно реосигурање. Међутим, пакет осигурања заштите од сајбер ризика није један од њих.[16]

Законом нису прописане санкције за случај да лице са седиштем, односно пребивалиштем у Србији закључи уговор са страним друштвом за осигурање. Општа санкција би била ништавост уговора, у сми-

14 Закон о осигурању, *Сл. гласник РС*, бр. 139/2014, чл. 20 и чл. 3.

15 Закон о осигурању, чл. 7.

16 Вид. Уредба о одређивању ризика који се могу осигурати, односно реосигурати код страног друштва за осигурање, односно реосигурање, *Сл. гласник РС*, бр. 56/2015.

слу одредаба Закона о облигационим односима. Међутим, Закон о девизном пословању прописује одређене санкције:

- новчаном казном од 100.000 до 2.000.000 динара казниће се за прекршај резидент – правно лице, огранак страног правног лица, банка и нерезидент – правно лице ако изврши плаћање премија по основу уговора о осигурању који је закључен са нерезидентом – осигуравајућим друштвом, а који није дозвољен законом који уређује послове осигурања (члан 30 став 2);[17]
- новчаном казном од 10.000 до 500.000 динара казниће се за прекршај – предузетник ако изврши плаћање премија по основу уговора о осигурању који је закључен са нерезидентом – осигуравајућим друштвом, а који није дозвољен законом који уређује послове осигурања (члан 30 став 2);[18]
- новчаном казном од 5.000 до 150.000 динара казниће се за прекршај – физичко лице ако изврши плаћање премија по основу уговора о осигурању који је закључен са нерезидентом – осигуравајућим друштвом, а који није дозвољен законом који уређује послове осигурања (члан 30 став 2).[19]

Током израде овог рада, аутор је по инструкцији Сектора за надзор над обављањем делатности осигурања Народне банке Србије, упутио већим осигуравајућим друштвима питање, да ли исте пружају пакет осигурања заштите од сајбер ризика, на шта је свака од њих одговорила негативно. Поред тога, аутор је упутио сличан захтев Удружењу осигуравача Србије, где му је такође одговорено да ниједно друштво за осигурање које послује на територији Републике Србије нема посебно уврштене сајбер ризике, као пакет ризика против којег се пружа осигуравајућа заштита.

Закон о осигурању у својим прелазним и завршним одредбама предвиђа да се до дана приступања Републике Европској унији, код страног друштва за осигурање могу осигурати ризици за које се у Републици не врши осигурање, као и други ризици за које то пропише Влада Републике Србије.[20]

Узимајући претходно поменуту одредбу Закона о осигурању у обзир, заједно са резултатима спроведеног истраживања по основу питања упућених Народној банци Србије, Удружењу осигуравача Србије, као и

17 Закон о девизном пословању, *Сл. ɩласник РС*, бр. 62/2006, 31/2011, 119/2012, 139/2014 и 30/2018, чл. 59.

18 Закон о девизном пословању, чл. 61.

19 Закон о девизном пословању, чл. 62.

20 Закон о осигурању, чл. 274.

већим осигуравајућим друштвима која послују на територији Републике Србије, аутор недвосмислено закључује да се домаћи осигураници од сајбер ризика могу осигурати директно код иностраних осигуравајућих друштава.

VI Закључак

Учесници на тржишту, а поготово субјекти већих економских капацитета, су ти који су први почели да препознају опасности овакве дигиталне глобализације друштва, те су почели да улазе у уговорне аранжмане са највећим светским осигуравајућим кућама (нпр. Allianz, AXA, Anthem и др.), не би ли се, са једне стране, заштитили од последица сајбер ризика, односно, не би ли, са друге стране, подигли своју конкурентност на самом тржишту, а у ери друштвене дигитализације у којој живимо, осигурање од сајбер ризика је свакако један од показатеља конкурентности субјеката на тржишту. Домаћи, српски осигуравачи у овом домену касне за остатком света, још увек не предвиђајући посебне пакете осигурања којим би биле обухваћене различите категорије сајбер ризика. Међутим, ова ситуација убрзо ће се засигурно променити и та промена ће иронично доћи не од стране домаћих осигуравача, већ од стране притисака самих домаћих осигураника заинтересованих за сопствену сајбер заштиту са једне стране, као и притисака иностраних пословних партнера домаћих осигураника са друге стране, који често условљавају пословну сарадњу поседовањем полисе заштите од сајбер ризика.

Коришћена литература

Johnson James A., *Cyber insurance*, State Bar of Michigan – Inter Alia – Spring 2018, 2018.

Romanosky Sasha, Ablon Lillian, Kuehn Andreas, Jones Therese, *Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk*, 38 Pages Posted, 2017.

Third-Party Vs First-Party Cyber Risk Insurance: Protect Your IT Firm Right, доступно на адреси: *https://www.techinsurance.com/blog/cyber-liability/third-party-vs-first-party-cyber-risk-insurance/*, 28. 3. 2019.

Third-Party Cyber Risk Insurance, доступно на адреси: *https://www.ctrp.org/2018/03/21/differentiating-between-first-party-and-third-party-cyber-risk-insurance/*, 28. 3. 2019.

The 1 minute dialogue, доступно на адреси: *https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/silent-cyber.html#_ftn1*, 27. 3. 2019.

***Stefan* PETROVIĆ**
LL.M at Commercial Law

CYBER INSURANCE

Summary

Insurance is of a crucial importance for financial sector, and market participants, entrepreneurs, and specifically legal persons, which are, as entities of significantly larger economic capacities, especially interested in alleviating, i.e. leveling out the risks of everyday business with such mechanism that insurance offers. In the era where technology takes the essential part of individual and business life, cyber insurance becomes one of the crucial types of insurance for material security of various subjects, starting from individuals, legal entities of bigger economic capacities, and at the end even countries. Computers, internet and technological advancement in general, are heralds of global digitalization of society as a whole, which as its consequence has the advent of one new contemporary type of risk, cyber risk.

Key words: *Cyber insurance. – Cyber liability. – First party cyber insurance. – Third party cyber insurance. – Cyber risks. – Personal data. – Cyber extortions. – Network infrastructures. – Risk management.*

Датум пријема рада: 20. 1. 2020.
Датум прихватања рада: 10. 2. 2020.