Vilniaus universiteto Teisės fakulteto
Privatinės teisės katedra

Alekso Kučinsko,
V kurso, komercinės teisės
studijų šakos studento

Magistro darbas

Kibernetinių rizikų draudimo sutartis

Vadovas: Lekt. dr. Laurynas Didžiulis
Recenzentas: Lekt. dr. Tomas Kontautas

Vilnius 2016

TURINYS

ĮŽANGA

Bendroji tyrimo charakteristika. Kibernetinių rizikų draudimas yra viena iš naujausių draudimo sutarčių rūšių, kuri pasižymi savo dalyko specifiškumu – kibernetinėmis rizikomis. Kibernetinės rizikos – tai tikimybių visuma, kurios lemia neigiamas pasekmes bei žalos atsiradimą elektroniniams duomenims per elektroninių ryšių tinklais sujungtus kompiuterius ar kitokią informacinių technologijų įranga įvykdomas kibernetines atakas. Pasaulio ekonomikos forumas 2011 ir 2014 metais globalių rizikų ataskaitose, kibernetines rizikas pripažino kaip vienas iš penkių didžiausių šiuo metu susiduriamomis rizikomis visame pasaulyje[1]. Remiantis 2015 m. „Eurostat" statistika 97 procentai ūkio subjektų savo veiklą vykdo pasitelkdami informacines technologijas[2], todėl teigtina, jog artimiausiu metu neliks jokio visuomenės nario, kuris nebūtų suinteresuotas kibernetinėje erdvėje vykdyti savo verslą, vartoti prekes bei paslaugas ar tinklo ryšiais dalintis informacija su kitais žmonėmis. Pagal 2013 metų Eurostat statistiką 75 proc. Europos Sąjungos gyventojų reguliariai naudojasi internetu, 41 proc. naudojasi valstybinėmis paslaugomis per internetą, 61 proc. perka prekes internetu, 47 proc. naudojasi internetinės bankininkystės paslaugomis[3]. Bet kokios paslaugos, kurios yra tiekiamos ar valdomos informacinių technologijų tinklų priemonėmis yra kibernetinių atakų objektas. Tai gali būti padaroma įvairiais metodais, kaip ryšio sutrikdymu ar blokavimu, įsilaužimu į duomenų bazes, privačios klientų ir darbuotojų informacijos pasisavinimu, virusais ir kita kenksminga programine įranga. Kibernetinių rizikų draudimo sutartimis asmenys už tam tikrą atlygį siekia pernešti savo kibernetinę riziką draudimo bendrovėms taip siekiant sumažinti arba išvengti kibernetinių atakų neigiamus finansinius padarinius. Nors ir egzistuoja įvairios priemonės, kurios padeda sumažinti kibernetines rizikas kaip ugniasienės, anti-virusinės programos, protingo elgesio kibernetinėje erdvėje gerosios praktikos, įsilaužimų atpažinimo sistemos ir kita, tačiau nepaisant net ir patobulėjusiai kibernetinės apsaugos programinei įrangai bei elektroninių duomenų užkodavimo metodams, dėl atakų specifiškumo bei

[1] World Economic Forum. Global risks 2011 Sixth edition, An initiative of the Risk Response Network; World Economic Forum. Global risks 2014 Ninth edition.

[2] Eurostat. E-business integration. November 2015. [interaktyvus]. [žiūrėta 2016-03-29]. <http://ec.europa.eu/eurostat/statistics-explained/index.php/E-business_integration>.

[3] Eurostat. Internet use statistics – individual [interaktyvus]. [žiūrėta 2016-01-20]. <http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_use_statistics_-_individuals>.

jų gebėjimo prisitaikyti prie naujų apsaugos metodų, kibernetinių rizikų nėra įmanoma visiškai išvengti[4].

Tyrimo Aktualumas. Šiuo metu ypatingai yra padidėjusi ūkio subjektų dalis, kuri vykdo savo veiklą kibernetinėje erdvėje arba naudoja šiuolaikines technologijas darbo efektyvumui didinti. Kiekvieną dieną atsiranda naujų atakų, programinės bei aparatinės įrangos pažeidimo būdų, socialinės inžinerijos metodais nutekinama jautri informacija, prarandama privatūs klientų ir darbuotojų duomenys. Visa tai didina kibernetines rizikas. Žala padaroma kibernetinėje erdvėje, arba žala padaroma fiziniams objektams valdomiems tinklų ryšiais. Dėl tokių neišvengiamų aplinkybių kibernetinių rizikų draudimas įgauna vis didesnę paklausą. Pažymėtina, jog šia tema šio darbo rašymo metu nėra jokios literatūros lietuvių kalba, o rasta bei pasinaudota autorių darbais tik anglų kalba. Šiame darbe bus nagrinėjamas kibernetinių rizikų draudimo teisinis vertinimas, t. y. sutarties šalių teisės ir pareigos, kibernetinių rizikų draudimo suma, įmokos bei išmokos, draudžiamieji įvykiai, veiksniai didinantys bei mažinantys kibernetines rizikas. Pateikiamas vertinimas ar reikalinga kibernetinių rizikų draudimą išskirti nuo tradicinio draudimo.

2014 metais 90 procentų visų kibernetinių rizikų draudimo sutarčių rinkos dalį sudarė Jungtinės Amerikos Valstijos (toliau – JAV), todėl rašant šį darbą daugiausiai dėmesio skiriama į JAV susiformavusią kibernetinių rizikų draudimo sutarčių praktiką. Dažniausi asmenys, kurie naudojasi kibernetinių rizikų draudimu yra įprastiniai bei internetinių parduotuvių prekiautojai, sveikatos priežiūros įstaigos, viešbučiai bei finansines paslaugas teikiančios įstaigos. Vien Jungtinėje Karalystėje šio draudimo rūšis sudaro 3-4 milijonų svarų sterlingų rinką per metus, o visame pasaulyje bendra rinka apytiksliai vertinama tarp 500 ir 700 milijonų JAV dolerių[5]. Jungtinėje Karalystėje kibernetinių rizikų draudimą siūlo tik 9 draudimo bendrovės, o JAV tą patį draudimą siūlo 30-40 ūkio subjektų[6]. Šiuo metu dauguma draudimo bendrovių nedrįsta įeiti į šių draudimo sutarčių rinką, nes kol kas nėra pakankamai statistinių duomenų spręsti dėl kibernetinių rizikų draudimo finansinio atsiperkamumo[7]. O taip pat trūksta teorinio bei praktinio išnagrinėjimo dėl kibernetinių rizikų draudimo kiekvienos draudimo sutarties sąlygos. Dėl šių priežasčių šis

[4] ANDERSON, Ross; MOORE, Tyler. The economics of information security: A survey and open questions. University of Cambridge Computer laboratory. 2006.
[5] European Network and Information Security agency. Incentives and barries of the cyber insurance market in Europe. June 2012, p. 8.
[6] Ibid.
[7] VEYSEY, Sarah. Data scarce for insurers covering cyber risks [interaktyvus]. [Žiūrėta 2016-01-20]. <http://www.businessinsurance.com/article/20150610/NEWS06/150619981>.

darbas yra svarbus kaip teorinis bei praktinis pagrindas susisteminti teisinį kibernetinių rizikų draudimo vertinimą.

Tyrimo objektas. Teisiniai santykiai susiklostantys tarp kibernetinių rizikų draudimo sutarčių šalių.

Tyrimo Tikslas. Išanalizuoti kibernetinių rizikų draudimo sutarčių sąlygų teisinį vertinimą bei tokią praktikoje pasitaikančią problematiką kaip draudimo sutarties objekto, draudžiamųjų ir nedraudžiamųjų įvykių apibrėžimą.

Tyrimo Uždaviniai. Išsiaiškinti kibernetinių rizikų draudimo sutarčių sąlygų ypatumus, t. y. šalių teises ir pareigas, draudimo sutarties sumą, įmokas bei išmokas, kibernetines rizikas bei draudžiamuosius įvykius ir nedraudžiamuosius įvykius.

Tyrimo šaltiniai. Pagrindiniai šaltiniai, kuriais remtasi atliekant šį tyrimą yra Lietuvos Respublikos Civilinis kodeksas, draudimo įstatymas, draudimo teisės mokslininkų suformuluotos pozicijos įvairiuose teisės leidiniuose: straipsniuose, monografijose, kituose informaciniuose leidiniuose. Kibernetinės rizikos draudimų probleminiai aspektai analizuojami pasitelkus Jungtinių Amerikos Valstijų teismų praktika.

Tyrimo metodai. Atliekant tyrimą naudojami šie metodai: a) sisteminis – vertinamas loginis ryšys bei sąveika tarp apžvelgtų teisės aktų, doktrinos bei teismų praktikos; b) statistinis – vertinant kibernetinių rizikų draudimo paklausą atsižvelgiama į surinktus statistinius duomenis; c) lyginamasis – lyginama įvairių valstybių kibernetinių rizikų draudimo sutarčių suformuota skirtinga praktika bei daromos išvados atsižvelgiant į kitas panašias draudimo sutarties rūšis.

Tyrimo Originalumas ir naujumas. Pažymėtina, jog kibernetinių rizikų draudimo sutarčių tema informacijos nėra ypatingai daug. Šiuo metu nėra nė vieno vadovėlio ar kitokio mokslinio leidinio lietuvių kalba dedikuoto kibernetinių rizikų draudimo sutartims, o pasauliniu mąstu atrandami tik trumpi straipsniai detaliai nenagrinėjantys kibernetinių rizikų draudimo probleminius aspektus. Šio darbo originalumas pasireiškia tuo, kad darbe siekiama plačiai išanalizuoti kibernetinių rizikų draudimo sutarties nuostatas. Informacija yra kritiškai įvertinama ir apibendrinama.

1. Kibernetinių rizikų draudimo samprata

1.1.Kibernetinių rizikų sąvoka bei reikšmė

Draudimo tikslas yra ekonominės rizikos perėmimas ir paskirstymas kitam asmeniui (draudikui), kuriam rizika dėl teisinio santykio specifikos neatsiranda, tačiau pagal draudimo sutartį visiškai ar iš dalies pereina draudėjo patirtos rizikos turtiniai padariniai. Draudimo santykiuose draudėjas suvokia, jog ateityje galimai susidurs su tam tikromis rizikomis, kurių jis pats negalės išvengti arba nors ir galės sumažinti riziką, tačiau visai jos neeliminuos dėl įvairių, iš anksto nenumatytų priežasčių, dėl kurių draudėjo turtinis interesas gali nukentėti. Dėl to draudimo teisiniais santykiais užtikrinama, jog įvykus draudžiamajam įvykiui draudėjas bus tokioje pačioje turtinėje padėtyje, kurioje buvo prieš įvykstant draudžiamajam įvykiui, lygtais jo nebūtų buvę[8]. Tokios rizikos gali būti įvairios, pavyzdžiui: sveikatos sutrikimas nelaimingo atsitikimo pakeliui į darbą metu, turtiniai praradimai patirti dėl žemės drebėjimo, darbo sutrikimas dėl neveikiančios tinklų bei informacinės sistemos.

Kibernetinių rizikų draudimas priskiriamas prie turto draudimo sutarčių. Draudėjas sudarydamas kibernetinių rizikų draudimo sutartį suvokia, jog vykdant ūkinę veiklą naudojant informacines technologijas per tinklo ryšių sistemas egzistuoja kibernetinės rizikos dėl kurių apdraustasis gali patirti didelių nuostolių. Kibernetinės rizikos plačiąja prasme laikomos visi pavojai kibernetinėje erdvėje, dėl kurių gali atsirasti turtiniai nuostoliai. Kibernetinės erdvės sąvoka apima tinklo ryšių sistemomis valdomus elektroninius prietaisus bei elektroninių duomenų perdavimą, keitimą, laikymą ir naudojimą per tinklo ryšius[9]. Pavyzdžiui, kibernetinėmis rizikomis laikoma juridinio asmens darbo sutrikimas dėl neveikiančio interneto, elektroninių prietaisų sugadinimas dėl kenksmingos programinės įrangos, juridinio asmens internetinių tinklalapių nepasiekiamumas dėl DDoS (angl. *distributed denial of service*) atakų, aparatinės ir programinės įrangos užkrėtimas kenksminga programine įranga, tinklo ryšių, kompiuterių sistemų bei serverių veikimo sutrikdymas, dėl kibernetinių atakų įvykdytų prieš juridinį asmenį sumažėjusi juridinio

[8] Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus nutartis civilinėje byloje nr. 3K-3-911/2002.
[9] LOUKAS, George. Cyber-Physical Attacks, A growing invisible threat. 2015. P. 2.

asmens reputacija, juridinio asmens klientų bei darbuotojų privačios informacijos pasisavinimas ar praradimas, komercinių paslapčių bei informacijos susijusios su juridiniam asmeniui priklausiančia intelektine nuosavybe pasisavinimas ar praradimas, finansiniai nusikaltimai, turto prievartavimas kibernetinėje erdvėje.

Kibernetinės rizikos 2014 metais buvo priskiriamos tarp dešimties svarbiausių pasaulyje susiduriamų rizikų[10]. 2011 m. bendras pasaulio kibernetinių rizikų draudimo rinkos dydis buvo vertinamas daugiau nei vieno trilijono JAV dolerių[11]. O remiantis 2015 metų statistika vidutiniškai kiekviena JAV bendrovė kiekvienais metais dėl kibernetinių rizikų patiria 15,4 milijonus JAV dolerių nuostolių, Vokietijos bendrovė – 7,5 milijonų JAV dolerių, Japonijos – 6,8 milijonų JAV dolerių nuostolių[12].

Kibernetinių rizikų draudimo sutarties dalykas yra draudėjo turtinis interesas išvengti nuostolių atsirandančių dėl kibernetinių rizikų. Šio draudimo turtinis interesas įvardijamas nurodant turtą, kuris yra apdraudžiamas arba nurodant finansinius nuostolius nuo kurių apsidraudžiama. Nurodomas turtas gali būti materialus ir nematerialius, pavyzdžiui, duomenų bazės (elektroniniai duomenys), kuriose saugoma ūkio subjekto klientų bei darbuotojų asmeninė informacija, informacijos saugojimo laikmenos, elektroniniai prietaisai valdomi tinklo ryšių sistemomis.

Apdraudžiamas gali būti ne bet koks turtinis interesas, tačiau tik teisėtas bei įstatymo ginamas interesas[13]. Pavyzdžiui, negalima apsidrausti nuo pačios įmonės tyčinės kibernetinės atakos savo atžvilgiu arba suplanuoto duomenų bazės pravalymo, kai vėliau pastebima, jog ištrinta svarbi informacija. Kibernetinių rizikų draudimo sutartis sudaroma ne vartotojų, o verslininkų, savo srities profesionalų, kurie darbuotojų ar nepriklausomų ekspertų pagalba suvokia kibernetines rizikas bei turi pakankamai informacijos būti lygiaverčiu derybininku su draudiku, dėl to draudėjas nelaikytinas silpnesniąja sutarties šalimi. Priešingai, kibernetinių rizikų draudėjas gali tinkamai pasirūpinti savo interesų apsauga bei tinkamai įvertinti kibernetines rizikas, kurias pats draudėjas gali kontroliuoti investuojant į kibernetinio saugumo informacines technologijas bei darbuotojų

[10] Allianz Risk Barometer on Business Risks 2014. [interaktyvus]. [Žiūrėta 2016-03-10]. < http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2014_EN.pdf>.
[11] LEMOS, Robert, Should SMBs Invest in Cyber Risk Insurance? 2010. [interaktyus]. [Žiūrėta 2015-12-17] < http://www.darkreading.com/smb-security/167901073/security/ security-management/227400093/index.html>.
[12] Average costs of cyber crime in selected countries as of August 2015 (in million U.S. dollars). [interaktyvus]. [Žiūrėta 2016-03-02]. http://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/.
[13] Lietuvos Respublikos Civilinio kodekso 6.988 str. 4 d. Valstybės žinios, 2000, Nr.74-2262.

apmokymus bei tas kibernetines rizikas, kurių draudėjas negali kontroliuoti bei atitinkama apimtimi įsigyti kibernetinių rizikų draudimą.

Spaudoje rašoma apie daugybę atvejų, kai nuteka asmeninė klientų bei darbuotojų informacija, sutrikdomas tinklalapių veikimas, pasisavinami svetimi pinigai dėl kibernetinėje erdvėje atliktų neteisėtų veiksmų[14]. Ši rizika yra itin aktuali šias laikais, nes neįmanoma prognozuoti informacinių technologijų bei kibernetinių atakų pobūdžio kaitos ateityje. Vertinant kibernetinių rizikų paplitimą, reikia turėti omenyje ne vien tik tokias kibernetinių atakų situacijas, apie kurias yra aprašoma spaudoje, bet ir apie tokias kibernetines atakas, dėl kurių juridiniai asmenys nesiskundžia dėl įvairių priežasčių, kaip, jog pačios atakų aukos nežino apie įvykusią kibernetinę ataką, techniškai neįmanoma nustatyti subjektų rato, kuris yra atsakingas už padarytą turtinę žalą, arba nenorima informuoti apie įvyki, nes pats ūkio subjektas nesilaikė protingų kibernetinio saugumo užtikrinimo praktikos taisyklių, o tai sužinojus klientams bei potencialiems akcininkams viešosios nuomonės atstatymo apie bendrovę (angl. *public relations*) kaštai būtų per ne lyg dideli arba juridinio asmens reputacija iš vis būtų neatstatoma iki prieš kibernetinė atakos įvykimo momentą buvusį lygį.

Didžiausia problema, su kuria susiduria draudikai norintis teikti kibernetinių rizikų draudimo paslaugas yra informacijos trūkumas apie kibernetinių rizikų statistiką. Kibernetinės rizikos atsirado visai neseniai, t. y. tik tada, kai XIX a. 8 dešimtmečio pabaigoje masiškai paplito tinklo ryšių naudojimas ne tik tarp informacinių technologijų mokslininkų, bet tarp ūkio subjektų ir privačių vartotojų[15]. Interneto naujumas reiškia tai, jog kibernetinių rizikų draudimo rinka nėra visiškai susiformavusi. Trūksta informacijos apie kibernetinių rizikų statistiką, draudimo įmokų bei sumų apskaičiavimo tvarką, padarytos kibernetinės žalos nematerialiam turtui apskaičiavimo tvarką, draudimo finansinį atsiperkamumą. Pačios kibernetinių atakų aukos nėra linkusios viešai pranešti apie įvykusias kibernetines atakas, nes bijo savo reputacijos sumažėjimo, o praneša tik tada, kai pranešimas atsipirks finansiškai dėl gautos draudimo išmokos. Dėl šios priežasties kibernetinių rizikų draudimo rinkoje yra susidariusi tokia situacija, jog ne visų nuostolių kibernetinė rizika gali būti apdraudžiama. Pavyzdžiui, jeigu draudimo rūšis yra itin nauja kaip kibernetinių rizikų draudimas ir rinkoje nėra pakankamai aktuarinių duomenų dėl draudimo

[14] Barbarians at the Digital Gate. Its cyberattacks show the world the nature of the Chinese regime. [interaktyvus]. [Žiūrėta 2016-02-25]. <http://www.wsj.com/articles/SB10001424127887323701904578275920521747756>.
[15] The first ISP. [Interaktyvus]. [Žiūrėta 2016-02-25]. <http://www.indra.com/homepages/spike/isp.html>.

atsiperkamumo arba nėra pakankamai kvalifikuotų specialistų gebančių ištirti kibernetinių rizikų draudžiamuosius įvykius, draudėjai nesiūlys konkrečios rizikos draudimo. Be to, kibernetinės rizikos priklauso nuo technologinės pažangos, kuri vyksta ypatingai sparčiai ir nėra prognozuojama. Dėl to sunku iš anksto numatyti ir spręsti teisines bei technologines problemas su kuriomis bus susiduriama ateityje, todėl siūlydami kibernetinių rizikų draudimą draudikai rizikuoja draudimo taisyklėse palikti teisinių spragų.

