MYKOLO ROMERIO UNIVERSITETAS

EKONOMIKOS IR VERSLO FAKULTETAS

LINA LELEŠIENĖ

Kibernetinio saugumo valdymas

KIBERNETINIO SAUGUMO PRIEMONĖS IR METODAI BANKŲ VEIKLOS RIZIKŲ VALDYMUI

Magistro baigiamasis darbas

Darbo vadovas –

Prof. dr. Tadas Limba

Vilnius, 2020

MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR VERSLO FAKULTETAS

KIBERNETINIO SAUGUMO PRIEMONĖS IR METODAI BANKŲ VEIKLOS RIZIKŲ VALDYMUI

Kibernetinio saugumo valdymo magistro baigiamasis darbas
Studijų programa 6211LX066

Vadovas
Prof. dr. T. Limba

Atliko
KSVvmis18-1 gr. stud.
L. Lelešienė

Vilnius, 2020

TURINYS

LENTELĖS

PAVEIKSLAI

ĮVADAS

Temos aktualumas ir ištirtumas. „Dabartiniais laikais, kai kibernetinių grėsmių skaičius sparčiai auga, o kibernetinių atakų, kurias naudoja nusikaltėliai, metodai tampa vis įvairesni, būtina mąstyti apie sprendimus, kurie kompleksiškai nagrinėja visus organizacijos vykdomos veiklos procesus“ (Limba ir kt., 2017). Kibernetinio saugumo klausimas tapo aktualus siekiant apsaugoti nacionalinę šalių kibernetinę erdvę. Pastaruoju metu kibernetinės atakos prieš vartotojus suaktyvėjo visame pasaulyje ir jos gali sutrikdyti gyvybiškai svarbias kasdien teikiamas paslaugas: pažeisti bankų veiklą, kenkti šalies ekonomikai, neigiamai veikti visuomenės gerovę. „Elektroninės erdvės globalumas sukūrė beprecedentes sąlygas daryti nusikaltimus iš bet kurio pasaulio taško, kuriame yra internetas. Todėl labai svarbu apsisaugoti nuo elektroninių nusikaltimų, vykdomų pasitelkiant internetą. Kibernetinis saugumas tampa vienu iš pagrindinių tikslų, turint omenyje, kad grėsmės elektroninėje erdvėje kyla ne tik atskiriems vartotojams, bet net valstybėms“ (Štitilis, 2013). „Valdžios institucijos, finansų sektorius, viešąsias ir privačias paslaugas teikiančios organizacijos savo įprastoje kasdienėje veikloje naudoja informacines technologijas bei šių technologijų sukurtus produktus. Vadinasi, visos šios organizacijos yra stipriai priklausomos nuo kibernetinio saugumo“ (Limba ir kt., 2017).

Temos naujumas. „Kibernetiniai incidentai kelia grėsmę piliečiams, atskiroms įmonėms ir organizacijoms, jų funkcionavimui, taip pat netgi pačiai valstybei. Kibernetinio saugumo valdymas tampa kertiniu elementu. Tiek Lietuvoje, tiek kitose užsienio valstybėse kuriamos naujos institucijos, naujos pareigybės, nauji teisės aktai, įvardijama kritinė infrastruktūra.“(Kibernetinio saugumo valdymas, mruni.eu, 2018) Bankai suinteresuoti diegti kibernetines saugumo priemones ir metodus, nes pinigų operacijos yra atliekamos internetu. Kibernetinis saugumas tampa neatskiriama bankų veiklos dalimi. „<...> kibernetinis saugumas yra ne tik technologinių aspektų rinkinys, bet reiškinys, kurį sudaro daug platesnis disciplinų sąrašas (Limba ir kt., 2017).“

Mokslinė problema. Mokslo šaltiniuose nepakankamai išanalizuoti subalansuoti bei suderinti kibernetinio saugumo metodai ir priemonės, kas gali daryti įtaką kibernetinio saugumo stokai bankų veiklos rizikų valdyme.

Tyrimo objektas: kibernetinio saugumo priemonės ir metodai bankų veiklos rizikų valdymui.

Tyrimo tikslas: išanalizavus kibernetinio saugumo priemonių ir metodų taikymo bei naudojimo teorinius aspektus ir atlikus kibernetinio saugumo bankų veiklos rizikų valdyme analizę, pasiūlyti Kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų bankų veiklos rizikų valdymui suderinamumo modelį.

Uždaviniai:

- išanalizuoti kibernetinio saugumo priemonių ir metodų teorinius aspektus;
- išnagrinėti JAV, Kinijos ir Baltijos šalių kibernetinio saugumo priemonių ir metodų taikymo ypatumus atvejo analizės kontekste;
- atlikti kokybinį tyrimą apklausiant tiesiogiai su kibernetiniu saugumu susijus specialistus;
- remiantis teorine analize, atliktu kokybiniu tyrimu ir gerosios pasaulio patirties analize sukurti Kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų suderinamumo modelį.

Darbo metodai. Magistro baigiamajame darbe buvo atlikta mokslinė literatūros analizė kibernetinio saugumo srityje. Buvo nagrinėjami moksliniai šaltiniai ir išanalizuoti kibernetinio saugumo priemonių ir metodų teoriniai aspektai. Septyni kibernetinio saugumo ekspertai buvo apklausti kokybinio tyrimo metodu (klausimynas, interviu). Kokybinis ekspertų tyrimas atskleidė kibernetinio saugumo priemonių ir metodų taikymo bankų veiklos rizikų valdymo pagrindines problemas, išskirti populiariausi kibernetinio saugumo priemonių ir metodų pavyzdžiai.

Darbo struktūra. darbą sudarys 4 dalys (žr. 1 pav.)