Yra daugybė aplinkybių, kurios didina ūkio subjekto kibernetinę riziką bei kurias draudikas turi įvertinti rengdamas kibernetinių rizikų draudimo taisykles. Vertinant ūkio subjekto veiklos rūšį, jeigu veikla vykdoma ar yra aptarnaujama tinklo ryšiais, tai ji savaime yra potencialus objektas tapti kibernetinės atakos auka. Kitaip tariant, jeigu darbuotojai yra prisijungę prie interneto naudojant kompiuterį, kuriame saugoma bet kokia informacija elektroniniu pavidalu, toks ūkio subjektas yra potencialus kibernetinės atakos objektas. Pavyzdžiui, bendrovės didžioji verslo dalis apima veiklą vykdomą internetu (prekių pardavinėjimas internetu, naujienų portalas). Nustojus veikti bendrovės tinklalapiams dėl DDoS (angl. *distributed denial of service*) atakos iki to momento, kai svetainės bus atkurtos internetinė parduotuvė ar tinklaraštis neveiks. Dėl to draudėjo veikla priverstinai yra nutraukiama ir jam atsiranda nuostoliai negautų pajamų forma dėl verslo nutraukimo dėl trečiųjų asmenų kaltės. Kitas pavyzdys yra sveikatos įstaigos, kuriose kaupiama privati informacija apie pacientus (vardai, pavardės, asmens kodai, paslaugų apmokėjimo duomenys, kiti kontaktai). Įsilaužus į sveikatos įstaigos duomenų bazes bei pasisavinant privačią informaciją atakuotojas ją gali panaudoti neteisėtiems finansiniams tikslams: parduoti privačią informaciją tretiesiems asmenims nusikalstamiems tikslams, pasisavinti svetimus pinigus remiantis apmokėjimo duomenų informacija, panaudoti paciento duomenis kibernetinei atakai įvykdyti bendrovės atžvilgiu, kurioje dirba pats pacientas.

Kitos kibernetinę riziką didinančios aplinkybės yra dėl bendrovės organizacinių ir techninių priežasčių. Paprastai susiduriama su tokiomis situacijomis, kai ūkio subjektų vadovai, akcininkai ir darbuotojai neturi jokių žinių apie informacines technologijas ir dėl to nemato kibernetinių rizikų galimų neigiamų turtinių padarinių. Jeigu įvyksta kibernetinė ataka, vadovai yra linkę manyti, jog tai yra informacinių technologijų padalinio darbuotojų reikalas ir viską sutvarkys specialistai specializuojantis informacinių technologijų srityje. Tačiau tai yra labai ydinga praktika, nes kibernetinės atakos dažniausiai įvyksta panaudojant ne prietaisų spragas, o socialinę inžineriją, kurios tikslas yra apgauti darbuotojus melu ir manipuliacija išviliojant

prisijungimui prie bendrovės sistemų reikalingus duomenis[16]. Pavyzdžiui, darbuotojas gauna apsimestinį elektroninį laišką iš banko, kuriame melagingai pranešama, jog prie darbuotojo banko internetinės paskyros buvo bandoma prisijungti iš neatpažįstamos vietovės, todėl darbuotojo banko paskyra buvo užblokuota bei nurodomas telefono numeris, kuriuo reikia kreiptis norint atkurti banko paskyrą. Darbuotojui paskambinus nurodytu telefono numeriu atsiliepia tikras žmogus, kuris remdamasis socialiniuose tinkluose ar kita viešai prieinama informacija apie darbuotoją meluodamas ir manipuliuodamas darbuotojo neišmanymu siekia išgauti tikruosius banko prisijungimo duomenis. Dažniausiai socialinės inžinerijos atakos įvykdomos per naujus neapmokytus darbuotojus, kartais net per pačius bendrovių vadovus. Kai kurios kompanijos paprasčiausiai yra per mažos ir dėl to joms neapsimoka investuoti į kibernetinį saugumą bei turėti darbuotojų, kurie specializuotųsi kibernetinio saugumo srityje. O jei samdomi ekspertai, kurie įvertina kibernetinio saugumo lygį bendrovėje, paprastai atlieka savo darbą *checklist* sąrašo pagrindu neužtikrinant saugumo ateityje, taip sukeliant iliuziją, jog ūkio subjektas yra saugus nuo visų galimų kibernetinių atakų, įskaitant socialinę inžineriją.

Draudikas vertindamas kibernetinių rizikų pavojingumo laipsnį ir rengdamas draudimo sutarties taisykles turėtų įvertinti draudėjo pastangas apmokyti vadovus bei darbuotojus protingo elgesio kibernetinėje erdvėje taisyklėmis, o ne vien palikimą keliems informacinių technologijų skyriaus darbuotojams rūpintis kibernetiniu saugumu. Manytina jog nesant adekvačių reguliarių apmokymų, kurie apima visus bendrovės darbuotojus, draudimo rizika būtų tokia didelė, jog draudikams apskritai neapsimokėtų siūlyti šio draudimo. Reikėtų atsižvelgti į darbuotojus pagal jų užimamas pareigas kompanijoje bei turimą prieigą prie konkrečios informacijos. Paprastai kuo aukštesnės darbuotojo pareigos, tuo svarbesnę informaciją jis gali valdyti. Taip pat reikšminga aplinkybė yra ta ar darbuotojas gali įvykdyti darbo funkcijas ne tik darbdavio patalpose, bet ir ar kavinėje, namuose, panaudojant ne tik dardavio valdomus bet ir asmeninius prietaisus, asmeninius ryšio tinklus.

Internetinėje erdvėje nebėra svarbu kokio dydžio yra juridinis asmuo bei kokioje teritorijoje jis vykdo savo veiklą. Visais atvejais, jeigu prietaisai prijungiami prie interneto, reiškia tai, jog jie gali būti randami internete iš bet kurios pasaulio vietos pasinaudojant prietaisų,

[16] 2014 Cost of a Data Breach Study: Global Analysis, the Ponemon Institute, sponsored by IBM, May 2014.

prijungtų prie interneto paieškos įrankiais[17]. Veiklą vykdant tinklo ryšiais bendrovė tampa tarptautinė ir veikia visą parą, ji yra pažeidžiama atakų iš viso pasaulio, bet kuriuo paros metu. Teisinė sistema tampa nepajėgi kovoti su kibernetinėmis rizikomis dėl tarptautiškumo elemento, ypatingai dėl teisinių sistemų skirtumo, o dažniausiai net neįmanoma nustatyti atakuotojų tapatybės.

Kibernetinių rizikų ratas nuolatos platėja ir keičiasi kibernetinių atakų įvykdymo metodai. Paprastai dėl turimų ribotų kaštų technologija yra perkama penkerių, dešimties ar dvidešimties metų laikotarpiui. Tokia įranga palaipsniui tampa nesaugi, nes atrandami įrangoje esantys pažeidžiamumo taškai (angl. *vulnerabilities*), kurie vėliau ne visada laiku ištaisomi programinės įrangos atnaujinamu. Tačiau kiekviena ataka atsižvelgia į atnaujintą programinę įrangą panaudojant reversinę inžineriją ir sekanti kibernetinė ataka yra protingesnė už praeitą ataką. Pažymėtina, jog dauguma programinės įrangos gamintojų turi imunitetą dėl gamintojo atsakomybės taikymo dėl jų sukurtos programinės įrangos saugumo defektų. Kibernetines atakas vykdo ne vienas subjektas ar viena valstybė, jas gali vykdyti bet koks asmuo ar organizacija nepriklausomai nuo jo finansinių pajėgumų. Kuo toliau, tuo verslo erdvėje naudojami prietaisai pinga. Atakuotojui pajėgiant įsigyti identišką prietaisą, į kurį siekiama įsilaužti, atakuotojas praktikuojasi kaip nulaužti konkretų prietaisą. Laikui bėgant taip atrandami nauji pažeidžiamumo taškai. Vien išmaniųjų telefonų su „Android“ operacine sistema kenksmingos programinės įrangos paplitimas nuo 2012 iki 2013 metų siekė 2577 procentų. Darbuotojai turi po kelis asmeninius ir darbinius telefonus ir nešiojamus kompiuterius, kuriuose išsaugo su darbu susijusią informaciją. Ketvirtadalis Amerikiečių pameta savo mobiliuosius telefonus kiekvienais metais. Iš 800 tūkstančių pamestų ar pavogtų mobilių prietaisų 97 procentai prietaisų niekada nebuvo rasti. O kiekvieną savaitę JAV oro uostose pametama ar pavagiama po 12 tūkstančių nešiojamų kompiuterių[18]. Telefonuose laikoma ta pati informacija kaip ir kompiuteriuose ar debesyse, tačiau telefonai yra lengviau nulaužiami dėl jų mobilumo savybių, nes jie yra pametami ar pavagiami. Dauguma telefonų, nešiojamųjų kompiuterių ar duomenų laikmenų apskritai neturi slaptažodžių. Visa tai didina pametamų ir pavagiamų prietaisų skaičių, kuriuose yra informacija turinti vertę juodojoje rinkoje[19].

[17] Žr. <https://www.shodan.io/>.
[18] Mac Donnel Ulsch. Cyber threat. How to manage the growing risk of the cyber attacks.2014. P. 106.
[19] Cisco Systems Inc., “The Internet of Things,”. [interaktyvus]. [Žiūrėta 2016-02-15]. <http://share.cisco.com/internetof-things.html>.

Kiti kibernetinių nuostolių atsiradimo atvejai atsiranda dėl darbuotojų naivių veiksmų, įrangos, su kuria dirbama neišmanymo arba aparatinės ir programinės įrangos defektų. 2012 m. Jungtinėse Karalystėse veikiančios bendrovės „RBS“ programinės įrangos skirta pinigų operacijoms atlikti saugumo pažeidimas kainavo 125 milijonų svarų sterlingų vartotojams kompensacijoms išmokėti bei 56 milijonai svarai sterlingų padengti baudoms valstybės finansinio reguliavimo institucijoms[20]. O dėl Jungtinės Karalystės mokesčių inspekcijos (HM Revenue and Customs) darbuotojų kaltės 2007 m. buvo prarasti du kompaktiniai diskai (angl. *compact disk*), kuriuose buvo išsaugota elektroninė informacija apie 25 milijonus mokesčių mokėtojų, o Jungtinės Karalystės krašto apsaugos ministerijos darbuotojai prarado kietąjį diską (angl. *hard disk*), kuriame buvo daugiau nei 100 tūkstančio karių duomenys bei 600 tūkstančių kandidatų į kariuomenę asmeninė informacija[21].

Vertinant kibernetines rizikas baudžiamosios teisės kontekste pažymėtina, jog transnacionalinio organizuoto nusikalstamumo sąvoka apibrėžta Jungtinių Tautų Organizacijos konvencijoje prieš organizuotą transnacionalinį nusikalstamumą. Kibernetinės atakos priskiriamos prie nusikaltimų, kurie yra įvykdomi daugiau nei vienoje valstybėje arba nusikaltimai įvykdyti vienoje valstybėje, tačiau jie buvo suplanuoti ir pasiruošta kitoje valstybėje[22]. Šiuos finansinius nusikaltimus, lyginant su „tradiciniais“ nusikaltimais, kaip vagytė ar plėšimas yra sunku kontroliuoti. Teisės aktų leidimas savaime nereiškia kibernetinės rizikos kontrolę, nes nėra bendro organo, kuris galėtų įgyvendinti prieš kibernetines atakas nukreiptus įstatymus. Kibernetinės atakos paprastai naudoja atakuotojų duomenų užkodavimą (angl. *encryption*) bei „Tor“ programinę įrangą. „Tor“ įranga sukuria seriją užkoduotų tinklų, kurie atakuotojo naudai yra saugūs ta prasme, jog atakuotojo identifikacijos duomenys nėra tiesiogiai siunčiami į atakuojamą objektą, o naudojami paprastai trys kompiuteriai esantys skirtingose valstybėse. Tokia įranga leidžia atakuotojams prisijungti prie svetimų kompiuterių sistemų bei iš jų atsijungti nepaliekant pėdsakų.

Metodai, kurie naudojami įvykdyti kibernetines atakas pasižymi tam tikrais panašiais požymiais. Visų pirma, asmuo siekiantys įvykdyti kibernetinę ataką identifikuoja pažeidžiamumo

[20] http://www.bbc.co.uk/news/business-30125728

[21] Previous cases of missing data. BBC News. 2009. [interaktyvus]. [Žiūrėta 2016-03-05}. <http://news.bbc.co.uk/1/hi/uk/7449927.stm>.

[22] United Nations convention against transnational organized crime and the protocols thereto, United Nations, New York, 2004.

taškus, per kuriais tiesiogiai bus įmanoma komunikuotis su aktuatoriais ir davikliais arba netiesiogiai paveikti jų veikimą. Tam reikalinga konkreti informacija apie kibernetinės atakos objektą. Pirma, paprastai surenkama tokia informacija kaip objekto loginis adresas, naudojamos programinės įrangos rūšis bei versija, vidinės sistemos tinklo topologija, aparatinės įrangos rūšis bei versija, darbuotojų vardai, pavardės, elektroniniai paštai bei bet kokia kita reikšminga asmeninė informacija randama viešojoje erdvėje. Visa tai daugiausiai randama internete panaudojant „Google“ paieškos sistemą bei pasinaudojant tokiais tinklo įrankiais kaip, pavyzdžiui, nemokamai prieinama „Kali linux“ operacinės sistemos tinklo saugumo įrankių rinkinys arba „Microsoft Windows“ operacinės sistemos komandinės eilutės (angl. *command line interface*) tinklo pažinimo programomis. Internete randami naudojamos programinės ar aparatinės įrangos naudojimo vadovai, kuriuose aprašoma kaip naudotis prietaisu ar programa, kokie yra gamykliniai nustatymai bei gamyklinis vardas ir slaptažodis, kurie dažnai vartotojų nėra vėliau pakeičiami (pavyzdžiui, labai dažnas atvejis yra namuose naudojami maršrutizatoriai, kurie pajungiamia *plug and play* metodu).

Dažniausiai kibernetinių atakų rengėjai yra valstybės, o tokių grupuočių kaip „Lulszec“ ir „Anonymous“ JAV vyriausybės yra klasifikuotinos kaip tarptautinės teroristinės organizacijos, dėl to gali kilti problema dėl draudiko atsisakymo padengti teroristų organizuotų kibernetinių atakų nuostolius[23]. Dėl to reikėtų atsižvelgti į draudimo taisyklių formuluotes įvertinant tai ar jos apima teroristinius išpuolius.

Antra, naudojamos socialinės inžinerijos tikslas yra palengvinti priėjimą prie bet kokios sistemos, kurią operuoja žmonės. Galima apsimesti kitu žmogumi – bendradarbiu, šiukšlių dėžėje surasti išmestus dokumentus, gautame elektroniniame laiške gali būti klaviatūros paspaudimo registravimo kenksminga programa (angl. *keylogger*), atakuotojas gali surinkti informaciją apie darbuotojų darbo metu dažniausiai lankomus tinklalapius ir juose patalpina kenksmingą programinę įrangą.

Trečia, pažeidžiamumo taškų atradimas. Atlikus tyrimą pagaliau randamos įrangos klaidos arba programinės įrangos trūkumai per kuriuos galima patekti į bendrovės kompiuterių sistemą. Tai paprastai atliekama panaudojant tokią nemokamą programinę įrangą kaip „Nmap“, „Nessus“ ir „Wireshark“[24]. Šių programų pagrindu tikrinant kiekvieną individualų tinklo duomenų paketą

[23] FERILLO, Paul *et alia*. Cyber Security, Cyber Governance, and Cyber insurance. Harvard law journal. 2014.P. 9.
[24] Žr. <http://nmap.org>; <http://www.tenable.com/products/nessus>; <http://www.wireshark.org>.

galima nustatyti visų prie tinklo prisijungusių prietaisų specifikacija, t. y., pavyzdžiui, kokią operacinę sistemą naudoja atakuojamas objektas, tinklo topologija, neapsaugotus (angl. *unencrypted*) slaptažodžius, atvirus tinklo prievadus (angl. *ports*).

Ketvirta, įvykdomas įsilaužimas. Panaudojus visus atakuotojui prieinamus įrankius atakuotojas ištiria sistemą ir suranda silpnumo taškus, per kuriuos galima įsilaužti. Silpnumo taškai – tai jungtys tarp valdymo, komunikavimo, daviklių bei aktuatorių elementų. T. y. (1) komunikacijų kanalai per kuriuos perduodama daviklių surinkta informacija bei jais kontroliuojami aktuatoriai; (2) pagrindinio tinklo, įskaitant individualius kontroliavimo taškus kaip variklio valdymo kompiuteriai (angl. *engine control unit*), programuojami loginiai valdikliai (angl. *programmable logic controller*) ir panašiai; (3) komunikacijos kanalai arba prievadai tarp pagrindinio tinklo ir bet kurio antrinio vidaus tinklo, įskaitant kiberfizines sistemas, t. y. tokias sistemas, kurios valdomos tinklo ryšių sistemomis, bet kontroliuoja ne kompiuterius, o tokias fizines sistemas kaip vandentiekius, šilumos valdymo sistemas, daiktų internetą (angl. *internet of things*) ir pan.; (4) antriniai vidiniai tinklai ir jų susikirtimo taškai (paprastai bendro naudojimo kompiuteriai); (5) komunikaciniai kanalai tarp vidinių ir išorinių tinklų; (6) išoriniai tinklai, įskaitant internetą ir kitas kiberfizines sistemas.

Penkta, atakavimas. Pavyzdžiui, juodosios ir pilkosios skylės: tinklas užkraunamas su dideliu kiekiu srauto, kuris sustabdo bet kokių duomenų paketų siuntimą. Kodo įterpimas: kompiuterio tikslinė operacija yra vykdoma įprastai, tačiau kartu įterpiamas kenksmingas kodas, kuris yra vykdomas kartu su tikslinę operacija. Komandos įterpimas – asmuo turintis prieigą prie kompiuterio paleidžia kenksmingą komandą. T. y. priešingai negu kodo įterpimo atveju panaudota komanda jau yra egzistuojanti ir sukurta programos gamintojo, tačiau panaudojama kenksmingais tikslais. Komunikacijos spūstis – tyčinis įsikišimas į tinklo srautą su tikslu pažeisti tinklo srauto greitį. Atakuotojas turi būti bevielio tinklo ribose bei siųsti stiprų bevielį signalą tokiu pačiu dažniu, kurį naudoja draudėjas. Tinklo sutrikdymas (angl. *denial of service*) – nutraukia tinklo prieinamumą nusiunčiant į tinklą daugiau užklausų negu jis gali apdoroti. Pavyzdžiui, didžiausia ataka 2013 metais galėjo pasiekti 400 Gbps greitį[25]. Ši ataka taip pat naudojama, kad būtų iššvaistyta elektroninio prietaiso baterija. Į duomenų bazes/daviklius įskiepijami netikri duomenys – atakuotojas sutrikdo daviklių perduodamos informacijos kanalą, užblokuoja tikslinių daviklių

[25] LOUKAS, George. Cyber-Physical Attacks, A growing invisible threat. 2015. P. 161.

signalą ir siunčia netikrą informaciją. Kenksmingos programinės įrangos apkratas – tai gali būti virusai, loginės bombos, kirminai, trojos arkliai, slapti įėjimai (angl. *backdoors*) ir kt. Virusai – tai parazitinės programos, kurios apkrečia kitas programas kenksmingu kodu ir yra aktyvuojamos, kai apkrėstos programos yra paleidžiamos veikti. Kirminai – tai yra tas pats kas virusai, tačiau jie padaro žalą be kompiuterio vartotojo aktyvių veiksmų. *Backdoors* – tai programos, kurios įgalina atakuotojus be autentikacijos informacijos prisijungti prie svetimos sistemos. Trojos arkliai – tai yra programinė įranga, kuri yra iš esmės naudinga, tačiau kartu su minėta įranga yra paslėpta kenksminga programa. Slaptažodžių nulaužimas – atspėjant pagal dažniausiai naudojamus slaptažodžius, suradus viešai ir ne viešai internete prieinamose slaptažodžių duomenų bazėse, prievarta (angl. *brute force*) bandant visus galimus slaptažodžius iš eilės pagal atitinkamą protingą eiliškumą iš visų galimų simbolių kombinacijų.