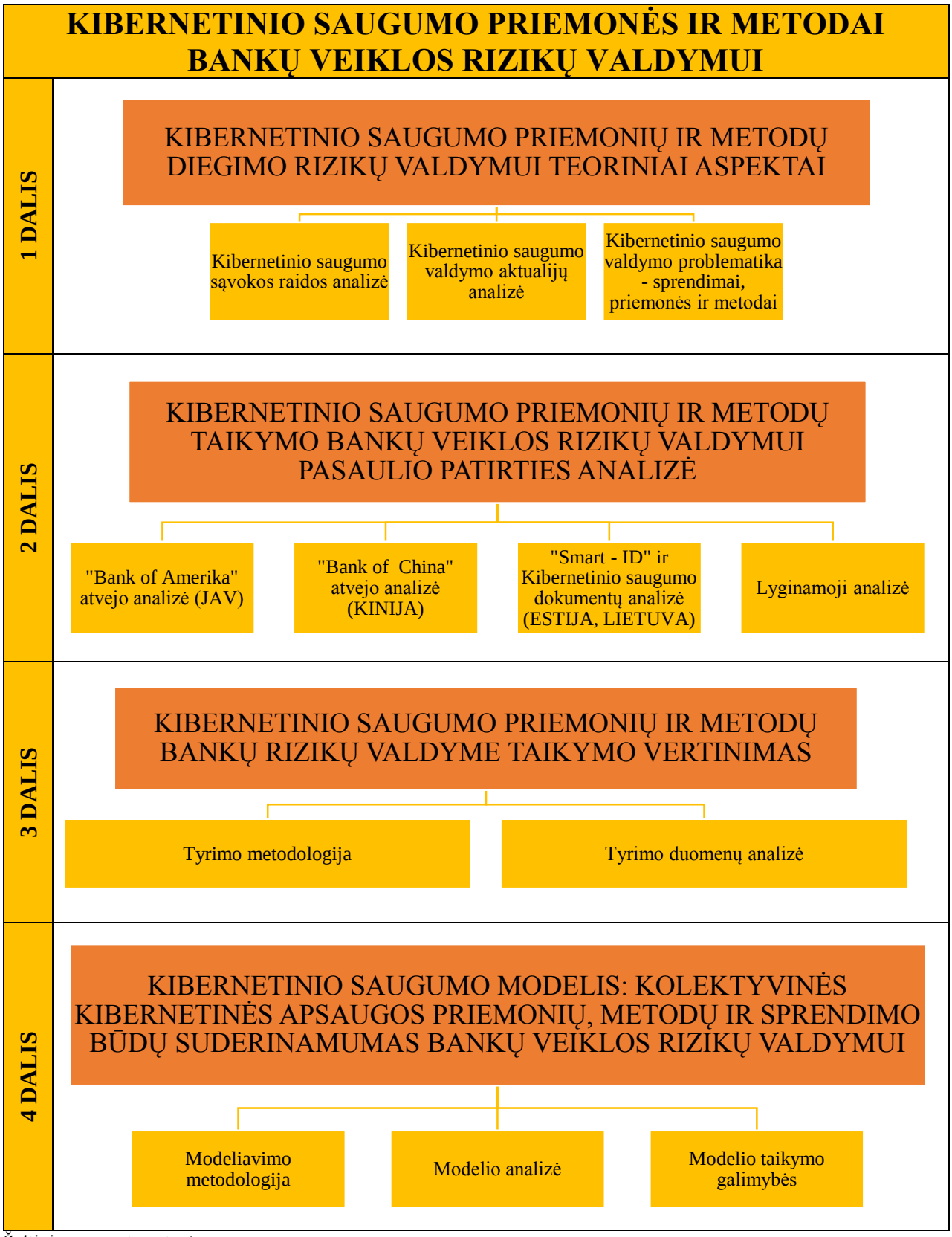
1 dalis: nagrinėjami kibernetinio saugumo priemonių ir metodų diegimo rizikų valdymui teoriniai aspektai: kibernetinio saugumo priemonių ir metodų sąvokos ir raidos analizė, kibernetinio saugumo priemonės ir metodai, kibernetinio saugumo priemonių ir metodų diegimo bankų veiklos rizikų valdymui problematika.

2 dalis: nagrinėjama kibernetinio saugumo priemonių ir metodų taikymo bankų veiklos rizikų valdymui pasaulio patirties analizė.

3 dalis: nagrinėjamas kokybinis ekspertinis tyrimas, kuriuo siekiama išsiaiškinti kibernetinio saugumo priemones ir metodus naudojamus bankuose; pagrindines sąvokas ir problemas, išskirti populiariausius kibernetinio saugumo priemonių ir metodų pavyzdžius.

4 dalis: remiantis teorine analize ir kokybinio tyrimo rezultatais, sukurti kibernetinio saugumo modelį: Kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų suderinamumas. Darbo pabaigoje pateikiami rezultatai ir išvados.

Darbo praktinis reikšmingumas. Magistrinio darbo tyrimo rezultatai gali būti pritaikyti siekiant tobulinti Lietuvos kibernetinio saugumo užtikrinimą. Praktinis reikšmingumas gali būti siejamas diegiant kibernetinį saugumą bankų rizikų valdyme pasinaudojant sukurtu Kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų bankų veiklos rizikų valdymui suderinamumo modeliu. Taip pat ekspertinės apklausos rezultatai gali būti pritaikyti tobulinant kibernetinio saugumo sritį bankuose.



Šaltinis: parengta autorės

1 pav. Magistro baigiamojo darbo struktūros loginė schema

1. KIBERNETINIO SAUGUMO PRIEMONIŲ IR METODŲ DIEGIMO RIZIKŲ VALDYMUI TEORINIAI ASPEKTAI

1.1. Kibernetinio saugumo sąvokos raidos analizė

Kibernetinio saugumo sąvoka yra svarbi bet kurioje organizacijoje, „bet kuri organizacija (viešojo ar privataus sektoriaus atstovai) ar jos struktūrinis padalinys, valdantys informacinių išteklių infrastruktūrą, o ypač kritinę infrastruktūrą, turi aiškiai suvokti, kad visiškas kibernetinis saugumas yra mitas arba, tiksliau sakant, – nepasiekiama svajonė“ (Limba ir kt., 2017). Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinis saugumas apibrėžtas kaip „visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos.“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Remiantis Užkaraityte G. (2015) „pasak Lietuvos Respublikos ryšių reguliavimo tarnybos, kibernetinis saugumas paprastai suprantamas kaip apsauga nuo neteisėtos prieigos prie informacijos, jos panaudojimo, keitimo, manipuliavimo, praradimo. Bendrąja prasme saugumas - tai būsena, kai negresia joks pavojus.“ (Užkaraitytė G., 2015)

Grincevičius R., savo disertacijoje (2019) teigia, kad „pagal Camp ir Lewis (2005), kibernetinis saugumas apima techninius, socialinius ir ekonominius aspektus ir, kadangi iš esmės jis pats yra moralinė vertybė (Nissenbaum, 2005), saugumo konceptas turi ir etinių savybių (Siponen, 2000). Saugumas turėtų būti vartojamas kartu su tokiomis sąvokomis kaip privatumas, intelektinės vertybės, lygybė. (Nissenbaum, 2005).“ (Grincevičius R., 2019)

William A. Carter, William D. Crumpler (2019) pateikia Kibernetinio saugumo apibrėžimus pasaulyje (žr. lentelė Nr. 1). Tačiau tik kai kurios šalys turi kibernetinio saugumo apibrėžimą, dalis jį aprašo arba jis yra numanomas.