Distributed denial of services atakos (DDoS) sukuria didžiausio lygio nepatogumus, tačiau jos yra vienintelės atakos, kurios visada yra iš karto pastebimos, o visas kitas atakas yra sunku pastebėti, kad jos vyksta. Priklausomai nuo kompanijos taikomos kibernetinės rizikos prevencijos programos lygio paprastai gali praeiti keli metai iki kada tokios atakos yra pastebimos. Nors kai kurie juridiniai asmenys atlieka internetinių technologijų atliekamų veiksmų monitoringą, t. y. renka bei išsaugo visą informaciją apie darbuotojų atliktus veiksmus naudojant informacines technologijas, tačiau tokios informacijos neanalizuoja ir nepalygina su įprastinės darbo dienos be kibernetinių atakų duomenimis, o tikrina tik po kibernetinių atakų. Nėra investuojama į kibernetinio saugumo sistemos palaikymą bei modernizavimą. Pavyzdžiui, juridinio asmens padaliniuose naudojama programinė įranga (angl. *software*) yra tinkama ir pakankama, jog darbuotojai įvykdytų savo darbo funkcijas, tačiau tokia programinė įranga yra pasenusi ir turi pažeidžiamumo taškų bei per jas gali būti nutekinama juridinio asmens privati komercinė informacija, intelektinės nuosavybės teisės ir panašiai. Tokiais atvejais juridinio asmens komercinė informacija yra kopijuojama palaipsniui mažomis dalimis. Tai reiškia, jog pagal išsiunčiamų duomenų srautą nepastebimomis dalimis yra kopijuojama informacija, kol per kelis mėnesius ar metus pasisavinama absoliučiai visa turima komercinė informacija bei panaudojama neteisėtais tikslais. Tokiu atveju žala nebegali būti atstatoma, o konkrečios padarytos žalos įvertinimas yra neįmanomas nei iš karto po kibernetinės atakos pastebėjimo nei ateityje, nes laiku nebuvo nustatytas kibernetinės atakos faktas. Nėra žinoma koks subjektas kada bei kokią informaciją nukopijavo, nėra žinoma kokia kenksminga programinė įranga buvo naudojama

kopijuoti informaciją bei kokia šios kenksmingos programinės įrangos kilmė. Ar apskaičiuoti žalą prireiks savaitės ar metų yra neįmanoma iš karto pasakyti[26]. Egzistuoja daug kintamųjų, kurie leidžia ištirti kibernetinę ataką. Kai kurios kibernetinės atakos įvykstą kartą, kai kurios pasikartoja periodiškai.

Draudėjas gali būti atakuojamas tiesiogiai arba netiesiogiai, pavyzdžiui, per darbuotoją, darbuotojo valdomą kompiuterį, kenksmingą automatizuotą kompiuterių tinklą (angl. *botnet*), trečiąjį asmenį, kuris nėra juridinio asmens darbuotojas, tačiau palaiko bendradarbiavimo ryšį su bendrove bei turi potencialią prieigą prie bendrovės tinklo, arba ataka gali kilti iš bendro pobūdžio viruso (angl. *wild virus*), kuris neturi jokio konkretaus taikinio, tačiau keliaudami tinklu nuolatos ieško sistemų, kuriuose yra žinomos ir nulaužiamos saugumo klaidos[27]. Įvykus atakai paprastai ji nėra pastebima iš karto, dažnai ji yra pastebima tik po kelių mėnesių, o kartais, kaip į vienos JAV restoranų įmonių grupės atveju įsilaužimas į mokėjimų sistemą buvo pastebėtas tik po devynių mėnesių[28].

1.2.Kibernetinių rizikų draudimo sutarčių atribojimas nuo kitų draudimo sutarčių rūšių

Vertinant kibernetinių rizikų draudimo vietą draudimo teisės sistemoje, reikia įvertinti verslo nutrūkimo draudimą, elektronikos prietaisų draudimą bei civilinės atsakomybės draudimą kaip panašias į kibernetinių rizikų draudimo rūšis, kurios gali būti naudojamos arba kartu su kibernetinių rizikų draudimu arba į minėtas draudimo sutartis įtraukiamos kibernetinių rizikų draudimo sutarties nuostatos.

Draudimo teisė yra privatinės teisės institutas. Verslo klientai, sudarantys draudimo sutartis kartu su draudikais yra lygiaverčiai rinkos dalyviai, vienodai išmanantys rinką arba gebantys pasisamdyti nepriklausomus ekspertus rinkos analizei atlikti. Dėl to šalys pačios susitaria dėl draudžiamųjų ir nedraudžiamųjų įvykių, tačiau remiantis sekančiame šio darbo skyriuje

[26] MAC DONNEL, Ulsch. Cyber threat. How to manage the growing risk of the cyber attacks.2014. P. 106.
[27] RAWLINGS, Philip. Cyber risk: insuring the digital age. Queen Mary University of London. 2015. P. 5.
[28] Travelers sues PF Chang's to avoid paying breach costs, Business Insurance, J. Greenwald 2014. [interaktyvus]. [Žiūrėta 2016-01-15]. < http://www.pfchangs.com/security/>.

analizuojama teismų praktika, vis dėl to ne visais atvejais tarp draudiko ir draudėjo yra vienodos pozicijos dėl kibernetinių rizikų draudimo sutarčių nuostatų, kuriose nurodomos rizikos, kurios yra apdraudžiamos, todėl svarbu, jog draudėjui tinkamai būtų paaiškintas draudimo sutarties turinys, o draudikas garantuotų bei pateiktų aiškų draudžiamųjų bei nedraudžiamųjų įvykių sąrašą su iliustracijomis.

Panašus draudimas lyginant su kibernetinių rizikų draudimu yra elektroninės įrangos draudimas. Šiuo draudimu draudikas padengia draudėjo nenumatytus nuostolius atsiradusius dėl elektroninės ir kompiuterinės įrangos sugedimo nuo tokių veiksmų kaip: vagystės, plėšimo, ugnies, sprogimo, drėgmės poveikio, potvynio, nekokybiškų medžiagų panaudojimo[29]. Tokiu draudimu paprastai nėra apsidraudžiama nuo kibernetinių rizikų. Pavyzdžiui, pagal ERGO Insurance SE Lietuvos filialo elektronikos draudimo taisykles draudikas neišmoka draudimo išmokos tais atvejais, kai žala yra nulemta dėl kompiuterinio viruso ar kitokios kenksmingos programinės įrangos[30].

Lyginant elektroninės įrangos draudimą su kibernetnių rizikų draudimu teigtina, jog draudimo objektai bei turtas, kuris yra apdraudžiamas, gali sutapti, tačiau skiriasi rizikos dėl kurių atsiranda nuostoliai. Kibernetinių rizikų draudime elektroninės įrangos gedimai yra nulemti kibernetinių rizikų. Pavyzžiui, dėl kibernetinių atakų, t. y. dėl trečiųjų asmenų tyčinių veiksmų, kurie panaudojant tinklo sistemų spragas padaro žalos draudėjui priklausantiems elektroninias prietaisams arba ne dėl kibernetinių atakų, tačiau dėl pačių draudėjo darbuotojų neatsargių veiksmų, dėl kurių buvo pažeista tinklo ryšiais valdoma sistema, kurios sugedimas lėmė draudėjo elektroninės įrangos netinkamą funkcionavimą, o to pasekoje visišką elektroninės įrangos sugadinimą. O elektroninės įrangos draudime draudžiamaisiais įvykiais pripažįstami tokie gedimai, kurie yra nulemti ne dėl kibernetinių rizikų, t. .y. ne dėl elektroninių prietaisų naudojimo per tinklo ryšių sistemas,o dėl įprastinių rizikų, su kuriomis susiduriama naudojant elektroninę įrangą įprastiniu būdu. Pavyzdžiui, dėl prietaisų svilimo, gaisro, drėgmės poveikio, nekokybiškų medžiagų panaudojimo ir kita.

Verslo nutrūkimo draudimo sutartimi draudikas įsipareigoja padengti draudėjo nuostolius patirtus dėl to, jog draudėjas dėl turto sugadinimo, sunaikinimo ar praradimo buvo priverstas

[29] ERGO Insurance SE Lietuvos filialo Elektronikos draudimo taisyklės Nr. 018. Galioja nuo 2014-08-01 4.1 punktas. Draudžiamieji įvykiai.
[30] Ibid 4.3 punktas m) dalis.

nutraukti verslą ir dėl to buvo negautos pajamos arba patirtos papildomos išlaidos dėl papildomo turto nuomos, elektroninių duomenų atstatymo išlaidos, papildomų darbuotojų samdymo išlaidos[31]. Pažymėtina, jog toks draudimas gali apimti verslo nutrūkimą ir dėl kibernetinių rizikų. Tačiau nėra aišku ar tokiu draudimu yra apdraudžiamas ir nematerialus turtas, kaip internetinės parduotuvės (svetainės) laikinas užblokavimas. Manytina, jog kibernetinių rizikų draudime turėtų aiškiai būti apibrėžtas materialaus ir nematerialaus turto atskyrimas. Turint omenyje, jog šiuo metu nėra vieningos teismų pozicijos dėl duomenų, kaip materialaus ar nematerialaus turto (apie tai diskutuotina šio darbo 2.1 dalyje).

Pagal vyraujančia praktiką paprastai civilinės atsakomybės draudimas apima draudėjo patirtų nuostolių atlyginimą tik tokiais atvejais, kai žala padaroma turtui, kuris laikomas materialiu, o nematerialus turtas nėra įtraukiamas į civilinės atsakomybės draudimo sutartį kaip draudimo objektas. Atsižvelgiant į kibernetinių rizikų draudimo sutarčių praktiką bei teismų pozicijas manytina, jog bendruoju civilinės atsakomybės draudimu draudėjas gali apsidrausti nuo kibernetinių rizikų neigiamų padarinių, tačiau dažnai kyla ginčai dėl draudimo sutarties konkrečių punktų aiškinimo, kurie yra nevisiškai aiškūs arba nėra detalizuoti atsižvelgiant į kibernetinių rizikų specifiką. Dėl to manytina, jog draudimo sutartyje šalys turėtų aiškiai apibrėžti tokias draudimo sutarties sąlygas kaip: ar pagal draudimo sutartį elektroniniai duomenys yra prilyginami materialiam turtui, ar elektroniai duomenys yra prilyginami nematerialiam turtui, tačiau nematerialų turtą draudikas įsipareigoja apdrausti. Todėl manytina, jog į civilinės atsakomybės draudimo sutartį galima inkorporuoti nuostatas dėl kibernetinių rizikų draudimo arba draudėjui būtų verta apsidrausti dviejų rūšių draudimu (civilinės atsakomybės bei kibernetinių rizikų draudimu).

Apibendrinant teigtina, jog draudimo teisė yra privatinės teisės institutas. Dėl to šalys yra pajėgios susiderėti dėl bet kokių draudimo sutarties sąlygų, išskyrus tas, kurias imperatyviai draudžia įstatymas. Manytina, jog kibernetinių rizikų draudimo sutarties nuostatos gali būti iš dalies inkorporuotos į civilinės atsakomybės, verslo nutrūkimo bei elektroninės įrangos draudimą arba naudojami keli skirtingų rūšių draudimai.

[31] ERGO Insurance SE Lietuvos filialo Verslo nutrūkimo draudimo taisyklės Nr. 058. Galioja nuo 2014-08-18. 9.1 punktas

2. Kibernetinių rizikų draudimo sutarties kvalifikavimo ypatumai

Draudimo sutarties sąvoka pateikiama Civilinio kodekso (toliau – CK) 6.987 straipsnyje, kuris draudimo sąvoka apibrėžia per draudimo sutarties turinį. Pagal CK 6.987 str. draudimo sutartis yra laikoma sutartimi, kurios viena šalis (draudikas) įsipareigoja už sutartyje nustatytą draudimo įmoką (premiją) sumokėti kitai šaliai (draudėjui) arba trečiajam asmeniui, kurio naudai sudaryta draudimo sutartis, įstatyme ar draudimo sutartyje nustatytą draudimo išmoką, apskaičiuotą įstatyme ar draudimo sutartyje nustatyta tvarka tuo atveju, jeigu įvyksta įstatyme ar draudimo sutartyje nustatytas draudžiamasis įvykis. Taigi įprastiniams draudimo teisiniams santykiams yra būdingi šie esminiai elementai: sutarties dalyviai (draudikas, draudėjas, trečiasis asmuo, kurio naudai sudaryta draudimo sutartis), draudimo įmoka (premija), draudimo išmoka bei jos apskaičiavimo tvarka, draudžiamieji įvykiai (rizika), turtas, kurį siekiama apdrausti, draudimo galiojimo laikotarpis. Toliau šio darbo dalyje bus išnagrinėti šie kibernetinių rizikų draudimo sutarties elementai.

2.1. Kibernetinių rizikų draudimo sutarties dalykas (objektas)

Kibernetinių rizikų draudimo sutarties dalykas yra draudėjo turtinis interesas išvengti turtinių nuostolių atsiradusių dėl kibernetinių rizikų. Šio draudimo turtinis interesas įvardijamas nurodant turtą, kuris yra apdraudžiamas. Tačiau kyla problemą dėl turto apibrėžimo, nes dėl kibernetinių rizikų žala gali būti padaromi ne tik materialiems objektams, tačiau ir nematerialiems objektams tokiais atvejais, kai prarandama ar pasisavinama kompiuterinėje atmintyje išsaugota informacija elektroninių duomenų pavidale.

Pažymėtina, jog šiuo klausimu nėra jokios Lietuvos Respublikos teismų praktikos, todėl daugiausiai dėmesio skiriama užsienio teismų praktikai, o ypatingai JAV teismų pozicijoms, nes

kibernetinių rizikų draudimo sutarčių praktika yra labiausiai išsivysčiusi būtent Jungtinėse Amerikos Valstijose.

Remiantis JAV teismų praktika šiuo metu nėra susiformavusi vieninga teismų pozicija dėl nematerialių objektų kaip draudimo sutarties objekto, teismų praktika nėra nuosekli ir susisteminta. JAV teismų praktikoje didžiausios problemos kyla vertinant komercinių civilinės atsakomybės (angl. *commercial general liability*) draudimo sutarčių nuostatas dėl elektroninių duomenų (angl. *computer data*) laikymo materialia nuosavybe bei vertinant ar elektroninių duomenų praradimas ar sunaikinimas laikomas turto praradimu.

Pažymėtina, jog JAV draudikų bendrovės vadovaujasi pozicija, jog komercinis civilinės atsakomybės draudimas nepadengia kibernetinių rizikų[32]. Remiantis standartinėmis komercinės civilinės atsakomybės draudimo taisyklėmis elektroniniai duomenys laikomi informacija, faktais ar programomis, kurios yra išsaugotos, sukurtos ar perkeliamos iš vieno kompiuterio į kitą, įskaitant kietuosius diskus, kompaktinius diskus, laikinąsias atmintines. O tokie duomenys nėra laikomi materialia nuosavybe[33].

Remiantis 1991 m. JAV teismų byla, kurioje draudėjas prarado kliento kompiuterinę juostą, teismas pripažino, jog draudikas privalo atlyginti ne tik sumą, kuri yra lygi kompiuterinės juostos vertei, bet sprendžiant žalos atlyginimo klausimą turi būti įvertinta ir kompiuterinėje juostoje esančios informacijos vertė, nes, teismo nuomone, išsaugota informacija laikytina materialaus objekto nuosavybės dalimi[34]. Vėliau 2001 m. elektroniniai duomenys (angl. *computer data*) pagal JAV teismų sprendimus buvo pripažinti nematerialiais objektais, motyvuojant tuo, jog kompiuteriniai duomenys negali būti paliesti, laikomi, ar juntami žmogaus pojūčiais; jie neturi jokios fizinės substancijos[35]. Teismas šiuo atveju turto materialumą aiškino per fizinio sąveikavimo funkciją. O dar vėliau, 2012 metais teismų laikytasi pozicijos, jog elektroniniai duomenys laikytini materialiais objektais, nes jie gali būti matomi bei keičiami žmogaus veiksmais[36].

---

[32] Insurers fight to bar cyber coverage under commercial general liability policies. Business Insurance, J. Greenwald. 2014. [interaktyvus]. [Žiūrėta 2016-01-18]. < http://www.businessinsurance.com/article/20141026/NEWS07/141029850/insurers-fight-to-bar-cyber-coverage-under-commercial-general>.

[33] Ibid.

[34] Court of Appeals of Minnesota. Retail Systems v. CNA Ins. CompaniesAnnotate this Case 469 N.W.2d 735 (1991).

[35] United States District Court, W.D. Oklahoma. STATE AUTO PROPERTY AND CASUALTY INSURANCE COMPANY, Plaintiff, v. MIDWEST COMPUTERS & MORE, Defendant. 147 F. Supp. 2d 1113 (2001).

[36] United States District Court of Louisiana. Landmark American Insurance Company v. Gulf Coast Analytical Laboratories, Inc., No. 3:2010cv00809 - Document 45 (M.D. La. 2012).

Teismui vertinant komercinių civilinės atsakomybės draudimo sutarčių nuostatas buvo konstatuota, jog fizinė žala nėra apribojama vien tik fizinės žalos padarymu materialiai kompiuterinei įrangai, bet į žalą įeina ir negalėjimas tam tikrą laiką prieiti prie elektroninių duomenų, negalėjimas jais naudotis. Taip pat duomenų ištrynimas buvo pripažintas fizinės nuosavybės sunaikinimu[37].

Vienoje iš bylų draudžiamasis įvykis įvyko dėl atakuotojo paleisto viruso, dėl kurio bendrovė buvo priversta pakeisti kompiuterį bei iš naujo įvesti duomenis. Teismas tokį įvyki pripažino draudžiamuoju bei įpareigojo draudiką išmokėti draudimo išmoką padengiančią duomenų įvesties kaštus[38]. Kitas draudžiamasis įvykis, kuriuo metu dėl atakuotojų kaltės buvo pasisavinta klientų privati informacija, bendrovei pagal teko pareiga pranešti kiekvienam klientui individualiai dėl įvykusios kibernetinės atakos bei pasamdyti viešųjų ryšių ekspertus reputacijos žalai sumažinti. Tokio įvykio nuostoliai teismo buvo pripažinti kaip padengtini kibernetinių rizikų draudimo[39].

Vertinant tai, jog nėra vieningos teismų praktikos dėl nematerialaus turto kaip draudimo objekto, tais atvejais, kai prarandami elektroniniai duomenys nesiejant tokių duomenų praradimo su fizinių objektų sugadinimu, teigtina, jog siekiant užtikrinti teisinį aiškumą bei išvengti ginčų, kylančių dėl šalių skirtingo draudimo objekto suvokimo bei aiškinimo, kibernetinės rizikos draudimo taisyklėse draudikas turėtų aiškiai išskirti apdraudžiamą materialų ir nematerialų turtą, kartu pateikiant rizikų pavyzdžius nurodant kokiais metodais kibernetinės rizikos padaro žalą konkrečiam materialiam ir nematerialiam turtui.

2.2. Kibernetinių rizikų draudimo rizika bei draudžiamieji įvykiai

Žodis “rizika” kilo iš italų kalbos žodžio „risco“ arba „rischio“, kas reiškė pavojų, riziką. Dabartinis tarptautinis žodžių žodynas riziką apibrėžia kaip tikimybę, jog įvyks kažkas blogo ar

[37] NMS Services, Inc v Hartford 62 Fed Appx 511 (CA4 (Va), 2003).
[38] Lambrecht & Associates, Inc v State Farm Lloyds 9 119 SW3d 16 (Tex App,2003).
[39] Retail Ventures, Inc v National Union Fire Ins Co of Pittsburgh, Pa 691 F3d 821 (CA6 (Ohio), 2012).

netikėto arba kažkas (žmogus ar įvykis) sukels neigiamus arba neplanuojamus padarinius. Rizika vienu atveju gali reikšti ateityje įvyksiančius veiksnius, kurių tikimybė įvykti yra reali ir ją galima apskaičiuoti, tačiau nėra žinoma kada rizika materializuosis.

Draudimo sutartis yra rizikos sutartis. Viena iš sutarties sudarymo sąlygų yra ta, jog šalys nežino kada įvyks draudžiamasis įvykus bei apskritai ar jis įvyks draudimo sutarties galiojimo laikotarpiu. Tai yra esminė draudimo sutarties sąlyga, todėl jos nenurodžius arba nurodžius tokią riziką, kuri draudėjo žinioje tikrai įvyks, sutartis laikoma nesudaryta. Draudimo įstatymo 2 str. 26 p. draudimo riziką apibrėžia kaip tikėtiną pavojų, gresiantį draudimo objektui.

Draudėjas suvokia, jog egzistuoja tam tikri pavojai, nuo kurių draudėjas negali apsisaugoti, jų kontroliuoti bei išvengti jų sukeliamų pasekmių. Šie pavojai materializuodami įvairiais būdais draudėjui gali sukelti nesuplanuotus neigiamus turtinius padarinius. Pavyzdžiui, klientų informavimo kaštai dėl trečiųjų asmenų privačios darbuotojų ir klientų informacijos pasisavinimo ar praradimo, programinės ir aparatinės įrangos sugedimas ar praradimas ir kt. Dėl to draudėjas siekia išvengti neigiamų turtinių rizikos padarinių sudarydamas kibernetinių rizikų draudimo sutartį.

Bazelio Bankų Stebėjimo komitetas (angl. *Basel Committee on Banking Supervision*) išskiria operacinę riziką kaip vieną iš specialių rizikos rūšių, su kuria susiduria ūkio subjektai vykdantys ūkinę komercinę veiklą. Operacinė rizika – tai praradimų rizika kylanti dėl neadekvačių ar netinkamai atliktų vidinių procesų (žmonių ir sistemų klaidų) ar dėl išorinių trečiųjų asmenų veiksnių. Nepaisant to, jog šis apibrėžimas buvo sukurtas bankų veiklai, toks apibrėžimas tinka bet kokiai ūkinei komercinei veiklai[40]. Nors Bazelio Bankų Stebėjimo komitetas pateikia operacinės rizikos apibrėžimą, tačiau nepateikia gilesnio paaiškinimo, ką šioje sąvokoje reiškia žmonės, procesai, sistemos ir išoriniai veiksniai, t. y. nekonkretizuojamos aplinkybės, kurios laikomos operacinėmis rizikomis. Šiuos reiškinius apibrėžia doktrina.

Žmonių rizikos veiksmai apima apgavystes (angl. *fraud*), neautorizuotą veiklą (pavyzdžiui, kompiuterių sistemų tikrinimas darbuotojo, kuris nepriklauso informacinių technologijų personalui), netinkamą darbuotojų priežiūrą bei netinkamus darbuotojų apmokymas apie dažniausiai susiduriamas rizikas konkrečioje ūkinėje veikloje. Rizika kylanti dėl procesų apima klaidas dėl pinigų pervedimų, netinkama informacijos dokumentacija. Sistemų rizika apima sistemų diegimo bei priežiūros klaidas (pavyzdžiui, informacinėje sistemoje nebuvo įdiegtas

[40] BLUNDEN, Tony and THIRLWELL, John. Mastering operational risk. 2010. P. 8.

naujausias programinės įrangos atnaujinimas, dėl to sistemoje liko viešai žinomos saugumo ar funkcionalumo klaidos). Išoriniai trečiųjų asmenų veiksmai apima rizikas, susijusias su asmenų veiksmais, kurie nėra įmonės darbuotojai ar jiems prilyginami asmenys (verslo partneriai), o būtent išoriniai veiksmai apima trečiųjų asmenų nusikalstamas veikas (bandymai manipuliuojant ir meluojant darbuotojams išvilioti privačią informaciją, DDoS atakos ir kt.), konkurenciją, gamtos nelaimes (ryšių sutrikimas dėl audros), teisinės veiklos reglamentavimą.

Draudžiamojo įvykio sąvoką apibrėžia draudimo įstatymo 2 str. 33 d. pagal kurį draudžiamasis įvykis yra draudimo sutartyje nurodytas atsitikimas, kuriam įvykus draudikas privalo mokėti draudimo išmoką. Tai reiškia, jog įvykus draudžiamajam įvykiui yra realizuojama rizika nuo kurios apsidraudžia draudėjas bei ji materializuojasi nuostolių pavidale bei tarp realizuotos rizikos bei draudžiamojo įvykio yra priežastinis ryšys[41]. Kibernetinių rizikų draudime aktuali yra priežastinio ryšio teorija, kuri teigia, jog jeigu rizika, kuri nėra apdrausta nulėmė draudžiamąjį įvykį, kurio rizika yra apdrausta ir tai lėmė nuostolių atsiradimą, tai draudikas nėra įpareigotas išmokėti draudimo išmoką, nes tarp apdraustos rizikos bei veiksmo, lėmusio rizikos realizavimą nėra faktinio priežastinio ryšio. Pavyzdžiui, juridinio asmens padalinio darbuotojas išjungė kelioms minutėms tinklo saugumo įrangą tam, kad galėtų greičiau įvykdyti tinklo maršrutizatorių konfigūraciją.

Draudikas draudimo taisyklėse nurodo draudžiamųjų įvykių apibrėžimą bei nebaigtinį sąrašą. Tačiau pažymėtina, jog visų draudžiamųjų įvykių draudimo sutartyje nurodyti nėra įmanoma, nes kibernetinėje erdvėje jie nuolatos kinta, todėl manytina, jog praktiškiausia draudimo sutartyje nurodyti baigtinį nedraudžiamųjų įvykių sąrašą, kaip tai numato draudimo įstatymo 92 str. 1 d. 3 p., o draudžiamuosius įvykius apibrėžti abstrakčiai atsižvelgiant į įvykdomų kibernetinių atakų metodus.

Draudimo rizika materializuojasi per kibernetines atakas. Remiantis 2013 metų statistika metodai, kuriais įgyvendinamos kibernetinės atakos bei padaroma daugiausiai nuostolių pasiskirstė taip: iš visų atakų 21 % sudarė DDoS (distributed denial of service) atakos, 21 % sudarė piktadariškas kodas (angl. *malicious code*), 13 % sudarė į tinklalapius nukreiptos atakos (angl. *web based attacks*), 11 % sudarė socialinės inžinerijos ir sukčiavimo (angl. *phising*) atakos, 9 % sudarė

[41] KONTAUTAS, Tomas. Draudimo sutarčių teisė. Vilnius. 2007 m. P. 70.

pavogti elektroniniai prietaisai, 8 % sudarė kenksmingi darbuotojų veiksmai, 7 % žalinga programinė įranga, 5 % virusai, trojanai ir kirminai, 5 % sudarė botinklai (angl. *botnet*)[42].

Kibernetinių atakų rengėjų motyvai gali būti labai įvairūs. Paprastai tai yra asmeninė finansinė nauda, teroristiniai išpuoliai, šnipinėjimas (pavyzdžiui, 2009 m. įvykdytas Irano atominės industrijos šnipinėjimas Stuxnet kirminu, kurio metu panaudojant ataką greitai besisukančios centrifugos skirtos iš urano rūdos išskirti urano 235 izotopą buvo priverstos sugesti[43]), darbuotojų ar vartotojų protestavimas prieš bendrovę (pavyzdžiui, DDoS atakų nukreipimas į paslaugų tiekėjo serverius).

Juridinis asmuo, kurio atžvilgiu buvo įvykdyta kibernetinė ataka gali patirti įvairių nuostolių, kurie pasireiškia tokiais būdais: duomenų bazės atkūrimu rankiniu būdų darbuotojams surinkus ir suvedus tą pačią informaciją, kuri buvo prarasta, programinės ar aparatinės įrangos gamyklinių parametrų atstatymas bei įrangos atkūrimas į tokią padėtį, kuri buvo prieš ataką, atakos atlaikymo kaštai (pasipriešinimas atakai, protokolų rengimas, identifikavimas), klientų, kurių privati informacija buvo pasisavinta informavimas, viešieji ryšiai dėl reputacijos valdymo, pagalba dėl tapatybės pasisavinimo nusikaltimų, pavogti pinigai, sukčiavimas, išpirkos prašymas dėl duomenų grąžinimo ar atkodavimo, jei tokie duomenys buvo užkrėsti specifinės kenksmingos programinės įrangos (angl. *ransomware*). Pavyzdžiui, teismų praktikoje pripažįstama, jog sąjungos narių informacijos neapsaugojimas nuo kibernetinės atakos, kuri lėmė narių su tapatybės pasisavinimu susijusių nusikaltimų įvykdymą[44].

Atkreiptinas dėmesys, jog įvykus kibernetinei atakai draudėjo pardavimai bei akcijų kaina rinkoje paprastai sumažėja, nes sužinojus apie atskleistas ir panaudotas saugumo spragas sumažėja klientų pasitikėjimas bendrove. Nuo viso to padidėja tikimybė bendrovei laikinai nutraukti ūkinę veiklą arba net bankrutuoti. Taip pat pažymėtina, jog, JAV rinkoje juridiniai asmenys, kurie pardavinėja savo akcijas viešojoje rinkoje, pagal „Standarts and Poor‘s“ financinių paslaugų bendrovę, kuri vertina JAV akcijų bei obligacijų rinkos vertę, tie JAV bankai, kurie nėra

[42] Cost of Cyber Crime: United States, Ponemon Institute. 2013. [interaktyvus]. [Žiūrėta 2016-03-01]. <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf>.
[43] WATERMAN, S. ‘US-Israeli cyberattack on Iran was “act of force”, NATO study found’, Washington Times. 2013. [Interaktyvus]. [Žiūrėta 2016-03-01]. <http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-oniran-was-act-of-force-na/?page=all>.
[44] State of Michigan Court of appeals. Audrey Bell vs. Dentry Berry. 2005.

apsidraudę savo veiklos kibernetinių rizikų draudimu, automatiškai praranda atitinkamus balus akcijų vertės S&P reitingavimo sistemoje[45].

2013 m. JAV bendrovės vykdančios mažmeninę prekybą „Target“ mokėjimų sistema buvo apkrėsta žalinga programine įranga (angl. *malware*), dėl kurios atakuotojai įgijo 40 milijonų „Target“ klientų asmeninę informaciją, tarp kurios buvo bankinių mokėjimų kortelių informacija. Dėl šios kenksmingos programinės įrangos kiekvienas „Target“ klientas, esantis debitinių kortelių vartotojas patyrė po 331 JAV dolerių nuostolių, o kreditinių kortelių vartotojai patyrė po 530 JAV dolerių nuostolių. Bendrovė klientų ir bankų buvo paduota į teismą, o „Target“ pelnas nukrito 46 procentais, pardavimai sumažėjo, o generalinis direktorius atsistatydino[46].

Į kibernetines rizikas taip pat įeina kiberfizinės atakos. Tai kibernetinės atakos, kurių tikslas yra kontroliuoti fizinius objektus tinklo ryšių sistemomis (vandens sistemas, medicininius implantus, automobilius, degalų tiekimo vamzdžius ir pan.) neturint tam leidimo[47]. Nors kiekviena kibernetinė ataka turi padarinius fiziniams objektams, tačiau šiuo atveju fiziniai objektai suprantami tiesiogine siauriąja prasme, t. y. fiziniai objektai, kurie yra sumodeliuoti taip, kad juos kontroliuoti galima būtų pasinaudojant ryšių tinklus.

Pažymėtina, jog kibernetinių rizikų draudimo sutartis priskiriama privatinės teisės institutui, kuriai galioja taisyklė, jog viskas yra leidžiama išskyrus tai, kas įstatymo imperatyviai uždrausta. Dėl to draudikai turi labai plačią teisę su draudėju susitarti dėl draudimo sutarties sąlygų, o konkrečiai sutarties sąlygas daugiau lemia ne įstatymų nuostatos, o draudėjo leidžiami kaštai kibernetiniam saugumui užtikrinti investuojant į informacines technologijas ir darbuotojų mokymus. O didžiausi ginčai tarp draudiko ir draudėjo teismų praktikoje kyla dėl to, jog šalys nėra pakankamai detalizavusios draudžiamųjų įvykių atvejus[48].

Svarbi aplinkybė, kurią reikėtų įvertinti parengiant draudimo taisyklių nuostatas yra ta, jog reikia atsižvelgti ar darbuotojai prie draudėjo tinklo gali prisijungti tik iš darbovietės ar savo darbą gali vykdyti ir iš namų, kavinės ir pan. Ar prisijungimas iš ne darbovietės yra paprastas

[45] S&P to consider cyber security in bank credit ratings. 2015. [interaktyvus]. [Žiūrėta 2016-03-01] <http://www.ft.com/fastft/2015/09/29/sandp-consider-cyber-security-bank-credit-ratings/>.
[46] American Bankers Association, Target Breach Impact Survey. 2014. [Interaktyvus]. [Žiūrėta 2016-03-01] < http://www.aba.com/Tools/Function/Payments/Documents/TargetBreachBankImpact.pdf>.
[47] LEE, E. A. Cyber physical systems: Design challenges. 2008. P. 363.
[48] Is Computer Data "Tangible Property" or Subject to "Physical Loss or Damage"? Michael Rossi. 2001. [Interaktyvus]. [Žiūrėta 2016-03-03]. <https://www.irmi.com/articles/expert-commentary/is-computer-data-tangible-property-or-subject-to-physical-loss-or-damage-part-1>.

prisijungimas ar sukuriant virtualų privatų tinklą (angl. *virtual private network*)? Taip pat reikia įvertinti ar darbuotojai gali prie darbdavio tinklo prisijungti tik per asmeninius kompiuterius ar ir per asmeninius mobiliuosius telefonus, planšetinius kompiuterius. Kuo yra mažesnė darbdavio kontrolė bei mažesnis laipsnis numatyti kaip ir kokios informacinės technologijos ir kur jos bus naudojamos gali lemti didesnę riziką. Tai įvertinus draudikas turėtų atsisakyti sudaryti draudimo sutartį ar pasiūlyti didesnę premijų dydį.

Antra, reikia įvertinti kokiais atvejais darbo nutraukimą draudikas laikys kaip draudžiamąjį įvykį. T. y. (a) ar bus padengtas ūkinės veiklos sustabdymas tik už tą laiką, kurio metu bendrovė negalėjo vykdyti savo veiklos dėl atakuotojo kaltės, (b) ar draudžiamuoju įvykiu bus laikytinas ir tas laiko tarpas, kurio prireikė pačiam draudėjui atstatyti savo veiklą, (c) ar draudimo išmoka apims ir tą laiką, kuriuo metu teisėsaugos institucijos baigs ištirti kibernetinę ataką ir leist tęsti veiklą.

Trečia, ar draudimo taisyklės apims tokius draudžiamuosius įvykius, kai nutrūksta draudėjo ūkinė veikla dėl interneto paslaugų tiekėjo kaltės (angl. *internet service proveder*)? Ar draudžiamasis įvykis laikomas ryšio sutrikimu dėl (a) „tier 1“ lygio tinklo ryšių savininkų (b) ar dėl „tier 2“ lygio tinklų ryšių savininkų interneto tiekėjų, kurie yra suteikę draudėjui interneto paslaugų tiekimą.

Ketvirta, draudimo taisyklėse aiškiai reikėtų apibrėžti prieš ką nukreiptas kibernetines atakas draudžia draudikas. Ar draudžiamuoju įvykiu laikytini atvejai, kai kibernetinės atakos įvykdomos per (a) vadovų valdomus elektroninius prietaisus, ar (b) atitinkamas pareigas einančius darbuotojų valdomus elektroninius prietaisus, ar (c) atakas nukreiptas prieš visus darbuotojus. Ar draudikas vertina darbuotojus pagal jų informacijos prieinamumo laipsnį? Ar draudžiamuoju įvykiu laikomas nuostolių atsiradimas dėl asmenų kaltės, kurie nėra draudėjo darbuotojai ar jais prilyginami asmenys, tačiau jie buvo draudėjo darbuotojai ar kitokiu teisniu pagrindu turėjo prieigą prie draudėjo žinioje esančios informacijos, tačiau dėl jų kaltės draudėjo sistemoje atsirado saugos spragų? (buvęs darbuotojas parduoda ankščiau naudotus slaptažodžius).

Penkta, ar draudimo taisyklės apima išpirkos išmokėjimą atakuotojui dėl atakos nevykdymo, užkoduotų duomenų atkodavimo, apkrėstos sistemos atkūrimo, ar griežtai atsisako vykdyti derybas dėl išpirkos išmokėjimo.

Šešta, ar dėl draudžiamosios išmokos galima kreiptis tik tuo atveju, kai draudžiamasis įvykis įvyko draudimo sutarties galiojimo momentu, bet ar į draudiką dėl draudžiamosios išmokos išmokėjimo galima kreiptis sutarties galiojimui pasibaigus, tokiu atveju, kai įrodoma, kad

draudžiamasis įvykis draudimo sutarties galiojimo metu, tačiau kibernetinė ataka buvo pastebėta tik draudimo sutarčiai pasibaigus. Pavyzdžiui, „Red October“ kenksmingos programinės įrangos ataka[49] buvo nepastebėta penkerius metus, dėl to iškilo problema kaip reikėtų teisiškai vertinti draudėjo suvokimą, kad prieš jį yra vykdoma kibernetinė ataka. Iš vienos pusės, draudėjas turi pareigą pranešti draudikui apie draudžiamąjį įvykį, tačiau tik tais atvejais, kai draudėjas suvokia, jog ataka yra vykdoma prieš jį. Manytina, jog draudėjas pats turėtų būti atsakingas dėl draudžiamojo įvykio fakto (vykdomos kibernetinės atakos) atskleidimo draudimo sutarties galiojimo metu. Draudėjas turėtų elgtis protingai, t. y. reguliariai atlikti bendrovės kibernetinio saugumo monitoringą bei nenutraukti draudimo sutarties neįsitikinus, jog jis nėra kibernetinės atakos objektu.

Viena iš rizikų, kuri yra aktuali bet kuriam ūkio subjektui yra reputacinė rizika. Reputacinės rizikos atveju nėra padaroma tiesioginė žala ūkio subjektui, tačiau žala pasireiškia klientų sumažėjusiu pasitikėjimu bendrove kaip prekių ir paslaugų tiekėju. Yra atvejų, kai įsilaužus į serverį, kuriame talpinamas tinklalapio turinys sutrikdoma įprastinio svetainės savininko turinio skelbimo veikla ir turinys yra pakeičiamas įprastinį svetainės vartotoją atgrasantį ar įžeidžiantį turinį, kaip pornografija, žiaurūs vaizdai ar kitas nelegalus interneto turinys. Tai yra laikoma viena iš didžiausių rizikų dėl kurios gali sužlugti verslas.

Kita prieš juridinio asmens reputaciją nukreipta rizika yra ta, jog klientai nepatenkinti pardavėjo veikla organizuoja veiką, kurios metu surenkamas būrys žmonių, kurie visi kartu, iš anksto sutartu laiku savo naršyklėse atsidarys pardavėjo tinklalapį. Taip užkraunamas pardavėjo tinklalapis tokiu dideliu srautu, jog tinklalapį talpinantys serveriai bei tinklų ryšiai nėra pajėgūs patenkinti visų svetainės vartotojų užklausas. Dėl to pardavėjo tinklalapio veikimas yra sustabdomas iki atakos pabaigos ir pardavėjas negali toliau vykdyti savo veiklos. Tokia praktika teisiniu požiūriu nėra laikoma legalia, tačiau atsižvelgiant į tokios DDoS atakos specifiką atakuotojų yra tūkstančiai skirtingų asmenų, kurių paprastai neįmanoma susekti ir apkaltinti. Dėl to svetainės savininkas turi tik kelis galimus sprendimus sumažinti šią riziką: serverių bei tinklo

[49] Kaspersky Lab Identifies Operation “Red October,” an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide. 2013. [interaktyvus]. [Žiūrėta 2016-03-03]. <http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide?ClickID=clzvvllsepsiffqeknvqxa4x4vqkwvslznqn>.

ryšių sustiprinimas (galingesnės aparatinės įrangos pirkimas), programinės įrangos nukreiptos prieš tokią veiklą įsigijimas, kibernetinių rizikų draudimo įsigijimas.

Vertinant draudimo sutartyje apibrėžiamas draudimo rizikas, manytina, jog negalima kibernetinių rizikų draudimo taisyklių apibrėžti abstrakčiai tokiu būdu, kaip „draudėjas kibernetinėje erdvėje privalo elgtis protingai, jog jo duomenų saugumas būtų užtikrintas“, o kiekviena rizika turėtų būtų įvardinta bei aprašyta konkrečiai, su iliustracijomis. Tokiu būdu draudėjas suvoktų rizikas, nuo kurių jis yra apdraudžiamas ir vėliau tarp draudiko ir draudėjo nekiltų ginčų.