1 lentelė. Kibernetinio saugumo apibrėžimai pasaulyje

Šalis	Apibrėžimas	Kibernetinis saugumas
AUS *Australija*	apibrėžimas	Priemonės, susijusios su informacijos, kuri tvarkoma, saugoma ir perduodama elektroninėmis ar panašiomis priemonėmis, konfidencialumu, prieinamumu ir integralumu.
CAN *Kanana*	aprašomas	Kibernetinėms atakoms – elektroninės informacijos ir (arba) elektroninės ar fizinės infrastruktūros, kuri naudojama tokiai informacijai tvarkyti, perduoti ir (arba) saugoti, tyčinei ar nesankscionuotai prieigai, naudojimui, apdorojimui, pertraukimui ar

		sunaikinimui (elektroninio ryšio priemonėmis) – skiriamas atitinkamas reagavimo ir (arba) sumažinimo lygis.
DEU *Vokietija*	apibrėžimas	IT saugumo situacijos, kurioje (visuotinės) kibernetinės erdvės rizika buvo sumažinta iki priimtino minimumo, pageidaujamas tikslas.
FRA *Prancūzija*	apibrėžimas	Informacinė sistema, leidžianti pasipriešinti iš kibernetinės erdvės atsirandantiems įvykiams, kurie gali pakenkti saugomų, tvarkomų ar perduodamų duomenų bei informacijos ir ryšių technologijos (IRT) sistemų siūlomų susijusių paslaugų prieinamumui, integralumui ar konfidencialumui.
GBR *Didžioji Britanija*	aprašomas	Apima tiek nacionalinių interesų apsaugą kibernetinėje erdvėje, tiek platesnės nacionalinio saugumo politikos vykdymą, pasinaudojant daugybe kibernetinės erdvės siūlomų galimybių.
IND *Indija*	apibrėžimas	Informacijos ir informacinių sistemų (tinklų, kompiuterių, duomenų bazių, duomenų centrų ir taikomųjų programų) apsaugojimo veikla su tinkamomis procesinėmis ir technologinėmis saugumo priemonėmis.
NLD *Olandija*	apibrėžimas	Neturi būti jokio pavojaus ar žalos dėl IRT sutrikimo ar sunaikinimo ar dėl IRT piktnaudžiavimo.
NZL *Naujoji Zelandija*	apibrėžimas	Tinklų, kurie kiek įmanoma labiau apsaugo kibernetinę erdvę nuo įsibrovimų, išlaiko informacijos konfidencialumą, prieinamumą ir integralumą, aptinka įvykusius įsibrovimus ir incidentus, reaguoja į juos ir atitaiso, kūrimo praktika.
ROU *Rumunija*	apibrėžimas	Normali būklė, atsirandanti pritaikius prevencines (proaktyvias) ir reagavimo (reaktyvias) priemones, kurios užtikrina elektroninės informacijos, kibernetinės erdvės viešųjų ir privačių išteklių bei paslaugų konfidencialumą, integralumą, prieinamumą, autentiškumą ir pripažinimą.
UGA *Uganda*	numanomas	Nuorodos į „informacijos saugumą“: „informacijos ir informacinių sistemų apsauga nuo neteisėtos prieigos, naudojimo, atskleidimo, trikdymo, keitimo ar sunaikinimo.“

Šaltinis: William A. Carter William D. Crumpler, 2019

Abibendrinant galima teigti, kad kibernetinio saugumo sąvokos apibrėžimų yra daug ir skirtingų. Analizuojant įvarių šalių pateiktus apibrėžimus, kai kur jis yra numanomas arba tik aprašomas. Vienas tiksliausių kibernetinio saugumo apibrėžimų buvo išskirtas Lietuvos Respublikos kibernetinio saugumo įstatyme: „visuma teisinių, informacijos sklaidos, organizacinių ir techninių

priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos.“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

1.2. Kibernetinio saugumo valdymo aktualijų analizė

„Aštuntajame dešimtmetyje, siekiant pagerinti saugumą, buvo sukurta keletas kompiuterio programavimo naujovių, tokių kaip administratoriaus privilegijos, failų sistemos leidimai ir atsitiktiniai slaptažodžiai. Kita naujovė buvo duomenų srauto tarp kompiuterių šifravimas, pvz., IBM, siekdama apsaugoti bankines operacijas, pradėjo naudoti šifravimą komerciniais sumetimais ir, reaguodama į raginimą sukurti federalinę skaitmeninę šifravimo sistemą, kurį 1974 m. paskelbė Nacionalinis standartų biuras, pasiūlė savo algoritmą. Diskusijos dėl standarto (galiausiai priimto kaip Skaitmeninis šifravimo standartas [DES]) dar kartą atkreipė visuomenės dėmesį į NSA ir pabrėžė NSA potencialą atliekant svarbų vaidmenį vyriausybės kompiuterių saugume. Tai atskleidė, koks prieštaringas gali būti šis vaidmuo. NSA buvo apkaltinta siekiu numalšinti DES konkurentus ir DES manipuliavimu įdiegti anoniminį reguliavimą, leisiantį agentūrai slapta klausytis amerikiečių. Senato specialusis žvalgybos komitetas ištyrė šiuos ieškinius ir nustatė, kad jie yra nepagrįsti, tačiau 1978 m. Komiteto personalo ataskaita vis dar yra reikšmingas pagrindas išlaikant informacijos jautrumą, susijusį su karinių ir žvalgybos agentūrų vaidmeniu saugant privačius ryšius. (JAV Senatas. 1978)

„Internetas ir vieta, kurioje jis egzistuoja (daugelis vadina tai kibernetine erdve), nuėjo ilgą kelią per gana trumpą laiką. 1990-ųjų pradžioje JAV, kai daugelis gyventojų namų kompiuteriams prijungti prie įvairių elektroninių skelbimų lentų naudojo modemus, viceprezidentas Alas Goras kalbėjo apie informacinio „greitkelio“ plėtojimą.“ (Butrimas V., 2016)

„Pasaulį apglėbė kompiuterių tinklai. Jie atvėrė neišsemiamas galimybes našiau dirbti, patogiau gyventi, įdomiau ilsėtis, efektyviau spręsti šių veiklų valdymo kibernetines problemas. Kompiuterių tinklai, informacinės technologijos gyventojams, įmonėms, įstaigoms, organizacijoms tampa veiksmingais ekonominės ir socialinės gerovės puoselėjimo įrankiais.“ (Telksnys L., 2016)