2.3. Kibernetinių rizikų draudimo sutarties dalyviai

Draudimo sutarties dalyviai yra draudikas, draudėjas, trečiasis asmuo, kurio naudai sudaroma draudimo sutartis, nukentėjęs trečiasis asmuo, apdraustasis asmuo. Draudikas yra draudimo sutartį sudarantis ar sudaręs asmuo, teisės aktų nustatyta tvarka turintis teisę vykdyti draudimo veiklą[50], kuriam pagal draudimo sutartį atsiranda sutartinė pareiga suteikti draudimo apsaugą ir įvykus draudžiamajam įvykiui sumokėti draudimo išmoką. Draudikų veikla yra griežtai reglamentuojama ir draudiku gali būti tik toks asmuo, kuriam priežiūros institucijos (Lietuvos Banko) nutarimu suteikta draudimo veiklos licencija. Draudiko įstatinis kapitalas negali būti mažesnis kaip 1 000 000 Eurų[51]. Teisės doktrinoje manytina, jeigu draudikas neturi licencijos, tačiau sudaro draudimo sutartį, tokiu atveju laikoma, jog draudikas, nors ir elgėsi nesąžiningai, tačiau pagal CK 1.83 str. 1 d. yra atsakingas draudėjui dėl savo, kaip fiktyvaus draudiko pareigų vykdymo bei privalo atlyginti iš sutarties kylančią pareigą draudėjui bei atsakyti administracine tvarka[52].

Draudėjas yra asmuo, kuris sudarė draudimo sutartį su draudiku[53]. Draudėjas ne visada yra tas asmuo, kurio rizikos yra apdraudžiamos. Paprastai draudimo sutartyje nurodomas asmuo, kuris

[50] Lietuvos Respublikos Draudimo įstatymo 2 str. 8 d. Valstybės žinios, 2003, Nr. 94-4246.
[51] Ibid 33 str. 1 d.
[52] Lietuvos Respublikos Administracinės teisės pažeidimų kodeksas 173 str. Valstybės žinios, 1985, Nr.1-1.
[53] Ibid 1 str. 7 d.

yra apdraudžiamas (apdraustasis asmuo arba trečiasis asmuo). Tačiau jeigu tai nenurodoma, preziumuojama, jog apdraudžiamas yra pats draudėjas. Draudėju bei trečiuoju asmeniu, kurio naudai sudaroma draudimo sutartis gali būti bet kuris fizinis arba juridinis asmuo. Teisę reikalauti išmokėti draudimo išmoką iš draudiko savarankiškai turi draudėjas, apdraustasis, nukentėjusysis trečiasis asmuo, taip pat trečiasis asmuo, kurio naudai sudaryta draudimo sutartis.

Kibernetinės rizikų draudimo sutarties dalyviai yra draudikas, draudėjas, apdraustasis, taip pat trečiasis asmuo, kurio naudai sudaroma draudimo sutartis. Šios rūšies draudimo sutarčių atveju abi šalys yra savo sritį išmanantys profesionalai, dėl to kibernetinių rizikų draudimo sutartis negali būti laikytina vartojimo sutartimi, o šalys laikytinos lygiaverčiais vienodą derybinę galią turinčiais ūkio subjektais, esantys vienodai atsakingi už draudimo sutarties sąlygų suderinimą.

Kibernetinių rizikų draudėjai kaip ir draudikai paprastai yra didelės kompanijos, vykdančios ūkinę veiklą ir turinčios savo padalinių įvairiose pasaulio valstybėse, todėl kyla klausimas kokią veiklos teritoriją turi apimti draudimo sutartis? Tarkime, jeigu draudėjo pagrindinė veiklos buveinė yra Jungtinėse Amerikos Valstijose, o kibernetinė ataka įvykdyta draudėjo padalinyje esančiame Vokietijoje bei taip buvo pasisavinta draudėjo disponuojama informacija, kuri naudojama ne tik aptarnaujant Vokietijos klientus, bet ir Jungtinių Amerikos Valstijų. Dėl to reikia įvertinti kokia apimtimi išmokama draudiminė išmoka. Ar draudimo apsauga apima draudžiamuosius įvykius įvykdytus tik vienoje ar keliose valstybėse?

Manytina, jog jeigu žala padaryta apdraustajam kibernetinėje erdvėje, nėra pagrindo susieti žalos atsiradimą su vieta, kurioje įvykdyta kibernetinė ataka arba kurioje buvo įvykdyti pirmieji atakos etapai, o žala atsirado kitoje vietoje. Vertinant tuos atvejus, kai žala yra nematerialli, jos atlyginimas neturėtų priklausyti nuo atakos atsiradimo vietos (angl. *origin of attack*), nes žala pasireiškia visam juridiniam asmeniui, t. y. visoje jo veikimo teritorija nepaisant valstybių ribų, nes paprastai tie patys duomenys yra išskaidomi į kelias dalis ir saugomos identiški duomenys skirtingose valstybėse laikomose serveriuose, todėl sudaryta draudimo sutartis su Jungtinėse Amerikos Valstijose įregistruotu draudiku užtikrins žalos atlyginimą apdraustajam nepaisant kur atsiras nematerialli žala. Vertinant materialią žalą, įskaitant kiberfizines atakas, galioja bendra taisyklė, jog žalos atsiradimo vieta nulemia taikytiną teisę.

2.4. Kibernetinių rizikų draudimo suma

Draudimo suma laikytina sutartyje nustatyta pinigų suma, kuri turi būti išmokama įvykus draudžiamajam įvykiui arba draudimo sutartyje nustatyta tvarka apskaičiuotina suma, kurios negali viršyti draudimo išmoka, nebent draudimo sutartyje numatyta kitaip[54]. Draudimo suma siejama su apdraudžiamo turto verte. Draudikas pasitelkdamas savo ekspertus nustato draudžiamojo turto vertę, t. y. draudimo sudarymo metu nustatoma turto vertė bei tuo pačiu maksimali draudimo išmokos riba. Draudimo vertė nustatoma įvairiais kriterijais. Pavyzdžiui, turto vertė gali būti nustatyta šalių susitarimu, ją siejant su draudžiamo turto verte arba apibrėžiant tokia suma, kurią reikėtų padengti norint atkurti turtą į tokią būklę, kokioje jis buvo iki draudžiamojo įvykio. Jeigu šalys nesusitaria dėl draudimo vertės ar jos apskaičiavimo metodikos, preziumuojama, jog draudimo vertė yra lygi apdrausto daikto rinkos kainai sutarties sudarymo metu[55].

Nustačius draudimo vertę yra nustatoma draudimo suma. Draudimo suma nustatoma atsižvelgiant į apdraudžiamo turto vertę bei atitinkamas taisykles, kurias lemia apdrausto turto vertės ir draudimo sumos santykis. T. y. jeigu apdraudžiamas turtas proporciniu draudimu, tai draudėjas neapdraudžia visos rizikos, o tik jos dalį, todėl draudimo suma bei išmoka yra proporcinga apdraustos rizikos daliai. Pirmosios rizikos draudimu draudėjas apdraudžia draudimo objektą mažesne nei draudimo vertė draudimo suma, o įvykus draudžiamajam įvykiui draudikas išmoka draudiminę išmoką, kuri yra lygi draudėjo patirtiems nuostoliams, tačiau neviršijantiems draudimo sumos.

Jeigu draudimo vertė sutarties galiojimo metu padidėja, laikoma, jog galioja nevisiškas draudimas, o dėl visiško turto apdraudimo rizika tenka pačiam draudėjui. Draudimo vertei sumažėjus, draudikas neturi atlyginti nuostolių, kurie yra didesni nei draudimo vertė, dėl to laikoma, jog draudimo sutartis negalios ta dalimi, kuria draudimo suma viršija draudimo vertę. Įvykus draudžiamajam įvykiui draudikas turi teisę paneigti draudimo sutartyje nustatyto apdrausto turto vertę tai įrodant[56].

[54] Lietuvos Respublikos Draudimo įstatymo 2 str. 27 d.. Valstybės žinios, 2003, Nr. 94-4246.
[55] Ibid 104 str.
[56] Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus nutartis civilinėje byloje nr. 3K-3-746/2003.

Paprastai pagal savo rizikos apimtį skiriamos dviejų rūšių kibernetinių rizikų sutartis. Vienų kibernetinių rizikų draudimo sutarties pagrindu draudėjas turi garantuoti aukšto standarto apdairų elgesį bei prisiimti moralinę riziką už savo darbuotojų veiksmus. Tai reiškia, jog draudėjas moka mažesnes draudimo įmokas draudikui, tačiau jis turi pareigą imtis griežtų veiksmų laikantis kibernetinio saugumo gerųjų praktikų. Draudėjas turi būti pats atsakingas ir apmokyti savo darbuotojus apie naujausias bei dažniausiai pasitaikančias kibernetines rizikas, socialinės inžinerijos metodus naudojamus suklaidinti darbuotojus apgaule išviliojant privačią vertingą informaciją. Antruoju kibernetinių rizikų sutarčių atveju draudėjas garantuoja mažesnį apsauginį elgesio standartą. Dėl informacinių technologijų žinių trūkumo dauguma ūkio subjektų apskritai ignoruoja veiksnius, kurie lemia kibernetines rizikas. 57 procentai kompanijų mano, jog kibernetinė rizika yra išimtinai tik informacinių technologijų skyriaus problema, t. y. kibernetinė erdvė yra vertinama taip pat kaip bet kokie kiti elektronikos prietaisai, dėl to bendrovės vadovai nėra linkę gilintis į kibernetinio saugumo problemas. Įmonių vadovai mano, jog tai nėra kiekvieno darbuotojų problema, nes dauguma žmonių neturi informacinių technologijų išsilavinimo ar suvokimo kaip tai veikia, o manytina, jog už kibernetines rizikas atsakingas yra tik įmonės informacinių technologijų padalinys. Dėl to rizika įvykti draudžiamajam įvykiui yra didesnė, tačiau ši rizika išlieka apdraudžiama brangesniu arba ne visišku draudimu. Pažymėtina, nors kibernetinių rizikų ignoravimas yra reali praktika, tačiau ji yra kritikuotina. Manytina, jog ateityje neliks nei vieno ūkio subjekto, kuris nevykdytų savo veiklos be informacinių technologijų, todėl anksčiau ar vėliau bendrovės neišvengiamai taps kibernetinių atakų aukomis.

Dėl to manytina, jog optimaliausias variantas yra tarp abiejų kibernetinių rizikų draudimo sutarčių rūšių. T. y. draudėjas pats turėtų įvertinti kokia apimtimi jam reikia draudimo vertinant apdraudžiamo turto vertę ir kokį draudimą finansiškai gali pajėgti įsigyti draudėjas[57].

Pažymėtina, jog kibernetinių rizikų draudimo premijų bei išmokos suma apskaičiuojama atsižvelgiant ne vien tik į patirtus materialius nuostolius, bet ir į juridinio asmens patirtus kaštus dėl veiklos administravimo bei darbuotojų užimtumo siekiant atstatyti iki draudžiamojo įvykio buvusią padėtį, nes, kaip minėta, draudimo tikslas yra atkurti apdraustojo asmens turtinę padėtį į tokią, kokia būtų buvusi, jeigu draudžiamojo įvykio nebūtų buvę. Taip pat į draudimo premijos dydį turi įeiti draudiko patiriamų draudimo sutarties sudarymo, administravimo kaštai bei jo

[57] FERILLO, Paul *et al*. Cyber Security, Cyber Governance, and Cyber insurance. Harvard law journal. 2014.P. 4.

pelnas, nes draudikas yra kaip ir bet kuris kitas ūkio subjektas vykdantis veiklą dėl pelno gavimo, o pati draudiko veikla nėra savitikslė.

Vidutinės kibernetinių rizikų draudimo premijos 2012 metais JAV buvo 100 tūkst. JAV dolerių dėl 10 milijonų JAV dolerių maksimalios draudimo sumos. O Didžiojoje Britanijoje premijos buvo 30 tūkst. svarų sterlingų, kai maksimali draudimo suma buvo 1 milijonas svarų sterlingų, draudime, kuris neapima juridinio asmens padalinius veikiančius JAV[58].

Draudimo suma vertinama atsižvelgiant į realų patiriamų nuostolių dydį. Bendroji praktika yra to, jog nėra žinoma kokia realiai žala yra patiriama, nes dėl reputacijos sumažėjimo baimės bendrovės nėra nusiteikusios pranešti apie įvykius, dėl kurių buvo pažeistas jų informacinis saugumas. Pavyzdžiui, 2015 metais kibernetinio saugumo firmos parengtoje apžvalgoje buvo teigta, jog daugiau nei šimtas finansines paslaugas teikiančios firmos vykdančios veiklą daugiau nei 30 pasaulio valstybėse buvo kenksmingos programinės įrangos „Carbanak“ aukos bei bendrai patyrė 300 milijonų JAV dolerių nuostolių, tačiau nei viena iš šių firmų pranešė apie ataką[59].

Dėl informacijos trūkumo rinkoje sunku apibrėžti kibernetinių rizikų draudimo sumą, įmokas bei išmokas. Šiai problemai spręsti buvo nusamdytas privačios kibernetinio saugumo firmos tyrimas bei draudikai surinko rinkos informaciją apie kibernetinių atakų padaromą žalą[60]. Remiantis jų duomenimis kiekvienais metais visame pasaulyje kibernetinių nusikaltimo padariniai siekia 375-575 milijardų JAV dolerių žalą, o vien Didžiojoje Britanijoje per metus padaroma 20 milijardų svarų sterlingų žala[61]. 2014 metų Ponemono instituto atlikta kibernetinės erdvės apžvalgoje nustatyta, jog kiekvienai didelei JAV kompanijai kiekvienais metais tenka 3.5 milijonų JAV dolerių žala[62]. O kibernetinį saugumą užtikrinančią programines įrangas pardavinėjanti bendrovė „Norton“ teigimu 2013 m. 431 milijonai suaugusiųjų buvo kibernetinių atakų aukos, o jų nuostoliai sudarė 114 milijardus JAV dolerių[63].

---

[58] Airmic Review of recent developments in the cyber insurance market, 2012. [interaktyvus]. [Žiūrėta 2016-03-03]. <http://docplayer.net/15695701-Airmic-review-of-recent-developments-in-the-cyber-insurance-market-commentary-on-the-increased-availability-of-cyber-insurance-products-guide.html>.

[59] Bank hackers steal millions via malware. The New York Times. 2015. [interaktyvus]. [Žiūrėta 2016-03-03]. < http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html>.

[60] GORDON, Lawrence *et al*. CSI/FBI Computer Crime and Security Survey, COMPUTER SEC. INST. 2006. [interaktyvus]. [Žiūrėta 2016-03-06]. <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf>.

[61] Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime. 2014. [interaktyvus]. [žiūrėta 2016-03-06]. <http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf>.

[62] 2014 Cost of a Data Breach Study: Global Analysis, the Ponemon Institute, sponsored by IBM, May 2014.

[63] Norton Cybercrime report 2011. [Interaktyvus]. [Žiūrėta 2016-03-05]. <http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport.>.

Taip pat draudimo suma priklauso nuo to, ar draudimas apima pirmojo asmens atsakomybę (angl. *first-party liability*) ar ir trečiojo asmens atsakomybę (angl. *third-party liability*)[64]. Pirmo asmens atsakomybę apdraudžianti draudimo sutartis apima nuostolius susijusius su skaitmeniniu turtu, kaip prarasti duomenys, programinė įranga (nuostoliai susiję su jų atstatymu ar pakeitimu), verslo veiklos nutraukimo nuostoliai dėl neveikiančių tinklo ryšių, kibernetinio plėšikavimo, elektroninių vagysčių ar kitokių kibernetinių nusikaltimų. Trečiojo asmens atsakomybės draudimas apima saugumo ir privatumo pažeidimus, kurie susiję su ištyrimo, advokatų, teismų, baudų valstybės institucijoms, darbuotojų ir klientų konfidencialumo pažeidimo, klientų informavimo apie jų informacijos nutekėjimą (pašto paslaugos bei reklamos, jeigu to reikalauja vietiniai įstatymai), trečiųjų asmenų duomenų praradimo, sutartinių įsipareigojimų su trečiaisiais asmenims vykdymo nuostoliais.

Pavyzdžiui, bendrovė, kuri turi 70 darbuotojų ir jų pajamos per metus siekia 8 milijonus JAV dolerių turėtų tikėtis 420 JAV dolerių premijų dydį, kai draudimo apimtis yra 1.6 milijonų JAV dolerių. Taip pat atsižvelgiant į bendrovės „Brookeland Fresh Water Supply“ esančios rytų Teksase, JAV, atvejį, kibernetinių rizikų draudimas tampa vis įperkamesnis. Kai ši bendrovė patyrė 35 tūkstančių JAV dolerių žalą dėl įvykdytos kibernetinės atakos, kibernetinių rizikų draudimo bendrovei nebankrutavo, o visa tai kainavo tik 500 JAV dolerių franšizė.[65].

Dėl kibernetinės rizikos draudimo sutarčių informacijos trūkumo draudikai nėra tikri dėl draudimo premijų bei išmokamų sumų. Draudikams sunku parengti pilnavertį klausimyną draudėjams, kurie jį užpildytų prieš sudarant draudimo sutartį rizikos įvertinimui. Ta pati problema egzistuoja dėl kibernetinių rizikų draudimų taisyklių, išmokant išmokas.

Taip pat, siekiant įvertinti draudimo sumą, draudikas turėtų išsiaiškinti apie ankstesnes prieš draudėją įvykdytas kibernetines atakas. O draudimo premija paprastai turėtų būti mažesnė tuo atveju, kai draudėjas yra užtikrinęs tam tikro lygio kibernetinio saugumo standartus arba kai draudėjas turėjo kibernetinių rizikų draudimą bet nebuvo reikalavęs draudiko išmokėti draudiminę išmoką. Manytina, jog pilnavertei draudimo sutarties sumai ir sąlygoms nustatyti draudikas turi teisę reikalauti savo lėšomis įvykdyti draudėjo kibernetinio saugumo auditą prieš sudarant sutartį,

[64] FERILLO, Paul *et al*. Cyber Security, Cyber Governance, and Cyber insurance. Harvard law journal. 2014.P. 8.
[65] The Case for Cybersecurity Insurance, Part II. [Interaktyvus]. [Žiūrėta 2016-03-03]. <http://krebsonsecurity.com/2010/07/the-case-for-cybersecurity-insurance-part-ii/>.

bei, jeigu reikalinga, po kiekvienos įvykdytos kibernetinės atakos, ar pasikeitus esminėm aplinkybėm, kurios yra reikšmingos draudimo rizikai įvertinti.

2.5. Kibernetinių rizikų draudimo laikotarpis

Reikia atskirti dvi teisines kategorijas: draudimo sutarties galiojimo terminas bei draudimo apsaugos laikotarpis. Draudimo sutartis galioja iki juridinių faktų atsiradimo, dėl kurių sutartis laikoma nebegaliojanti. Pavyzdžiui, išnyko galimybės įvykti draudžiamajam įvykiui, sutarties galiojimo termino pasibaigimas, sutartis pripažinta negaliojančia ir kita. Draudimo apsaugos laikotarpis yra laiko tarpas, kurio metu galioja draudimo apsauga, t. y. įvykus draudžiamajam įvykiui apdraustasis bus grąžintas į tokią turtinę padėtį, kurioje būtų buvęs jeigu nebūtų įvykęs draudžiamasis įvykis. Pagal draudimo įstatymo 2 str. 21 d. draudimo laikotarpis nebūtinai turi sutapti su draudimo sutarties galiojimo terminu. Pavyzdžiui, jeigu draudimo sutartyje yra sulygta, jog draudėjui laiku nesumokėjus periodinių draudimo įmokų apdraustajam nebus taikoma draudiminė apsauga, tačiau bus laikoma, jog draudimo sutartis toliau galios, o draudimo apsauga atsinaujins nuo to momento, kai draudėjas sumokės nesumokėtas draudimo įmokas.

Kita problema su kuria susiduriama kibernetinių rizikų draudimo sutarties šalys yra draudžiamojo įvykio vertinimas pasibaigus draudimo sutarties ir draudimo apsaugos galiojimui. Dažnai kibernetinės atakos vyksta ištisus mėnesius ar net metus, o pačios bendrovės nepastebi, jog prieš jas vykdoma ataka. Dėl to kyla problema, kai draudimo sutarčiai pasibaigus draudėjas pastebi kibernetinę ataką, kuri buvo pradėta draudimo sutarčiai galiojant, tačiau buvo nutraukta ir pastebėta tik jai pasibaigus. Manytina, jog draudėjas turėtų prisiimti riziką dėl kibernetinės atakos nepastebėjimą. Draudėjas yra savo srities profesionalas, kuris gali pasitelkti savo darbuotojus arba trečiuosius nešališkus ekspertus, kurie atliktų kibernetinio saugumo auditą. Ir tik atlikus auditą ir nustačius, jog draudžiamųjų įvykių nėra nutraukti draudimo sutartį. Tačiau atsižvelgiant į tai, jog kibernetinių rizikų draudimo sutartis turėtų išvengti teisminių ginčų ateityje, todėl manytina, jog tai turėtų būti detaliai aptarta draudimo taisyklėse. Ypatingai atsižvelgiant į tokius atvejus, kai dėl

atakos specifiškumo ir rinkos technologijų ar ekspertų trūkumo draudžiamojo įvykio objektyviai kibernetinių rizikų draudimo sutarties galiojimo metu ngalima nustatyti.

Vertinant ankščiau minėtas nuostatas, draudėjui derantis su draudiku dėl draudimo taisyklių taip pat yra galimybė draudimo sutartyje numatyti retroaktyvųjį draudimą, pagal kurį draudimo apsauga būtų taikoma draudžiamajam įvykiui, kuris būtų įvykęs iki sutarties sudarymo momento, tačiau sutarties sudarymo momentu nebūtų žinomi draudžiamojo įvykio padariniai[66].

2.6. Kibernetinių rizikų draudimo sutarties forma bei sudarymo ypatumai

Draudimo sutartims taikomas rašytinės formos reikalavimas. Draudimo sutarties sąlygos paprastai yra įtvirtintos trijuose dokumentuose: draudėjo prašyme sudaryti draudimo sutartį, draudimo taisyklėse bei draudimo liudijime (polise). Draudimo įstatymo 92 str. 1 d. reglamentuoja draudimo taisyklių sąlygų turinį. Draudimo taisyklėse privaloma nurodyti šias sąlygas: draudžiamuosius bei nedraudžiamuosius įvykius, draudimo objektą, draudimo sumą, įmokų bei išmokų apskaičiavimo, mokėjimo bei išmokėjimo tvarką, įmokų mokėjimo tvarkos nesilaikymo padarinius, žalos nustatymo tvarką ir kt. Prašyme sudaryti draudimo sutartį atsispindi draudėjo pateikta informacija apie jį patį. Tai yra informacijos pagrindas draudikui spręsti apie būsimas draudimo sutarties sąlygas. Draudimo poliso turinį reglamentuoja CK 6.991 str. 1 d., pagal kurį draudimo polise turi būti nurodyta informacija apie draudimo sutarties šalis, draudimo objektą, draudimo sumą, draudimo įmokas bei mokėjimo tvarką, draudimo rūšį bei galiojimo terminą.

Draudimo sutartis gali būti sudaroma prisijungimo arba individualiai aptartu būdu, draudikui akceptuojant draudėjo pasiūlymą arba draudėjui akceptuojant draudiko pasiūlymą[67]. Prisijungimo būdu sudaromiems draudimo sandoriams draudėjai turi ribotas arba jokių galimybių derėtis dėl sutarties sąlygų, todėl joms taikomos CK 6.185-6.187 str. įtvirtintos sutarčių standartinių sąlygų taisyklės. Dėl šios priežasties draudėjai paprastai yra laikomi silpnesniąja

[66] KONTAUTAS, Tomas. Draudimo sutarčių teisė. Vilnius. 2007 m. P. 77.

[67] Ibid 6.990 str. 1 d.

sutarties šalimi. Susipažinti su standartinėmis draudimo sutarties sąlygomis draudėjui turi būti prieinama iki sutarties pasirašymo.

Draudimo sutartis yra konsensualinė sutartis. Tai reiškia, jog sutartis laikoma sudaryta nuo to momento, kai sutarties šalys susitaria dėl esminių draudimo sutarties sąlygų ir tai padaro įstatymo reikalaujama rašytine forma. Esminėmis draudimo sutarties sąlygomis laikytinas konkretus turtas, kuris yra apdraudžiamas, draudimo rizika, draudimo laikotarpis, bei sumų draudimo atveju papildoma esminė sąlyga yra draudimo suma ir apdraustasis asmuo, jeigu draudėjas yra juridinis asmuo[68]. Pažymėtina, jog teisės doktrinoje yra skiriami atskiri juridiniai faktai tarp draudimo sutarties įsigaliojimo momento bei draudimo apsaugos atsiradimo momento. Kaip minėta, draudimo sutartis laikoma sudaryta pagal konsensualinių sutarčių taisykles, o draudimo sutarties taikoma apsauga atsiranda tik tada, kai draudėjas įvykdo draudimo sutartyje numatytą sąlygą laiku mokėti sutartas draudimo įmokas[69].

Sutarčių teisės doktrinoje draudimo sutartys priskiriamos prie kauzalinių sutarčių. Draudimo sutarties pagrindas yra šalių susitarimas dėl draudimo teisinių santykių atsiradimo bei apsaugos nuo draudžiamojo įvykio rizikos nuo to momento, kai įsigalioja draudimo sutarties taikoma apsauga draudėjui laiku pilnai sumokėjus draudimo įmoką. Taip pat draudimo sutartis priskiriama prie atlygintinių sutarčių, nes draudimo teisiniai santykiai pagal savo prigimtį gali būti tik atlygintinis.

3. Kibernetinių rizikų draudimo sutarties šalių teisės ir pareigos

3.1. Draudėjo pareiga atskleisti informaciją

Draudimo teisės doktrinoje draudimo santykiai grindžiami visiško pasitikėjimo doktrina. Lietuvos Aukščiausiasis teismas savo praktikoje ne vieną kartą yra pažymėjęs, jog draudimo sutartis yra rizikos sutartis, pagal kurią draudikas perima iš draudėjo nuostolių atsiradimo riziką;

[68] KONTAUTAS, Tomas. Draudimo sutarčių teisė. Vilnius. 2007 m. P. 59.
[69] Ibid p. 29.

be to, tai yra fiduciarinė sutartis, t. y. grindžiama jos šalių didžiausio tarpusavio pasitikėjimo principu (lot. uberrimae fidei); dėl to draudimo sutarties šalys privalo būti viena kitai absoliučiai atviros ir atskleisti viena kitai visą informaciją, kuri gali būti reikšminga šiai sutarčiai sudaryti bei jos sąlygoms nustatyti ir vykdyti[70]. Draudėjas turi pareigą draudikui sąžiningai atskleisti tikrovę atitinkančią informaciją apie faktus, kurie turi esminę reikšmę draudikui suteikiančiam draudimo apsaugą, o draudikas turi konfidencialumo pareigą neatskleisti informacijos apie draudėją tretiesiems asmenims. Tokia informacija paprastai leidžia draudikui nustatyti adekvačius draudimo premijų dydžius. Kadangi draudikas yra tas asmuo, kuris perima riziką ir jam paprastai nėra galimybių tiksliai žinoti draudėjo riziką lemiančių aplinkybių, tai būdamas protingas draudikas prisiims tik tokią riziką, apie kurios aplinkybes draudėjas nėra nieko nuslėpęs. Kitos draudėjo fiduciarinės pareigos yra pranešti apie draudžiamojo įvykio rizikos padidėjimą, apie įvykusi draudžiamąjį įvykį kuo greičiau po pranešti draudikui, bendradarbiauti siekiant ištirti draudžiamąjį įvykį bei apskaičiuoti patirtų nuostolių dydį. Pažymėtina, jog visi išvardyti draudimo santykių ypatumai lemia didesnę nei kitų civilinių sutarčių rūšių šalių pareigą bendradarbiauti ir kooperuotis[71].

Pareiga įvertinti draudėjo riziką tenka draudikui, tačiau draudėjas turi priešpriešinę pareigą padėti draudikui įvertinti riziką atskleidžiant tikslią informaciją apie apdraudžiamo asmens veiklą. CK 6.994 str. 1 d. reglamentuoja draudiko teisę įvertinti draudimo riziką. Šis straipsnis reglamentuoja draudiko teisę prieš sudarant draudimo sutartį apžiūrėti draudžiamą turtą arba pasinaudoti ekspertais draudžiamo turto vertei nustatyti. Reikia atsižvelgti į kibernetinių rizikų ypatumus, t. y. jog ne visais kibernetinių rizikų draudimo atvejais yra apdraudžiamas turtas, o tik tais kai žala padaroma nematerialiems objektams (informacijos kopijavimas, darbo sutrikdymas). Kibernetinės atakos yra įvykdomos per tinklo ryšio priemones nepadarant žalos materialiems objektams. Dėl to manytina, jog CK 6.994 str. 1 d. reikėtų aiškinti plečiamai, atsižvelgiant į šios normos tikslą – draudiko teisę pilnavertiškai įvertinti draudimo riziką, įskaitant ir nematerialų turtą.

[70] Pavyzdžiui, Lietuvos Aukščiausiojo Teismo 2000 m. gegužės 3 d. nutartį civilinėje byloje UAB „Pozicija“ v. AB „Lietuvos draudimas“, bylos Nr. 3K-3-486/2000; 2001 m. birželio 7 d. nutartį civilinėje byloje AB „Lietuvos draudimas“v. I. Z. N., bylos Nr. 3K-7-397/2001; 2003 m. gegužės 5 d. nutartį civilinėje byloje UAB „Vigidas“ v. UAB DK „Censum“, bylos Nr. 3K-3-546/2003.

[71] Lietuvos Respublikos Civilinio kodekso 6.38 str. 3 d.. Valstybės žinios, 2000, Nr.74-2262.

Draudėjo tikimybė patirti nuostolių dėl kibernetinės atakos priklauso nuo vartotojo taikomų kibernetinių saugumo priemonių bei nuo tinklo ir darbuotojų saugumo. Todėl teigtina, jog draudimo rizikos įvertinimas kibernetinių rizikų draudimo sutartyse turėtų būti atliekamas draudikui atliekant kibernetinio saugumo auditą. Į tai įeina tinklo kabelių fizinio išdėstymo bei jungčių patikrinimo, naudojamos aparatinės įrangos naujumas bei saugumo specifikacijos, visos naudojamos programinės įrangos įvertinimas, darbuotojų informacinių technologijų išmanymo lygis, naudojimosi elektroniniais prietaisais politika, ar darbuotojai gali prisijungti prie ūkio subjekto tinklo ne tik būdami darbdavio patalpose ir pan. Jei audito metu nustatoma, jog bendrovė yra linkusi tapti kibernetinių rizikų auka arba prieš ją praeityje buvo įvykdyta ne viena kibernetinė ataka, tai tokiam draudėjui teks didesnės premijos. Pavyzdžiui, jeigu bendrovė naudojasi pasenusia programinę įrangą, kurios pažeidžiamumo taškai viešai yra žinomi, kaip „Microsoft Windows NT“, jų premijos bus didesnės.

Draudėjas turi atskleisti tik tokią informaciją, kuri turi esminę reikšmę draudikui įvertinti draudimo riziką. Paprastai laikoma, jog draudėjas atskleidė esmines aplinkybes, jeigu tinkamai atsakė į klausimus draudiko parengtoje prašymo sudaryti draudimo sutartį formoje[72]. O draudikui gavus draudėjo pateiktą informaciją bei manant, jog informacijos nepakanka draudimo rizikos įvertinimui, draudikas privalo kreiptis į draudėją dėl papildomos informacijos pateikimo, o to nepadarius draudikas prisiima neigiamų padarinių riziką[73].

Draudėjo atsakomybė dėl tinkamos informacijos neatskleidimo priklauso nuo to ar draudėjas informacijos neatskleidė tyčia, dėl neatsargumo ar informacijos neatskleidimą nesant draudėjo kaltės[74]. CK 6.993 str. 4 d. reglamentuoja, jog tyčia draudėjui neatskleidus esminės draudimo rizikai įvertinti reikalingos informacijos draudėjas netenka teisės į draudimo išmoką, jeigu draudžiamasis įvykis įvyko, o draudikas turi teisę reikalauti pripažinti draudimo sutartį negaliojančia *ab initio*. Siekiant įrodyti draudėjo tyčią nuslėpti informaciją reikia įrodyti, jog draudėjas suvokė, jog konkrečios informacijos nenurodymas leis jam sudaryti draudimo sutartį patiriant mažesnius kaštus (gaunant mažesnę draudimo premiją ar didesnę išmoką). Neatskleidžiant tikslios informacijos dėl neatsargumo, draudikas turi 2 mėnesius nuo tikslios informacijos sužinojimo momento per kuriuos privalo pasiūlyti draudėjui pakeisti sutartį.

[72] KONTAUTAS, Tomas. Draudimo sutarčių teisė. Vilnius. 2007 m. P. 92.
[73] Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus nutartis civilinėje byloje nr. 3K-3-1029/2003.
[74] KONTAUTAS, Tomas. Draudimo sutarčių teisė. Vilnius. 2007 m. P. 94.

Draudikui per minėtą terminą nepasiūlius pakeisti sutarties, draudikas prarandą teisę remtis neatskleista informacija. O draudėjui atsisakius pakeisti sutartį draudikas turi teisę nutraukti sutartį vienašališkai[75].

Nustatant mokėtinų premijų dydžius draudikai yra linkę potencialius draudėjus klasifikuoti pagal rizikos grupes atsižvelgiant į draudėjo pateiktą individualią informaciją, kuri yra reikšminga draudimo rizikos laipsniui įvertinti bei atskirti draudėjui į skirtingą rizikos grupę. Rizikos grupių tikslas – kuo ekonomiškiau nustatyti premijų dydį, neatliekant itin didelius kaštus kainuojančius individualių rizikų įvertinimus, kibernetinio saugumo auditus. Vertinant draudėjo informaciją draudikai atsižvelgia į statistiką, pavyzdžiui, ar teisines paslaugas teikiančios įmonės yra linkusios būti kibernetinių atakų aukomis, ar ankščiau prieš ją buvo įvykdyta kibernetinė ataka. Tačiau iškyla statistikos trūkumo problema dėl dviejų priežasčių, kurios apsunkina draudėjų skirstymą pagal rizikos grupes: kibernetinė erdvė yra gana naujas reiškinys visuomenėje, o nukentėjusios bendrovės dėl reputacinių ir mažo atakų išaiškinamumo skaičiaus neskelbia apie prieš jas įvykdytas kibernetines atakas.

Doktrinoje vyrauja vieninga nuomonė, jog kibernetinis saugumas nepriklauso vien tik nuo naudojamų technologijų[76]. Todėl net įvertinus visą pateiktą draudėjo informaciją ir atlikus kibernetinio saugumo auditą, kibernetinės rizikos išlieka. Pažymėtina, jog kibernetinės rizikos draudimas padidina draudėjo gerbūvį, tačiau tai nepadidina juridinio asmens kibernetinio saugumo. Dėl to draudėjui įvertinus saugumo spragas, kurias jis gali pašalinti, jam vis tiek išliks turtinis interesas apdrausti neapsaugomą kibernetinę riziką.

3.2. Draudėjo pareiga imtis veiksmų draudžiamiesiems įvykiams išvengti arba sumažinti žalą

Draudėjas sudarydamas kibernetinių rizikų draudimo sutartį apsidraudžia nuo neigiamų finansinių padarinių dėl minėtų rizikų kibernetinėje erdvėje, tačiau tai nereiškia, jog draudėjas

[75] Ibid p. 95.
[76] ANDERSON, R *et al*. Security economics and european policy. In Proceedings of WEIS'08, Hanover, USA, Jun. 25-28 2008.

neprivalo laikytis tam tikrų protingo elgesio standartų draudimo sutarties galiojimo laikotarpiu bei jai pasibaigus. Kaip minėta, draudimo apsauga galioja draudėjo atžvilgiu įvykusiems draudžiamiesiems įvykiams. Kibernetinių rizikų draudime ypatingai reikia atsižvelgti į tai, jog ateityje kibernetinės erdvės bei atakų dinamikos nėra įmanoma numatyti, todėl trūksta teisinio apibrėžtumo kibernetinėje erdvėje įvykusio draudžiamojo įvykio sąvokos apibrėžimo. T. y. draudėjas draudimo sutarties galiojimo laikotarpiu privalo domėtis apie kibernetinio saugumo naujoves bei diegti adekvačias technologijas lygiai taip pat kaip tą patį darytų jeigu nebūtų apsidraudęs.

Elgesio standartas, kurio reikalauja draudikas, jog draudimo sutarties laikotarpiu laikytųsi draudėjas turi būti proporcingas ir per ne lyg nevarantis draudėjo veiksmų, t. y. taip, jog nustatyti elgesio standartai nepaneigtų pačios draudimo sutarties esmės bei motyvų dėl kurių ji buvo draudėjo pasirašyta, o draudėjas kuo mažiau varžomas galėtų vykdyti savo ūkinę komercinę veiklą.

Taip pat šalia kiekvieno elgesio standarto turi būti aptarti jų nesilaikymo padariniai. T. y. išvardijamos konkrečios priežastys, kurių nesilaikius laikoma, jog padidėjo draudiminė rizika dėl draudėjo kaltės bei draudimo išmoka yra mažinama arba apskritai nemokėtina. Nustatant įvykusio draudžiamojo įvykio patirtą žalą yra nustatoma ir atsižvelgiama į draudėjo kaltės formą dėl protingo draudėjo elgesio standartų nesilaikymo, t. y. ar jų nesilaikyta tyčia ar dėl neatsargumo. Jeigu draudėjas tyčia nesilaikė atitinkamo elgesio standartų, tai pripažįstama, jog draudikas neturi pareigos išmokėti draudimo išmokos. Vertinama ar tarp draudžiamojo įvykio ir atsargumo priemonių (atitinkamo elgesio standarto) nesilaikymo yra priežastinis ryšys, ir draudžiamuoju įvykiu pripažįstama tai tik tada, kai nėra priežastinio ryšio tarp draudėjo tyčinių veiksmų. Vertinant neatsargumo kaltės formą pripažįstama, jog draudimo sutarties tikslas yra apsidrausti nuo neatsargių draudėjo veiksmų, dėl to įvykus draudžiamajam įvykiui dėl draudėjo neatsargumo draudikas privalo atlyginti draudėjo patirtus nuostolius, išskyrus didelio neatsargumo atvejais, kai tokie atvejais yra individualiai aptarti tarp draudiko ir draudėjo bei įtvirtinti draudimo sutartyje[77].

Draudėjas neturėtų jaustis ramus vien žinantis tai, jog įvykus kibernetiniai atakai, jo turtiniai praradimai bus atkurti į tokią padėtį, kokie būtų buvę iki įvykstant draudžiamajam įvykiui. Pažymėtina, jog kibernetinių rizikų draudimas savaime neišgelbės nuo visų kibernetinių rizikų neigiamų padarinių. Bendrovės privalo reguliariai tobulinti savo kibernetinį saugumą ir saugoti

[77] Lietuvos Respublikos Draudimo įstatymo 106 str. Valstybės žinios, 2003, Nr. 94-4246.

duomenis investuojant į užraktų ir apsaugos kamerų virtualius analogus, kurie greitai sutvarkytų programinės įrangos saugumo spragas bei užkoduotų svarbius duomenis. Protingo elgesio standartų taisyklė suponuoja tai, jog juridinis asmuo privalo turėti savo informacinių technologijų specialistus arba reguliariai samdytųsi ekspertus turinčius galiojančius tokių pripažintų organizacijų informacinių technologijų akredituotus saugumo inžinerijos sertifikatus kaip ITIL (angl. *Information Technology Infrastructure Library*), Cisco CCNP/CCIE Security[78] (angl. *Cisco Certified Network Professional/Internetwork Expert Security*), ISACA[79] (angl. *Information Systems Audit and Control Association*), CISO (angl. Chief Information Security Officer), CompTIA Security+[80].

Pavyzdžiui, buvo manoma, jog viena iš pirmaujančių informacinių technologijų kompanija „Sony“ turi aukštą kibernetinio saugumo užtikrinimo politiką. Manytina, jog tokia kompanija turi specializuotą vadovą informacinių technologijų saugumo užtikrinimo srityje. Tačiau, kai bendrovė buvo nulaužta 2011 metais, ji neturėjo kibernetinio saugumo užtikrinimo vadovo (angl. *Chief of Information Security*, CISO). Remiantis statistika, bendrovės, kurios turi CISO ar panašaus lygio informacinio saugumo vadovą patyrė mažesnius įsilaužimo nuostolius: po 157 JAV dolerius per pasisavintą dokumentą prieš 236 JAV dolerius tose bendrovėse, kurios neturėjo dedikuotų vadovų informacinio saugumo srityje tarp bendros komercinės rizikos mažinimo programos.