„Šiandien kibernetinis saugumas jau yra viena aktualiausių šiuolaikinės saugumo darbotvarkės temų, nes internetiniais kanalais vykdomos atakos neturi sienų, jos plinta žaibišku greičiu ir gali pridaryti didelių nuostolių.“ (Saudargas P., 2016)

Butrimas V. (2016) teigia, kad „reikia nepamiršti, kad interneto pirmasis „tinklas į tinklą“ jungimas buvo grindžiamas pasitikėjimu. Iš esmės tai prasidėjo nuo informacinių technologijų administratorių sutarimo tarpusavyje sujungti jų valdomas IT sistemas. Apsikeitimo informacija nauda buvo įvertinta iš karto. Niekas tuo metu nemanė, kad šio naujojo ryšio vartotojas blogai elgsis.“

(Butrimas V., 2016) Taip pat jis išskiria, kad „pirmasis kenkėjiškas elgesys kibernetinėje erdvėje prasidėjo nuo studentų išdaigų, kai jie išbandė bendrą koncepciją arba parodė įsilaužėlio sugebėjimus vartotojui (parodė pranešimą aukos kompiuterio ekrane: Virusas Kavos parduotuvė.“

Analizuojant „vėliau kenkėjiškas programas ėmė kurti nusikaltėliai, siekdami užsidirbti, pradedant nuo brukalų, kai siūlomos pardavimo paslaugos iki tokio ardomojo elgesio, kaip pavyzdžiui, dokumentų ir duomenų gadinimas aukos kompiuteryje.“ (Butrimas V., 2016)

Naujausioje NKSC saugumo būklės ataskaitoje (2020) teigiama, kad „Lietuvoje 2019 m. registruotas 3 241 kibernetinis incidentas, kai jų tyrimams atlikti reikėjo tiesioginio specialistų dalyvavimo. Automatinėmis priemonėmis apdorotų kibernetinių įvykių skaičius Lietuvos IP rėžyje siekė daugiau kaip 300 000.“(NKSC būklės ataskaita, 2020)

BDO (Binder Dijker Otte) tarptautinis viešosios apskaitos tinklas savo 2017 m. ataskaitoje apie kibernetinį saugumą bankų rizikų valdyme išskiria kelias pagrindines temas ir jas išsamiai aprašo: pagrindiniai faktai, apžvalga, pasaulinės tendencijos, iššūkiai ir saugumo perspektyvos:

Pagrindiniai faktai

Šiandien klientų lūkesčiai, technologinės galimybės, norminiai reikalavimai, demografija ir ekonomika – tai pagrindiniai esminių pokyčių veiksniai, dėl kurių bankų įstaigoms iškyla poreikis įveikti šiuos iššūkius ir saugumui pritaikyti veiksnius metodus. Bankininkystės pramonėje pastebimas žymus pokytis, kaip klientai tvarko savo operacijas. Sparčiai populiarėja skaitmeninių kanalų, tokių kaip internetinė bankininkystė, skaitmeninės piniginės, mobilioji bankininkystė, bankomatai, naudojimas. Dėl to padidėja neapsisaugojimas, taigi ir kibernetinės atakos, galinčios padaryti finansinių ir reputacijos nuostolių. Bankai gali prarasti klientų pasitikėjimą, o tai tik dar labiau sustiprins daromą poveikį. Pagrindiniai veiksniai, dėl kurių bankams būtina investuoti į saugumą, yra šie:

- Finansinių duomenų, įskaitant kortelių duomenis, asmenį identifikuojančią informaciją ir kt., praradimo padidėjimas.
- Neteisėta prieiga prie banko tinklo ir sistemų. (BDO, 2017)

Apžvalga

Didėjant kibernetinių grėsmių rizikai, bankai susiduria su precedento neturinčiu duomenų pažeidimų iššūkiu ir dėl to stiprina savo pozicijas kibernetinio saugumo kontekste. Kibernetinio saugumo požiūriu pastebimos bankininkystės pramonės tendencijos:

- Finansų sektorius, palyginus su kitomis pramonės šakomis, patyrė beveik tris kartus daugiau kibernetinių atakų.
- Dėl duomenų pažeidimų (tiek dėl vidinių sukčiavimo atvejų, tiek dėl išorinių pažeidimų dėl kibernetinių nusikaltėlių atakų) proporcingai didėja išlaidos. (BDO, 2017)
- Apskaičiuota, kad kibernetinio saugumo infrastruktūros diegimo ir tvarkymo išlaidos iki 2025 m. padidės daugiau kaip 40%.
- Didėja biometrinis atpažinimas ir tokenizacija, nes bankai pradėjo suprasti, kad šios kontrolės priemonės yra ne tik mokėjimų sprendimo būdas, bet ir pasitarnauja neskelbtinų asmens duomenų saugumui.
- Klientai naudoja biometrinį atpažinimą bankinei veiklai, tokiai kaip mobiliosios bankininkystės autentifikavimas, operacijos bankomatuose ir mokėjimai.
- Kadangi skaitmeniniai kanalai tampa pirmenybiniu klientų pasirinkimu bankinių paslaugų srityje, bankams taip pat reikės pasitelkti pažangius autentifikavimo ir prieigos kontrolės procesus, nepakenkiant klientų patirčiai. (BDO, 2017)

Pasaulinės tendencijos

- Augant technologijų plėtrai, bankininkystės pramonė vystosi nepaprastai sparčiai. Nepilotuojamos oro sistemos, daiktų internetas, artimojo lauko ryšių technologija (NFC) ir išmanieji vietos aptikimo prietaisai („Nearables“) - tai keletas technologinių pasiekimų, kuriuos bankai turės apsvarstyti artimoje ateityje.
- Keletas iš svarbiausių būsimų bankų prioritetų galėtų būti debesų platformos, robotizuotų procesų automatizavimas ir pažintinės technologijos. Automatizavimas užtikrins naują efektyvumą per visą saugumo gyvavimo ciklą, tačiau tam reikia sukurti kontrolės mechanizmus ir tvirtą valdymą. (BDO, 2017)

Iššūkiai

Proporcingas skaitmeninių mokėjimų platformos augimas pasaulyje ir postūmis į ekonomiką be grynųjų pinigų vėl atkreipė dėmesį į poreikį sustiprinti kibernetinio saugumo padėtį. Keletas pagrindinių iššūkių, su kuriais susiduria bankai, yra tokie:

- **Griežti atitikties nuostatai**: Bankams tapo nepaprastai sudėtinga suvaldyti norminių aktų laikymąsi. Per pastaruosius kelerius metus labai išaugo reglamentų skaičius. Ne tik didesnieji bankai, bet ir mažesnieji privalo vykdyti norminius įsipareigojimus.
- **Pastangos apsaugoti klientų duomenis**: Yra keletas būdų, kaip bankininkystės sektoriuje gali būti pažeidžiamas privatumas: pavogti ar pamesti kortelių duomenys, neteisėtas duomenų pasidalinimas

su trečiosiomis šalimis ir kliento asmens duomenų praradimas dėl netinkamų saugumo priemonių.
- **Trečiųjų šalių rizika**: Bankai turi atlikti trečiųjų šalių, su kuriomis jie yra susiję, išsamų patikrinimą. Pagal „Payments“ kortelių pramonės duomenų saugos standartą, trečiosios šalys turi pranešti bankui apie visas su kortelių duomenų aplinka susijusias svarbias problemas.
- **Besivystančios kibernetinės grėsmės aplinka**: Technologijų plėtra lemia naujausias kibernetines grėsmes, tokias kaip naujos kartos išpirkos prašančios programos, interneto atakos ir kt.
- **Operacijų sukčiavimai**: Turėtų būti įdiegtos sukčiavimo aptikimo technologijos, tinkamai įvertinant verslo faktoriaus pagrįstą riziką.
- **Saugus SDLC**: Bankininkystės produktuose ir taikomosiose programose bankai turi integruoti SDLC apsaugą. (BDO, 2017)

Saugumo aptarimas

Nors kiekvienas bankas skirtingai pritaiko įvairius metodus, būtina manyti, kad saugumo tema išliks ta pati įvairiems bankų kanalams:

Internetinė bankininkystė: Gali būti svarstomos tokios saugos kontrolės priemonės kaip kelių faktorių autentifikavimas, stiprių slaptažodžių kūrimas, adaptyvusis autentifikavimas, vaizdo autentifikavimas ir kt.

Mobilioji bankininkystė: Turėtų būti užtikrinta, kad mobiliosios programos yra atnaujintos ir išbandytos. Galima būtų įgyvendinti naujausius užgrūdinimo standartus.

Piniginės operacijos: Turėtų būti įtraukta informavimo apie duomenų vagystę, kenkėjiškų programų išpuolius, duomenų vagystę telefonu ir socialinę inžineriją, slaptažodžių saugą ir kt. medžiaga.

Bankomatų saugumas: Bankai turėtų įdiegti tokius biometrinius duomenis kaip akių tinklainė, balso nuskaitymas ar pirštų atspaudų nuskaitymas.

UPI (vieninga mokėjimo sąsaja): Bankai ir MPT turi apgalvoti savo saugumo strategijas, valdymo modelius ir numatomąją kontrolę, kad sukurtų saugią UPI aplinką, kuri užtikrintų sklandžią vartotojo patirtį ir tuo pačiu subalansuotų saugumo riziką. (BDO, 2017)

Apibendridant galima daryti išvadas, kad augant technologijų plėtrai, bankininkystės pramonė vystosi nepaprastai sparčiai, klientų lūkesčiai, technologinės galimybės, norminiai reikalavimai, demografija ir ekonomika – tai pagrindiniai esminių pokyčių veiksniai, dėl kurių bankų įstaigoms iškyla poreikis įveikti šiuos iššūkius ir saugumui pritaikyti veiksnius metodus. Pagrindiniai iššūkiai, su kuriais susiduria bankai: griežti atitikties nuostatai, pastangos apsaugoti klientų duomenis, trečiųjų šalių rizika, besivystančios kibernetinės grėsmės aplinka bei operacijų sukčiavimai.

1.3. Kibernetinio saugumo valdymo problematika - sprendimai, priemonės ir metodai

Sprendimo būdai	
Priemonės	**Metodai**
Draudimas nuo kibernetinių rizikų *(angl. Cyber Insurance)*	**Nuspėjamoji analitika** *(angl. Predictive Analytics)*
Klaidų aptikimo programos *(angl. "Bug Bounties")*	**Atsarginių duomenų kopijų kūrimas** *(angl. Back up Critical Data)*
Technologinės priemonės: • ***Žiniatinklio programos ugniasienė*** *(angl. Web Application Firewall)* • ***Komutatorius*** *(angl. Network switch)* • ***Serveris*** *(angl. Radius - Remote AAA)* • ***IDS apsaugos sistemos*** *(angl. IDS Intrusion Detection System)* • ***Tinklo prieigos valdymo standartas*** *(angl. IEEE 802.1X)* • ***„Wi-Fi" sauga*** *(angl. Wi-fi network encryption WEB (WPA2, WPA3)* • ***Pirminis/atvirkštinis tarpiniai serveriai*** *(angl. PROXY Forward and Reverse)* • ***Virtualus privatus tinklas*** *(angl. VPN)* • ***Antivirusai*** *(angl. Antivirus Software)* • ***Atvirojo kodo programa*** *(angl. Mimikatz)* • ***Smėliadėžė*** *(angl. Sandbox)* • ***Patikimas platformos modulis*** *(angl. Trusted platform module)* • ***Smart - ID*** • ***Galutinio taško sauga*** *(angl. Endpoint security)* • ***Žiniatinklio programos ugniasienė*** *(angl. Web Application Firewall)*	**SLA garantijos** *(angl. SLA Assurances)* **Kibernetinio saugumo sąmoningumas ir mokymai** *(angl. Training and Awareness)* **BYOD sprendimai** *(angl. Bring your own device)* **Nepageidaujamo masinio el. pašto prevencija** *(angl. Anti spam)*

Šaltinis: parengta autorės

2 pav. Kibernetinio saugumo priemonės ir metodai

Gyarmathy K. (2019) išskiria: **Svarbiausias kibernetinio saugumo problemas, su kuriomis susiduria bankai ir jų sprendimo būdus:**

Kibernetinės atakos tapo įprastiniu šiandieninio tarpusavyje susijusio pasaulio bruožu. Vis didesniam skaičiui organizacijų perkeliant savo duomenų operacijas į internetą, padidėjo ir kibernetinių atakų skaičius. Nuo 2016 m. iki 2017 m. bendras praneštų incidentų skaičius išaugo beveik dvigubai, tačiau šis skaičius neatspindi realaus nepraneštų atakų skaičiaus. Dar blogiau, daugelis šių atakų buvo nukreiptos į mažas įmones, kurios neturi apsiginimui tinkamų įrankių ar strategijų.