Draudėjo pareiga imtis veiksmų išvengti draudžiamųjų įvykių ar sumažinti jų padarytą žalą priklauso nuo metodų ir mechanizmų, kuriais pasinaudojus įvykdomos kibernetinės atakos. Dėl to draudimo sutartyje gali būti numatyti tokie kibernetinio saugumo reikalavimai:

1) Autentikacija. Tai yra pati paprasčiausia apsauga nuo galimų kibernetinių rizikų. Tai yra privalomas slaptažodžių naudojimas. Ne bet kokie slaptažodžiai yra laikytini saugūs, o tik tokie, kurie, atsižvelgiant į metodus, kuriais jie yra atspėjami, jų nuspėjamumo tikimybė yra kuo mažesnė[81]. Bendra taisyklė yra tokia, jog nėra neatspėjamų slaptažodžių, o skiriasi tik laiko tarpas, kurio reikia jį atspėti[82]. Pirmiausia atakuotojai atsižvelgia į sukauptas nulaužtų slaptažodžių duomenų bazes, kuriuose yra išsaugota šimtai tūkstančių vartotojų duomenų, įskaitant jų slaptažodžius. Išanalizavus viešose duomenų bazėse randamus

[78] http://www.cisco.com/
[79] https://www.isaca.org/Pages/default.aspx
[80] https://www.comptia.org/
[81] VERAS, R., COLLINS, C., and THORPE, J. On the semantic patterns of passwords and their security impact. In Network and Distributed System Security Symposium. 2014.
[82] LOUKAS, George. Cyber-Physical Attacks, A growing invisible threat. 2015. P. 182.

slaptažodžius informacija yra apibendrinama: sukuriamas dažniausiai naudojamų slaptažodžių sąrašas. Remiantis šiuo sąrašų išbandomi visi slaptažodžiai iš eilės, pagal jų naudojimo dažnumą duomenų bazėse *brute force* atakos būdu. Išbandžius visą sąrašą bandomi visi galimi slaptažodžių junginiai. Todėl efektyvi slaptažodžių naudojimo praktika susideda iš trijų dalių: a) reguliaraus slaptažodžių keitimo; b) įvairių simbolių, kaip skaičių, mažųjų ir didžiųjų raidžių (skirtingų kalbų), neraidinių ženklų naudojimas; c) to paties slaptažodžio nenaudojimu niekur kitur. Pažymėtina, jog ūkio subjektų požiūris į sudėtingų slaptažodžių naudojimą yra neigiamas, nes tai mažina bendrovės produktyvumą, tam reikalingas papildomas administravimas bei su juo susijusios išlaidos, o darbuotojai nuolatos keisti slaptažodžius nėra linkę.

2) Apribojimas (angl. *limitation*). Remiantis kiekvieno darbuotojo užimamos pareigomis bei jam reikalinga informaciją, turėtų būti vadovaujamasi taisykle, jog kiekvienas darbuotojas turėtų galimybę pasiekti kuo mažiau informacijos, t. y. minimaliai tiek, kad jam užtektų įvykdyti savo darbo funkcijas ir ne daugiau. Kibernetinio saugumo ekspertai turėtų kiekvieno bendrovėje sudaryti atskiras darbuotojų grupes, kuriems skirtingai sudaromos prieinamos informacijos kiekis. Pavyzdžiui, darbuotojas dirbantys juridinio asmens teisės skyriuje, turėtų teisę matyti tik teisės skyriaus dokumentus, o ne finansų ar kitų skyriaus duomenis, galėjimą keisti informacinių technologijų aparatinės ir programinės įrangos parametrus suteikta tik informacinių technologijų skyriaus darbuotojams, neleisti darbuotojams prisijungti prie darbovietės bevielio tinklo naudojant telefonus ar kitus asmeninius prietaisus. Tokiu būdu pašalinamos jungtys, per kurias kibernetinėje erdvėje gali nutekėti informacija.
3) Ugniasienės (angl. *firewall*). Tai yra filtruojanti įranga, kuri veikia kaip barjeras tarp vidinio (angl. *local area network*, LAN) bei išorinio (angl, *wide area network,* WAN) tinklo. Jos gali būti programinės arba aparatinės įrangos pagrindu. Ši įranga filtruoja iš vidinio tinklo išeinančius duomenų paketus bei iš išorinio tinklo įeinančius duomenų paketus į vidinį tinklą pagal iš anksto gamintojo nustatytas kibernetinio saugumo taisykles, autorizuojant ir neautorizuojant tam tikrus duomenų paketus pagal jų charakteristikas[83].

[83] BELLOVIN, S. M. and CHESWICK, W. R. (1994). Network firewalls. Communications Magazine, IEEE, Volume 32, No. 9. 1994. P. 57.

Ugniasienė analizuoja duomenų paketo šaltinio adresą, adresato adresą, prievado (angl. *port*) numerį, siunčiamus duomenis bei nusprendžia ar konkretų paketą praleisti ar ne.

4) Prieš kenksmingą programinę įrangą nukreiptos programos (angl. *anti malware, anti virus*). *Anti-malware* programos identifikuoja ir apsaugo prie tinklo prijungtus elektroninius prietaisus nuo kenksmingos programinės įrangos padaromos žalos, tačiau tai nėra labai veiksmingos programos naujų pažeidžiamumo taškų atžvilgiu.
5) Darbuotojų apmokymas. Pirma kiekvienam darbuotojui ypatingai svarbi informacija kibernetiniai saugumui užtikrinti yra į socialinės inžinerijos atakas nukreiptas apmokymai. Darbuotojai informuojami apie socialines inžinerijos taktikas, kaip. neatidarymas įtartinų elektroninių laiškų, jeigu nėra žinomas siuntėjas. Pavyzdžiui, kiekvieną dieną išsiunčiama po 144 milijardus elektroninių laiškų, iš kurių 70 procentai elektroninių laiškų gavėjai nėra niekaip susiję su jų siuntėjais. 99 milijardų laiškų išsiunčiamų kiekvieną dieną yra priskiriami prie šlamšto, reklamų ir kenksmingų laiškų (angl. *spam, advertisement, malware*), kurių tikslas yra pažeisti kibernetinį saugumą[84]. Taip pat darbuotojų nespaudimas ant nuorodų (angl. *hyperlink*) nuo nežinomų ar įtartinų adresatų, nesilankymasis tam tikrupose tinklalapiuose, kuriuose galimai yra patalpinta kenksmingos programinės įrangos užkratas, neatidarant failų su „.bat“, „.com“, „.exe“, „.pif“, „.vbs“ galūnėmis (angl. *extensions*), neskambinti elektroniniuose laiškuose nurodytais telefono numeriais, o kreiptis į partnerius tik jų nurodytais adresais.
6) Atsižvelgiant į ūkio subjekto turimus finansinius pajėgumus bei galimybes įdiegti kibernetines rizikas mažinančias programas, atkreiptinas dėmesys į CK nuostatą, jog jeigu draudiko nurodytos priemonės yra per brangios draudėjas turi pareigą jomis vadovautis, tačiau jų išlaidos tenka draudikui[85].
7) Šifravimas (angl. *encryption*) – tai procesas, kurio pagalba įprastinis tekstas pakeičiamas į užkoduotą tekstą. Kriptografijoje naudojamos privačios ir viešos monogramos (angl. *ciphesr*), su kuriomis tekstas yra užkoduojamas ir dekoduojamas. Užkoduoti tekstą gali bet koks vartotojas, tačiau jį atkoduoti gali tik tas asmuo, kuris turi privatų raktą. Pažymėtina,

[84] MAC DONNEL, Ulsch. Cyber threat. How to manage the growing risk of the cyber attacks.2014. P. 12.
[85] Lietuvos Respublikos Civilinio kodekso 6.1013 str. 2 d.. Valstybės žinios, 2000, Nr.74-2262.

jog bendrovė, kuri nešifruoja autentikacijos duomenų jokiais atvejais neturėtų gauti kibernetinio rizikos draudimo.

8) Infiltracija. Reikia įvertinti ar remiantis draudimo rizikos valdymo politika atakuotojai gali fiziškai patekti į draudėjo patalpas apsimesdami valymo, remontininkų ar kitu personalu arba neapsimetus, o esant draudėjo nusamdytam pagalbininkui pasinaudojus palankia galimybe pasisavinti vertingą informaciją.
9) Skatinamųjų premijų taikymas (angl. *bug bounty program*). Daugybę kompanijų yra viešai paskelbusios apie skatinamųjų premijų dalijimą tiems asmenims, kurie atranda jų tinklalapiuose saugumo spragas jomis pasinaudoti. Pavyzdžiui, kompanija Google siūlo iki 20 tūkst. JAV dolerių premiją už saugumo klaidų atskleidimą.
10) Elektroninių prietaisų netaisymas pas trečiuosius asmenis. Draudėjai turėtų turėti savus technikus, kurie taisytų visą jo įrangą, nes, pavyzdžiui, nunešus nešiojamą kompiuterį į servisą pas trečiuosius asmenis, gali būti pasisavinti klientų duomenys ar kita vertinga informacija.

Pažymėtina, jog atsižvelgiant į atakos pobūdį, nuo kurios nukentėjo draudėjas, kaštai, reikalingi investuoti į draudėjo saugumą ateityje neturėtų būti padengiami draudiko, o tai laikytini draudėjo įprastinėmis išlaidomis.

Įprastinėje draudimo sutartyje yra privaloma nurodyti draudžiamuosius ir nedraudžiamuosius įvykius, tačiau kibernetinių rizikų draudime, kurio teisiniai santykiai nėra atskirai reglamentuoti teisės aktų reikėtų vadovautis sveiku protu bei nustatyti nebaigtinį draudžiamųjų ir nedraudžiamųjų įvykių sąrašą. O šį neapibrėžtumą palikti reguliuoti kibernetinių rizikų draudimo sutartyje numatytais draudžiamaisiais įvykiais bei likusias spragas išspręsti abstrakčia draudžiamojo įvykio apibrėžtimi bei teismų praktika, kuri laikui bėgant suformuotų kibernetinių rizikų draudimo draudžiamojo įvykio aiškinimo taisykles.

Jeigu draudimo rizika draudimo sutarties galiojimo metu padidėja ar sumažėja, draudėjas turi pareigą informuoti draudiką apie reiškinius, kurie lėmė rizikos padidėjimą ar sumažėjimą, reikalauti sumažinti draudimo įmokas, o draudikas tai sužinojus turi teisę reikalauti pakeisti arba nutraukti draudimo sutarties nuostatas atsižvelgiant į padidėjusios rizikos aplinkybes. Rizika laikoma padidėjusi iš esmės tik tada, kai apie ją žinojus, draudikas nebūtų sudaręs draudimo sutarties ar būtų nustatęs didesnę draudimo įmoką. Tačiau reikia įvertinti ar draudikui sutarties sudarymo momentu buvo suprantama, jog draudimo rizika akivaizdžiai padidės, pavyzdžiui bus

atrasta naujų spragų programinėje įrangoje. Tokiu atveju laikoma, jog naujų spragų atsiradimo rizika tenka pačiam draudikui, todėl nelaikytina, jog draudimo sutartis turėtų būti keičiama tokiais atvejais.

Terminas, per kurį draudėjas privalo pranešti apie rizikos padidėjimą nėra reglamentuojamas įstatymu, tačiau pagal CK 6.993 str. 5 d. įstatymo analogiją laikoma, jog toks terminas yra 2 mėnesiai nuo momento, kada draudėjas sužinojo apie rizikos padidėjimą, nebent šalys draudimo sutartyje susitarė dėl kitokių terminų taikymo[86].

Draudėjo atsakomybė dėl nepranešimo apie padidėjusią riziką skiriasi pagal draudėjo kaltės laipsnį. Jeigu draudėjas nepranešė tyčia, tuo atveju, kai draudėjas objektyviai nustatė ir suvokė, jog kibernetinė rizika yra padidėjusi arba suvokė, jog nuo draudėjo veiksmų kibernetinė rizika padidės ir gali įvykti draudžiamasis įvykis, tai įvykus draudžiamajam įvykiui draudimo išmoka nėra išmokama. Jeigu kibernetinė rizika padidėjo padaryta dėl neatsargumo, t. y. draudėjas objektyviai galėjo numatyti padidėjusias kibernetines rizikas, tačiau to nepadarė ir neinformavo draudiko, draudikas mažina draudimo išmoką tokia dalimi, kokia jį būtų, jeigu draudimo rizika nebūtų padidėjusi.

Taip pat draudėjas turi pareigą elgtis taip, jog draudžiamųjų įvykių žala būtų kuo mažesnė. Tai reiškia, jog draudėjo veiksmai turi būti protingi siekiant patirti kuo mažesnę žalą bei naudotis objektyviai prieinamomis priemonėmis, įskaitant ir tuos atvejus, kai kibernetinė ataka yra pastebėta. Paprastai atliekama kaštų analizė dėl papildomų priemonių skirtų mažinti kibernetinių atakų žalą naudojimo. Vertinamos rinkoje egzistuojančių priemonių (ekspertų, aparatinės bei programinės įrangos) kainos, priemonių atsiperkamumas, draudiko požiūris į tam tikrą technologiją bei draudiko rekomendacijos. Pavyzdžiui, draudikas draudimo sutartyje atsižvelgiant į draudėjo pajėgumus nurodo protingo elgesio standartus su iliustracijomis, kokią konkrečią programinę įrangą naudoti, praktikas, kurias reikia įgyvendinti kiekvieną mėnesį bei pateikti draudikui ataskaitas, kaip jos vykdomos.

Teisinė aplinkybė, kurią reikšminga įvertinti kibernetinių rizikų draudimo sutarties kontekste yra draudėjo pranešimo apie kibernetinės atakos įvykdymą momentas. Pagal CK 6.1012 str. 1 d. draudėjas, sužinojęs apie įvykusį draudžiamąjį įvykį, privalo pranešti draudikui sutartyje nustatytu būdu per sutartyje nustatytą terminą. Manytina, jog kibernetinių rizikų

[86] KONTAUTAS, Tomas. Draudimo sutarčių teisė. Vilnius. 2007 m. P. 127.

Taip pat draudimo taisyklėse turėtų būti aptariama ar draudikas reikalauja draudėjo nuolatos gaminti informacijos kopijas, kokiu dažniu (kas dieną, kas valandą, kartą savaitėje), kiek atsarginių kopijų reikia gaminti, ar duomenys yra užkoduojami, kas kiek laikomi keičiami slaptažodžiai, kokia yra slaptažodžių parinkimo praktika, antivirusinė apsauga bei ugniasienės. Ar draudėjas privalo reguliariai vykdyti darbuotojų kibernetinio saugumo apmokymus? Ar draudėjas turi patvirtintus reakcijos į kibernetinę ataką bei padėties atkūrimo po atakos planus.

Remiantis kelių dešimtmečių praktika ripažįstama, jog dauguma programinės įrangos yra nesaugios, todėl reikėtų taip pat draudimo taisyklėse įvertinti situacijas, kai draudėjas naudoja programinę įrangą, kuri aiškiai yra žinoma kaip turinti pažeidžiamumo taškus (angl. *vulnerabilities*)? Ar draudėjas gali toliau naudotis ta programinę įrangą ar ją privalo pakeisti analogiška, tačiau neturinčia saugumo spragų? Galioja praktika, jog paklausiai programai turint trūkumų, ji nėra atnaujinama, o išleidžiama naują versija gamintojams nepatiriant atsakomybės, todėl draudėjai patirtų didelių kaštų. Ar dėl neegzistuojančios saugios analogiškos programinės įrangos bendrovė turi nutraukti veiklą, o draudėjas turi padengti su verslo nutrūkimu patirtus nuostolius?

3.3. Draudiko pareiga sumokėti draudimo išmoką

Kaip minėta kibernetinių rizikų draudimo išmoka siejama su faktiškai atsiradusiais draudėjo nuostoliais įvykus draudžiamajam įvykiui. Įvykus draudžiamajam įvykiui draudėjas turi tai užfiksuoti draudiko reikalaujamuose dokumentuose. Pavyzdžiui, policijos protokole, darbuotojų bei liudytojų parodymais, fiksuotais garso bei vaizdo įrašais, nuotraukomis, ekspertų išvadomis. Draudikas turi pareigą tinkamai ištirti įvykusį draudžiamąjį įvykį ir išmokėti draudiminę išmoką (Draudimo įstatymo 82 str.). Taip pat draudikas gali pareikalauti draudėjo papildomos informacijos, kuri draudiko manymu yra reikšminga vertinti įvykusį draudžiamąjį įvykį, arba rinkti informaciją apie draudėją kreipiantis į bet kuriuos juridinius asmenys, kurie gali pateikti su draudžiamojo įvykio išaiškinimu siejamą informaciją, pasisamdyti nepriklausomus ekspertus įvykio ištyrimui.

Draudimo sutarties pagrindu draudėjas perduoda draudžiamojo įvykio atsiradimo riziką draudikui. Tai reiškia, jog draudikas iš visų jo draudėjų draudimo įmokų sumų (ne tik iš besikreipiančio draudėjo įmokų) pagal draudimo sutartyje numatytas sąlygas išmoka draudėjui jo patirtų nuostolių dydžio ekvivalentinę draudimo išmoką. Tokiu būdu rizika paskirstoma draudėjams, o nuostolių nepatyrę kiti draudėjai solidarizuojasi su nuostolius patyrusiu draudėju[87].

Pagal draudimo sutarties išmokos pobūdį draudimo sutartys skirstomos į nuostolių bei sumų draudimų sutartis[88]. Nuostolių draudimo sutartimi draudikas įsipareigoja išmokėti draudimo išmoką, kuri yra lygi patirtų nuostolių dydžiui bei negali būti didesnė jokiu atveju, o sumų draudimu įsipareigojama išmokėti sutartyje sutarta išmoką nepriklausomai nuo patirtų nuostolių dydžio. Sumų draudimo sutartis paprastai sudaromos apdraudžiant tokias rizikas, dėl kurių padarinių specifikos nėra įmanoma tiksliai apskaičiuoti patirtos žalos dydžio. Todėl, pavyzdžiui, gyvybės, reputacijos draudimuose iš anksto susitariama dėl išmokos dydžio pagal draudėjo subjektyvųjį vertinimą bei įvykus draudžiamajam įvykiui nėra skaičiuojamas patirtų nuostolių dydis.

Draudikas turi pareigą visapusiškai ištirti draudžiamąjį įvykį ne tik remiantis draudėjo pateiktais dokumentais draudikas, bet ir pačiam atliekant įvykio tyrimą tam, kad tiksliai apskaičiuotų draudimo išmoks dydį. Draudimo išmokos dydis priklauso nuo draudimo sumos, apdrausto turto vertės, dėl draudžiamojo įvykio patirtų nuostolių dydžio bei kitas su draudžiamuoju įvykiu susijusias aplinkybes. Draudimo išmoka privalo būti išmokėta ne vėliau kaip per 30 dienų nuo tos dienos, kai gaunama visa informacija, reikšminga nustatant draudžiamojo įvykio faktą, aplinkybes, pasekmes ir draudimo išmokos dydį[89]. Pažymėtina, jog šis terminas nėra naikinamasis, t. y. draudikas gali šį terminą pratęsti laikantis tam tikrų sąlygų bei aplinkybių. Termino pratęsimas turi būti pateisinamas objektyviu negalėjimu per 30 dienų nuo draudžiamojo įvykio datos pilnai ištirti draudžiamąjį įvykį bei apskaičiuoti draudimo išmoką, o draudikas privalo raštu kas 30 dienų informuoti draudėją apie tyrimo eigą bei priežastis, dėl kurių tyrimas negalėjo būti laiku užbaigtas, kokie tyrimo veiksmai jau yra atlikti, kokius veiksmus ketinama atlikti, kokia informacija reikalinga surinkti tolesnei tyrimo eigai atlikti[90].

[87] KONTAUTAS, Tomas. Draudimo sutarčių teisė. Vilnius. 2007 m. P. 24.
[88] Ibid p. 38.
[89] Lietuvos Respublikos Draudimo įstatymo 98 str. 2d. Valstybės žinios, 2003, Nr. 94-4246.Draudimo įstatymo 98 str. 2 d.
[90] Ibid 98 str. 9 d.