Gyarmathy K. (2019) pateikia svarbiausias kibernetinio saugumo problemas, su kuriomis susiduria bankai, ir keletas jų sprendimo būdų, kurie turėtų būti apsvarstyti:

PROBLEMATIKA

- **DDoS (paskirstyto atsisakymo aptarnauti) atakos**

Paskirstyto atsisakymo aptarnauti (DDoS) atakos per pastaruosius kelerius metus tapo viena ryškiausių kibernetinių nusikaltimų formų. Nors nekyla jokių abejonių, kad padidėjo jų dažnis, DDoS atakų metu, perėmus pagrindines interneto svetaines, suformuojamos sensacingos antraštės, net jeigu joms tai pavyksta padaryti tik keletai minučių. DDoS atakos tikslas – apkrauti serverį prieigos užklausomis, kol šis galiausiai suges. Prie šių atakų paprastai prisideda „botnetai“ – tūkstančiai kenkėjiška programine įranga užkrėstų kompiuterių, užprogramuotų įsilaužėlio vieninteliam tikslui siųsti prieigos užklausas. Naujesnės, intensyvesnės DDoS atakų formos apima procesą, vadinamą „atminties kaupimu“, kuris naudoja neapsaugotas, atvirojo kodo objektų talpyklos sistemas, kad sustiprintų prieigos užklausas ir didesniu nei terabaitas srautu užplūstų interneto svetaines. (Gyarmathy K., 2019)

- **Kenkėjiška programa**

Klasikinė kibernetinės atakos forma – kenkėjiška programinė įranga – gali būti įvedama į sistemą įvairiais būdais. El. pašto priedai, programinės įrangos atsisiuntimai ir operacinės sistemos pažeidžiamumas – tai dažniausiai pasitaikantys kenkėjiškų programų šaltiniai. Įdiegus kenkėjišką programinę įrangą, ji slapta prisišlieja prie teisėto kodo ir plinta į kitas sistemas. Kenkėjiškos programinės įrangos tikslas paprastai yra suteikti nesankcionuotą prieigą prie kompiuterio ar sistemos. Išpirkos reikalavimo programinė įranga, per užkodavimą draudžianti vartotojo prieigą prie svarbių duomenų, kol nebus sumokėta išpirka už atrakinimą, pastaraisiais metais buvo atsakinga už keletą didelį dėmesį atkreipusių kibernetinių atakų, tačiau nuolat atsiranda vis naujų kenkėjiškos programinės įrangos formų, įskaitant Trojos arklius, virusus ir kirminus, kurios kelia grėsmę organizacijoms ir asmenims. (Gyarmathy K., 2019)

- **Duomenų vagystė**

Skaitmeninė labai seno sukčiavimo versija – duomenų vagystės atakos – susideda iš el. pašto pranešimų, kuriuose naudojamos įvairios psichologinės manipuliacijos ir apgaulės formos, siekiant įtikinti vartotojus paspausti nuorodą, kuri juos nukreips į kanalą asmeninės informacijos pasidalijimui. Šiuolaikiniai duomenų vagystės pranešimai yra itin apgaulingi, dažnai atrodantys kaip el. laiškai iš teisėtų, patikimų kompanijų. Ir nors dauguma interneto vartotojų žino, kad turėtų itin apdairiai elgtis su tokiomis užklausomis, 2016 m. „Verizon“ ataskaitoje nustatyta, kad žmonės šešis kartus dažniau spustelėjo ant suklastoto el. laiško nei ant įprastinio rinkodaros el. laiško. (Gyarmathy K., 2019)

- **Vidinis piktnaudžiavimas**

Net geriausios kibernetinio saugumo priemonės gali tapti neveiksmingos, darbuotojams priėmus sprendimą piktnaudžiauti savo prieigos teisėmis. Nors svarbiausiu tokio piktnaudžiavimo pavyzdžiu gali būti saugių duomenų nutekinimas į viešus šaltinius, daug dažniau darbuotojai paprastai pasisavina gyvybiškai svarbius duomenis ir informaciją, neturėdami jokio konkretaus plano, ką daryti su tokia informacija. Naujausių tyrimų metu nustatyta, kad 85 proc. darbuotojų pasisavino dokumentus ar informaciją, kurią jie sukūrė patys, o 30 proc. darbuotojų pasisavino duomenis, kurių jie nebuvo sukūrę. Šią informaciją sudarė strateginiai dokumentai, klientų duomenys ir netgi patentuotas šaltinio kodas. Nors darbuotojai kartais perimdavo duomenis dėl to, kad būdavo atleisti iš darbo, 90 procentų jų teigė, kad pasisavino duomenis, nes tuo metu nebuvo jokios galiojančios politikos ar technologijos, kuri galėtų juos sustabdyti. (Gyarmathy K., 2019)

Gyarmathy K. (2019) išskiria: **Svarbiausias kibernetinio saugumo problemų sprendimo būdus:**

SPRENDIMO BŪDAI *(metodai ir priemonės)*

- **Nuspėjamoji analitika** *(metodas)*

Norėdami veiksmingai pasipriešinti kibernetinėms atakoms, IT darbuotojai turi žinoti, kaip atrodo ataka, kada ji gali įvykti ir iš kur kildinama. Nuspėjamosios analitikos programinė įranga, pagrįsta mašinų mokymu, gali surinkti didžiulį kiekį duomenų apie žinomas kibernetines atakas ir gautus rezultatus pritaikyti esamiems saugos protokolams. Tai ypatingai naudinga aktyviam DDoS mažinimui, nes leidžia kibernetinio saugumo sistemoms identifikuoti grėsmes ir imtis veiksmingų priemonių, nukreipiant srautą prieš sistemos perpildymą. Labai svarbus greitas atsakymo laikas, norint išvengti blogiausių kibernetinių atakų padarinių, pavyzdžiui, kuo ilgiau

pažeidimas bus nepastebėtas, tuo daugiau duomenų bus pažeista, o tai gali brangiai kainuoti bet kokio dydžio įmonėms/bankams. Nuspėjamoji analitika gali iš anksto pranešti nuotolinio valdymo komandoms, kad jos privalo aktyviai kovoti su neteisėtos prieigos bandymais. (Gyarmathy K., 2019)

- **Atsarginių duomenų kopijų kūrimas** *(metodas)*

DDoS ir išpirkos reikalavimo programinės įrangos atakų atveju bankams svarbu turėti parengtą atsarginių duomenų kopijų kūrimo planą. Prieiga prie tikslui svarbių duomenų gali reikšti skirtumą tarp greito sistemų ir paslaugų atnaujinimo internete, naudojant minimalias prastovas ir patiriant katastrofišką serverio gedimą. Turėdamos išsamią atsarginių kopijų kūrimo strategiją, kuri dažnai kaupia gyvybiškai svarbius duomenis ir turtą atskiroje ir, pageidautina, už objekto ribų esančioje sistemoje, įmonės gali išvengti „viskas arba nieko“ kibernetinės atakos rizikos, kuri sukelia užsitęsusią prastovą. Duomenų centrai gali teikti išplėstinius atsarginių kopijų kūrimo sprendimo būdus, kurie būtų sustiprinti keliais kibernetinio ir fizinio saugumo sluoksniais. (Gyarmathy K., 2019)

- **SLA garantijos** *(metodas)*

Daugeliui organizacijų dalį IT infrastruktūros ar duomenų operacijų teikia trečiųjų šalių įmonės. Nors tai gali sumažinti išlaidas ir logistinę naštą, tuo pačiu sukuriama ir potenciali duomenų neapsaugojimo rizika, jei trečioji šalis netaiko tokio paties lygio kibernetinio saugumo priemonių, kad apsisaugotų nuo grėsmių. Siekdamos išvengti šios problemos, įmonės turėtų naudoti Aptarnavimo lygio susitarimus (SLA), kad nustatytų visų su santykiais susijusių šalių saugumo įsipareigojimus. Nors SLA savaime negali užkirsti kelio kibernetinėms atakoms, tačiau jis suteikia teisinį užtikrinimą, kad trečiųjų šalių teikėjai privalo laikytis tam tikrų saugumo standartų arba dėl jų nesilaikymo patirti rimtų finansinių pasekmių. (Gyarmathy K., 2019)

- **Kibernetinio saugumo sprendimai mokymų ir sąmoningumo kontekste** *(metodas)*

Daugybė duomenų pažeidimų atsiranda dėl duomenų vagysčių, įdiegiančių kenkėjiškas programas į tinklo sistemas. Darbuotojų mokymas apie naujausią sukčių naudojamą taktiką gali padėti sumažinti tikimybę, kad jie paspaus nuorodas į kenksmingą programinę įrangą. Pagrindinių duomenų saugumo politikų, paaiškinančių, kaip tinkamai tvarkyti įmonės duomenis, įgyvendinimas taip pat yra labai svarbus aspektas siekiant sumažinti vidinio piktnaudžiavimo grėsmę. Organizacijos taip pat turėtų griežčiau nustatyti, kas pirmiausiai turi prieigą prie neskelbtinų asmens duomenų. Šios strategijos gali ženkliai sumažinti vartotojo klaidų poveikį kibernetinio saugumo priemonėms.

Nors kibernetinės atakos vis dar kelia rimtą grėsmę organizacijoms, yra keletas sprendimų, galinčių sustiprinti pastangas apsaugoti duomenis ir maksimaliai padidinti paslaugos darbingosios būsenos trukmę. Stebėdamos naujausias rizikas, įmonės gali įgyvendinti efektyvesnes kibernetinio saugumo strategijas, kad save ir savo klientus apsaugotų nuo žalingų duomenų pažeidimų ir kitų grėsmių. (Gyarmathy K., 2019)

- **BYOD sprendimai** *(metodas)*

„Atsineškite savo įrenginį, taip pat vadinamas atsineškite savo technologiją (BYOT), atsineškite savo telefoną (BYOP) ir savo asmeninį kompiuterį (BYOPC) - nurodo, kad jam leidžiama naudoti asmeninį įrenginį, o ne reikalauti naudoti oficialiai pateiktą įrenginį.“
(Andy Weeger, Michael Loose, Heiko Gewald**,** 2013)

- **Nepageidaujamo masinio el. pašto prevencija** *(angl. Anti spam) (metodas)*

„El. pašto šlamšto (nepageidaujamo masinio el. pašto) prevencijai naudojami įvairūs kovos su šlamštu būdai. Nei viena metodika nėra visiškas šlamšto problemos sprendimas, ir kiekviena iš jų turi kompromisus tarp neteisėto ir teisėto el. laiško atmetimo.“ (Richard Segal, Jason Crawford, Jeff Kephart, Barry Leiba, 2004)

- **Draudimas nuo kibernetinių rizikų** *(priemonė)*

Neteisėtai prieigai tapus pripažinta rizika daugelyje pramonės šakų, dauguma įmonių reagavo į tai įsigydamos draudimo planus, kad apsisaugotų nuo galimų finansinių nuostolių. Tikimasi, kad iki 2025 m. draudimo nuo kibernetinių rizikų rinka išaugs iki 20 milijardų JAV dolerių. Kažkada buvusi tik prie bendrų verslo planų pridedama galimybė, savarankiška kibernetinio draudimo apsauga tapo tokia populiari, kad į rinką ateina daug naujų iš to siekiančių susikrauti kapitalą draudikų. Tokioms pramonės šakoms kaip sveikatos priežiūra, kuriai dėl įstatymų laikymosi sunku įgyvendinti tvirtas saugumo priemones, draudimas greitai tampa būtinybe finansiškai apsaugoti įmones nuo kibernetinių atakų jų pačių ar jų tiekėjų ir partnerių sistemose. (Gyarmathy K., 2019)

- **Klaidų aptikimo programos** *(angl. „Bug Bounties“) (priemonė)*

Programinės įrangos kodo pažeidžiamumų nustatymas gali būti varginantis ir daug laiko reikalaujantis procesas. Daugelis organizacijų paprasčiausiai neturi išteklių, kad galėtų griežtai tikrinti savo programas, siekiant nustatyti kiekvieną programos klaidą ar spragą, kurią galėtų panaudoti įsilaužėliai, tačiau pastaraisiais metais įmonės nusprendė perduoti šią užduotį per

klaidų aptikimo (angl. „bug bounty“) programas. Šios programos skatina įsilaužėlius ieškoti internetinės programinės įrangos pažeidžiamumų ir klaidų, išmokant grynuosius pinigus, kai nustatomos patvirtintos klaidos. Tiek privačios įmonės, tiek vyriausybinės institucijos įgyvendino „klaidų aptikimo“ politiką, kad sustiprintų savo programinės įrangos saugumą. (Gyarmathy K., 2019)

- **Žiniatinklio programos ugniasienė** *(angl. Web Application Firewall) (priemonė)*

„Žiniatinklio programos ugniasienė (arba WAF) filtruoja, stebi ir blokuoja HTTP srautą į ir iš žiniatinklio programos. WAF skiriasi nuo įprastos ugniasienės tuo, kad WAF geba filtruoti konkrečių žiniatinklio programų turinį, o įprastos ugniasienės tarnauja kaip apsauginiai vartai tarp serverių. Tikrindamas HTTP srautą, jis gali užkirsti kelią išpuoliams, atsirandantiems dėl žiniatinklio programų saugumo trūkumų, tokių kaip SQL įterpimas, vietinių scenarijų (XSS), failų įtraukimas ir netinkamos saugos konfigūracijos.“*(https://owasp.org/www-community/Web_Application_Firewall)*