Remiantis statistika, vidutinis laikas, kurio reikia pilnai ištirti kibernetinę ataką yra 32 dienos, o toks tyrimas vidutiniškai kainavo 1 milijoną JAV dolerių[91]. Vertinant 2014 metų informaciją su 2013, tyrimo kaina padidėjo 55 procentai nuo 591,780 JAV dolerių. O kartais panaikinti kenksmingą programinę įrangą gali užtrukti ir iki 65 dienų[92].

Pranešimo apie draudžiamąjį įvyki terminas nėra reglamentuojamas įstatymų. Paprastai šis terminas yra šalių susitarimo reikalas ir jis nebūna ilgesnis nei 14 dienų po atakos momento. Pranešimo termino nesilaikymas yra susitarančių šalių reikalas. Jis gali lemti atsisakymą išmokėti draudimo išmoką arba draudimo išmokos mokėjimo sumažinimą[93]. O dėl didelio neatsargumo atsisakyti išmokėti turto draudimo išmoką galima tik tuo atveju, jeigu tokie atvejai individualiai aptarti ir numatyti draudimo sutartyje[94].

Konkreti žala kibernetinių atakų yra padaroma aparatinės bei programinės įrangos veikimo sutrikimais, naivių darbuotojų neprotinga veikla su bendrovės technika bei veiksmai darbdavio patalpose, pavyzdžiui: darbuotojas ar jo šeimos narys atėjęs aplankyti darbuotojo prie darbdavio tinklo prisijungia su ne darbo poreikiais naudojamu išmaniuoju telefonu, kuriame yra patalpinta besidauginanti kenksminga programinė įranga, darbo poreikiais naudojamas nešiojamas kompiuteris ar USB atmintinė komandiruotės metu buvo pamestas arba pavogtas, kuriame yra vertingos juridiniui asmeniui priklausančios informacijos (klientų elektroninio pašto adresai, gyvenamosios vietos, asmens kodai, slaptažodžiai ir kt.), įsilaužėlis į sistemą įveda tikrovės neatitinkančius duomenis dėl kurių jis įgauna finansinius išteklius, elektroninio laiško su kenksminga programine įranga atidarymas, fizinis kenksmingos programinės įrangos implantavimas. Remiantis statistika teigtina, jog 43 procentų patiriamos žalos sudaro duomenų praradimas, 36 procentai sudaro verslo vykdymo sutrikdymas, 17 procentai sudaro pajamų praradimas dėl kibernetinių atakų, 4 procentai sudaro aparatinės ir programinės įrangos gedimai[95].

Vertinant ne materialią žalą, kurią patyrė draudėjas, nuostoliai apskaičiuojami pagal valandinį darbuotojų įkainį, kurie yra įpareigoti atstatyti iki kibernetinės atakos buvusią padėtį. Pavyzdžiui, laikas reikalingas surinkti ir įvesti į duomenų bazę atitinkamą informaciją. Duomenų praradimo atveju žala vertinama atsižvelgiant į ekspertų išlaidos tyrimams atlikti, reklamos kaštai

[91] HARTWIG, Robert, Ph.D., CPCU. Cyber risks: the growing threat. Insurance informatikon institute. 2014. P. 10.
[92] Ibid.
[93] Lietuvos Respublikos Civilinis kodekso 6.1012 str. 2 d.. Valstybės žinios, 2000, Nr.74-2262.
[94] Lietuvos Respublikos Draudimo įstatymo 106 str. Valstybės žinios, 2003, Nr. 94-4246.
[95] Cost of Cyber Crime: United States, Ponemon Institute. 2013. [interaktyvus]. [Žiūrėta 2016-03-01]. <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf>.

dėl klientų informavimo, klientams suteikiamos nuolaidos ateities produktams ir paslaugoms, negautos pajamos dėl klientų praradimo[96].

Taip pat pažymėtina, jog kibernetinių rizikų padaroma žala jos atsiradimo momentu nėra galutinė, nes visada lieka galimybė, jog žala bus daroma ateityje panaudojant tą pačią informaciją, kuri buvo gauta kibernetinės atakos metu, nes dauguma klientų ir darbuotojų yra linkę naudoti tuos pačius saugumo duomenis ne tik darbo reikmėms naudojamiems slaptažodžiams, bet ir asmeniniams elektroniniams paštams[97].

[96] Cost of a Data Breach Study: Global Analysis, the Ponemon Institute, sponsored by IBM, May 2014.
[97] ULSCH, Mac Donnel. Cyber threat. How to manage the growing risk of the cyber attacks.2014. P. 106.

IŠVADOS

1. Draudimo teisė yra privatinės teisės institutas, dėl to kibernetinių rizikų draudimo sutarties turinį lemia draudiko ir draudėjo derybiniai pajėgumai. Paskatos dėl skirtingų kibernetinių rizikų draudimo sutarčių sąlygų kyla iš draudėjo ūkinės komercinės veiklos specifiškumo, taikomų kibernetinių rizikų valdymo praktikų bei disponuojamų finansinių pajėgumų kibernetinių rizikų draudimui įsigyti.
2. Siekiant nustatyti kibernetinių rizikų draudimo turinį bei rinkai siūlyti kibernetinių rizikų draudimą didžiausia problema su kuria susiduria draudikai yra informacijos trūkumas apie kibernetinių rizikų įvykimo tikimybes bei padaromą žalą.
3. Didžiausia problema su kuria susiduria draudikai yra draudimo taisyklėse nepakankamai detalizuoti draudžiamieji bei nedraudžiamieji įvykiai, dėl to draudiko atsakomybė draudėjo atžvilgiu gali būti per ne lyg didelė. Manytina, jog siekiant teisinio aiškumo kibernetinių rizikų draudimo taisyklėse reikėtų konkrečiai nurodyti draudžiamuos ir nedraudžiamuosius įvykius išvardijant kibernetinių atakų metodus bei pateikiant iliustracijas.
4. Draudėjas, prieš sudarydamas kibernetinių rizikų draudimo sutartį turėtų įvertinti nuo kokių kibernetinių rizikų jis gali apsaugoti pasitelkdamas kibernetinio saugumo darbuotojų apmokymais bei investuojant į apsaugines technologines priemones, bei nuo kokių kibernetinių rizikų draudėjas negali apsisaugoti ir kokia apimtimi neigiamus kibernetinių rizikų padarinius jam finansiškai apsimoka perduoti draudikui.
5. Remiantis tuo, kad neegzistuoja vieninga teismų praktika dėl elektroninių duomenų kaip materialaus turto, teisės doktrinoje vyrauja pozicija, jog draudėjas turėtų siekti, kad draudimo taisyklėse *expressis verbis* būtų apibrėžtas apdraudžiamas turtas.

ŠALTINIŲ SĄRAŠAS

1. Teisės norminiai aktai.

1.1.Įstatymai.

a) Lietuvos Respublikos Civilinis kodeksas (su papildymais ir pakeitimais). Valstybės žinios, 2000, Nr.74-2262.

b) Lietuvos Respublikos Draudimo įstatymas (su papildymais ir pakeitimais). Valstybės žinios, 2003, Nr. 94-4246.

c) Lietuvos Respublikos Administracinės teisės pažeidimų kodeksas (su papildymais ir pakeitimais). Valstybės žinios, 1985, Nr. 1-1.

1.2.Konvencijos.

a) United Nations convention against transnational organized crime and the protocols thereto, United Nations, New York, 2004.

2. Specialioji literatūra.

a) Kontautas, Tomas. Draudimo sutarčių teisė. Vilnius. 2007 m.

b) George Loukas. Cyber-Physical Attacks, A growing invisible threat. 2015.

c) 2014 Cost of a Data Breach Study: Global Analysis, the Ponemon Institute, sponsored by IBM, May 2014.

d) Paul Ferrillo, Weil, Gotshal and Manges LLP. Cyber Security, Cyber Governance, and Cyber insurance. Harvard law journal. 2014.

e) Tony Blunden and John Thirlwell. Mastering operational risk. 2010.

f) Cost of Cyber Crime: United States, Ponemon Institute. 2013. [interaktyvus]. [Žiūrėta 2016-03-01]. <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf>.

g) S. Waterman. 'US-Israeli cyberattack on Iran was "act of force", NATO study found', Washington Times. 2013. [Interaktyvus]. [Žiūrėta 2016-03-01]. <http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-oniran-was-act-of-force-na/?page=all>.

h) Is Computer Data "Tangible Property" or Subject to "Physical Loss or Damage"? Michael Rossi. 2001. [Interaktyvus]. [Žiūrėta 2016-03-03]. <https://www.irmi.com/articles/expert-commentary/is-computer-data-tangible-property-or-subject-to-physical-loss-or-damage-part-1>.

i) Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide. 2013. [interaktyvus]. [Žiūrėta 2016-03-03]. <http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide?ClickID=clzvvllsepsiffqeknvqxa4x4vqkwvslznqn>.

j) Robert P. Hartwig, Ph.D., CPCU. Cyber risks: the growing threat. Insurance informatikon institute. 2014.

k) The Case for Cybersecurity Insurance, Part II. [Interaktyvus]. [Žiūrėta 2016-03-03]. <http://krebsonsecurity.com/2010/07/the-case-for-cybersecurity-insurance-part-ii/>.

l) Norton Cybercrime report 2011. [Interaktyvus]. [Žiūrėta 2016-03-05]. <http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport.>.

m) R. Anderson, R. Boehme, R. Clayton, and T. Moore. Security economics and european policy. In Proceedings of WEIS'08, Hanover, USA, Jun. 25-28 2008.

n) Average costs of cyber crime in selected countries as of August 2015 (in million U.S. dollars). [interaktyvus]. [Žiūrėta 2016-03-02]. <http://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/>.

o) Robert Lemos, Should SMBs Invest in Cyber Risk Insurance? 2010. [interaktyus]. [Žiūrėta 2015-12-17] < http://www.darkreading.com/smb-security/167901073/security/ security-management/227400093/index.html>.

p) Allianz Risk Barometer on Business Risks 2014. [interaktyvus]. [Žiūrėta 2016-03-10]. < http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2014_EN.pdf>.

q) The first ISP. [Interaktyvus]. [Žiūrėta 2016-02-25]. <http://www.indra.com/homepages/spike/isp.html>.

r) Previous cases of missing data. BBC News. 2009. [interaktyvus]. [Žiūrėta 2016-03-05}. <http://news.bbc.co.uk/1/hi/uk/7449927.stm>.

s) Philip Rawlings. Cyber risk: insuring the digital age. Queen Mary University of London. 2015.

t) Bank hackers steal millions via malware. The New York Times. 2015. [interaktyvus]. [Žiūrėta 2016-03-03]. < http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html>.

u) Lawrence A Gordon et al. CSI/FBI Computer Crime and Security Survey, COMPUTER SEC. INST. 2006. [interaktyvus]. [Žiūrėta 2016-03-06]. <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf>.

v) Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime. 2014. [interaktyvus]. [žiūrėta 2016-03-06]. <http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf>.

w) Veras, R., Collins, C., and Thorpe, J. On the semantic patterns of passwords and their security impact. In Network and Distributed System Security Symposium. 2014.

x) Bellovin, S. M. and Cheswick, W. R. (1994). Network firewalls. Communications Magazine, IEEE, Volume 32, No. 9. 1994. P. 57.

y) Airmic Review of recent developments in the cyber insurance market, 2012. [interaktyvus]. [Žiūrėta 2016-03-03]. <http://docplayer.net/15695701-Airmic-review-of-recent-developments-in-the-cyber-insurance-market-commentary-on-the-increased-availability-of-cyber-insurance-products-guide.html>.

z) S&P to consider cyber security in bank credit ratings. 2015. [interaktyvus]. [Žiūrėta 2016-03-01] <http://www.ft.com/fastft/2015/09/29/sandp-consider-cyber-security-bank-credit-ratings/>.

aa) American Bankers Association, Target Breach Impact Survey. 2014. [Interaktyvus]. [Žiūrėta 2016-03-01] < http://www.aba.com/Tools/Function/Payments/Documents/TargetBreachBankImpact.pdf >.

bb) Lee, E. A. Cyber physical systems: Design challenges. 2008. P. 363.

cc) Barbarians at the Digital Gate. Its cyberattacks show the world the nature of the Chinese regime. [interaktyvus]. [Žiūrėta 2016-02-25]. <http://www.wsj.com/articles/SB10001424127887323701904578275920521747756>.

dd) Travelers sues PF Chang's to avoid paying breach costs, Business Insurance, J. Greenwald 2014. [interaktyvus]. [Žiūrėta 2016-01-15]. < http://www.pfchangs.com/security/>.

ee) ERGO Insurance SE Lietuvos filialo Elektronikos draudimo taisyklės Nr. 018. Galioja nuo 2014-08-01.

ff) ERGO Insurance SE Lietuvos filialo Verslo nutrūkimo draudimo taisyklės Nr. 058. Galioja nuo 2014-08-18.

gg) Insurers fight to bar cyber coverage under commercial general liability policies. Business Insurance, J. Greenwald. 2014. [interaktyvus]. [Žiūrėta 2016-01-18]. < http://www.businessinsurance.com/article/20141026/NEWS07/141029850/insurers-fight-to-bar-cyber-coverage-under-commercial-general>.

hh) Mac Donnel Ulsch. Cyber threat. How to manage the growing risk of the cyber attacks.2014. P. 106.

ii) Cisco Systems Inc., "The Internet of Things,". [interaktyvus]. [Žiūrėta 2016-02-15]. <http://share.cisco.com/internetof-things.html>.

jj) The History Of Insurance by Andrew Beattie. [interaktyvus]. [Žiūrėta 2016.02.15]. <http://www.investopedia.com/articles/08/history-of-insurance.asp>.

kk) The history of insurance. [interaktyvus]. [Žiūrėta 2016.02.15] <https://www.esurance.com/info/car/the-history-of-car-insurance>.

ll) Sarah Veysey. Data scarce for insurers covering cyber risks [interaktyvus]. [Žiūrėta 2016-01-20]. <http://www.businessinsurance.com/article/20150610/NEWS06/150619981>.

mm) Eurostat. Internet use statistics – individual [interaktyvus]. [žiūrėta 2016-01-20]. <http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_use_statistics_-_individuals>.

nn) World Economic Forum. Global risks 2011 Sixth edition, An initiative of the Risk Response Network; World Economic Forum. Global risks 2014 Ninth edition.

oo) *Anderson, Ross; Moore, Tyler. The economics of information security: A survey and open questions. University of Cambridge Computer laboratory. 2006.*

pp) European Network and Information Security agency. Incentives and barries of the cyber insurance market in Europe. June 2012.

3. Praktinė medžiaga.
   a) Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus nutartis civilinėje byloje nr. 3K-3-1445/2002.
   b) Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus nutartis civilinėje byloje nr. 3K-3-1029/2003.
   c) Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus nutartis civilinėje byloje nr. 3K-3-911/2002.
   d) Lietuvos Aukščiausiojo Teismo 2000 m. gegužės 3 d. nutartį civilinėje byloje UAB „Pozicija“ v. AB „Lietuvos draudimas“, bylos Nr. 3K-3-486/2000;
   e) 2001 m. birželio 7 d. nutartį civilinėje byloje AB „Lietuvos draudimas“v. I. Z. N., bylos Nr. 3K-7-397/2001;
   f) 2003 m. gegužės 5 d. nutartį civilinėje byloje UAB „Vigidas“ v. UAB DK „Censum“, bylos Nr. 3K-3-546/2003.
   g) Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus nutartis civilinėje byloje nr. 3K-3-746/2003.
   h) United States District Court of Louisiana. Landmark American Insurance Company v. Gulf Coast Analytical Laboratories, Inc., No. 3:2010cv00809 - Document 45 (M.D. La. 2012).
   i) NMS Services, Inc v Hartford 62 Fed Appx 511 (CA4 (Va), 2003).
   j) Lambrecht & Associates, Inc v State Farm Lloyds 9 119 SW3d 16 (Tex App,2003).
   k) Retail Ventures, Inc v National Union Fire Ins Co of Pittsburgh, Pa 691 F3d 821 (CA6 (Ohio), 2012)
   l) *Eurostat. E-business integration. November 2015. [interaktyvus]. [žiūrėta 2016-03-29]. <http://ec.europa.eu/eurostat/statistics-explained/index.php/E-business_integration>.*
   m) State of Michigan Court of appeals. Audrey Bell vs. Dentry Berry. 2005.
   n) United States District Court, W.D. Oklahoma. STATE AUTO PROPERTY AND CASUALTY INSURANCE COMPANY, Plaintiff, v. MIDWEST COMPUTERS & MORE, Defendant. 147 F. Supp. 2d 1113 (2001).

o) Court of Appeals of Minnesota. Retail Systems v. CNA Ins. CompaniesAnnotate this Case 469 N.W.2d 735 (1991).

SANTRAUKA

Kibernetinių rizikų draudimas yra viena iš naujausių draudimo sutarčių rūšių, kuri pasižymi savo dalyko specifiškumu – kibernetinėmis rizikomis. Kibernetinės rizikos – tai tikimybių visuma, kurios lemia neigiamas pasekmes bei žalos atsiradimą per kibernetinę erdvę įvykdomas kibernetines atakas. Kibernetinių rizikų draudimo sutartimis asmenys už tam tikrą atlygį siekia pernešti savo kibernetinę riziką draudimo bendrovėms taip siekiant sumažinti arba išvengti kibernetinių atakų neigiamų finansinių padarinių. Nors ir egzistuoja įvairios priemonės, kurios padeda sumažinti kibernetines rizikas kaip ugniasienės, anti-virusinės programos, protingo elgesio kibernetinėje erdvėje gerosios praktikos, įsilaužimų atpažinimo sistemos ir kt., tačiau nepaisant net ir patobulėjusiai kibernetinės apsaugos programinei įrangai bei elektroninių duomenų užkodavimo metodams, dėl atakų specifiškumo bei jų gebėjimo prisitaikyti prie naujų apsaugos metodų, kibernetinių rizikų nėra įmanoma visiškai išvengti.

Siekiant nustatyti kibernetinių rizikų draudimo turinį didžiausia problema su kuria susiduria draudikai yra informacijos trūkumas apie kibernetinių rizikų įvykimo tikimybes bei padaromą žalą. O didžiausia problema su kuria susiduria draudėjai yra draudimo taisyklėse nepakankamai detalizuoti draudžiamieji bei nedraudžiamieji įvykiai. Manytina, jog siekiant teisinio aiškumo kibernetinių rizikų draudimo taisyklėse reikėtų konkrečiai nurodyti draudžiamuosius ir nedraudžiamuosius įvykius išvardijant kibernetinių atakų metodus bei pateikiant iliustracijas.

Draudėjas, prieš sudarydamas kibernetinių rizikų draudimo sutartį turėtų įvertinti kokias rizikas jis gali apsaugoti pasitelkdamas kibernetinio saugumo darbuotojų apmokymais bei investuojant į apsaugines technologines priemones, bei nuo kokių kibernetinių rizikų draudėjas negali apsisaugoti ir kokia apimtimi neigiamus kibernetinių atakų padarinius jam finansiškai apsimoka perduoti draudikui.

SUMMARY

Cyber Risk Insurance Contract

Cyber risk insurance is one of the newest kind of insurance, which distinguishes by its object – cyber risks. Cyber risks are the probability of financial damages caused by cyber-attacks in cyber space. Cyber risk insurance contract is used for insured, for a certain amount of pay, to move its risk to the insurer, and manage their cyber risk financial losses. Even though many different methods to manage cyber risks exist, like using firewalls, anti-virus programs, cyber security policies, however regardless newer and better cyber security technology and encryption, because of very specialized cyber-attacks cyber risk is not possible to be fully avoided by any means.

When deciding the cyber risk insurance contract matter the biggest problem that insurers face is information asymmetry about cyber risk occurrence probabilities and caused damage. And the biggest problem insureds face is not being able to unambiguously detail insured and not insured events. It is believed, that for the sake of legal clarity, cyber risk insurance contracts must have precisely indicate all insured and not insured events, provided with insured cyber-attack methods and illustrations.

The insured, before signing cyber risk insurance contract should estimate what kind of cyber risks he can safeguard by providing cyber security training for his employees and investing in cyber security technology, from what kind of cyber risks the insured cannot take precautions and what kind of cyber risks it is financially advisable to insure.