- **Komutatorius** *(angl. Network switch*) *(priemonė)*

„Tinklo komutatorius – aktyvusis kompiuterių tinklo elementas, valdantis duomenų srautus taip, kad jie pasiektų reikiamą adresatą su mažiausiais praradimais maksimaliu greičiu. Komutatoriaus pagalba išorinio tinklo segmento (WAN) interneto ryšys padalinamas į vidinius (LAN). Maršrutizuoti srautą komutatoriai gali tik pagal MAC adresą. Tai padidina tinklo saugumą ir našumą, nes kitiems tinklo segmentams nelieka būtinybės ir galimybės apdoroti ne jiems skirtus duomenis. Komutatoriai gali būti apjungti vienas su kitu per specialius prievadus. Komutatoriai būna įvairių konstrukcijų: nevaldomieji (paprastesni) arba valdomi protokolų (tinklo monitoringo RMON, paprasto stebėjimo SNMP ir pan.). Valdomieji komutatoriai gali vykdyti daug papildomų funkcijų (dubliavimas, virtualusis LAN, QoS, kelių kanalų sutelkimas).“ *(https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-vs-router.html)*

- **Serveris** *(angl. Radius - Remote AAA) (priemonė)*

„Įrenginys, kuris gauna ir atlieka prisijungimo užklausas ar apskaitos žinutes, siųstas RADIUS klientų arba RADIUS proxy. Atsižvelgdamas į prisijungimo prašymą, RADIUS serveris apdoroja RADIUS atributų sąrašą ryšio prašyme.“ (Andriuška G., 2011)

- **IDS apsaugos sistemos** *(angl. IDS Intrusion Detection System) (priemonė)*

„IDS (*Intrusion Detection System*) – įsilaužimo aptikimo sistema. IPS (*Intrusion Prevention System*) – apsaugos nuo įsilaužimo sistema.“ (Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz, 2005

- **Tinklo prieigos valdymo standartas *(angl. IEEE 802.1X)*** *(priemonė)*

„IEEE 802.1X yra IEEE standartas, skirtas tinklo prieigos valdymui (PNAC). Tai yra „IEEE 802.1“ tinklo protokolų grupės dalis. Tai suteikia autentifikavimo mechanizmą įrenginiams, norintiems prisijungti prie LAN ar WLAN.“ (Jyh-Cheng Chen, Yu-Ping Wang, 2005)

- **„Wi-Fi“ sauga** *(angl. Wi-fi network encryption WEB (WPA2, WPA3) (priemonė)*

„Belaidis saugumas - tai neteisėta prieiga prie kompiuterių ar duomenų arba jų sugadinimas naudojant belaidžius tinklus, apimančius „Wi-Fi“ tinklus. Dažniausiai pasitaikantis tipas yra „Wi-Fi“ sauga, į kurią įeina laidinio ekvivalento privatumas (WEP) ir apsaugota „Wi-Fi“ prieiga (WPA).“ **(**Frank H. Katz, 2009)

- **Pirminis/atvirkštinis tarpiniai serveriai** *(angl. PROXY Forward and Reverse) (priemonė)*

„pirminis tarpinis serveris yra tarpininkas, kurį klientas pateikia tarp savęs ir bet kurio serverio. Atvirkštinis tarpinis serveris yra kitame gale - tai, ką serveris pateikia tarp savęs ir bet kurio kliento. Atvirkštinis tarpinis serveris yra tarpininkas serverio, prie kurio jungiatės, pusėje.“ (R. Zehavi, U. Trugman, D. Drai, I. Safruti, 2012)

- **Virtualus privatus tinklas** *(angl. VPN) (priemonė)*

„Virtualus privatus tinklas yra ryšio metodas, naudojamas norint padidinti saugumą ir privatumą privačiuose ir viešuose tinkluose, tokiuose kaip „WiFi“ interneto prieigos taškai ir internetas. Virtualius privačius tinklus korporacijos dažniausiai naudoja siekdamos apsaugoti neskelbtinus duomenis.“ **(**Paul Ferguson, Geoff Huston, 1998**)**

- **Antivirusai** *(angl. Antivirus Software) (priemonė)*

„kompiuterinė programa, skirta aptikti ir nukenksminti kompiuterinius virusus. (R. Waldin, C. Nachenberg, 2000)

- **Atvirojo kodo programa** *(angl. Mimikatz) (priemonė)*

„Mimikatz“ yra kredencialų atvirojo kodo programa, naudojama abonemento prisijungimo ir slaptažodžio informacijai gauti, paprastai maišos ar aiškaus teksto slaptažodžio, iš operacinės sistemos ar programinės įrangos. Tada kredencialai gali būti naudojami šoniniam judėjimui atlikti ir prieigai prie ribotos informacijos gauti.“ (Vincent E. Urias, William M.S. Stout, Jean Luc-Watson, Cole Grim, Lorie Liebrock, Monzy Merza, 2017)

- **Smart – ID** *(priemonė)*

„Tai naujasis patogus asmens tapatybės nustatymo sprendimas. Jį yra paprasta bei lengva naudoti ir tai yra puiki alternatyva bankų kodų kortelėms. Naudodamiesi „Smart-ID“, galite jungtis prie elektroninių paslaugų ir patvirtinti operacijas bei susitarimus.“ *(https://www.smart-id.com/lt/pagalba/duk/bendroji-informacija/kas-yra-smart-id/)*

- **Smėliadėžė** *(angl. Sandbox) (priemonė)*

„Smėliavimas yra populiari technika, skirta uždarų vykdymo aplinkų, kurios gali būti naudojamos nepatikimų programų paleidimui, kūrimui.“ **(**Maximilian Schreieck, Robert Finke, Manuel Wiesche, Helmut Krcmar, 2017)

- **Patikimas platformos modulis** *(angl. Trusted platform module) (priemonė)*

„Patikimas platformos modulis (TPM, taip pat žinomas kaip ISO / IEC 11889) yra tarptautinis saugiojo kriptoprocesoriaus, skirto mikrovaldikliui, skirtas apsaugoti aparatūrą per integruotus kriptografinius raktus, tarptautinis standartas.“ (Sundeep Bajikar, 2002)

- **Galutinio taško sauga** *(angl. Endpoint security) (priemonė)*

„Galutinio taško sauga reiškia galinių taškų arba galutinių vartotojų įrenginių, tokių kaip staliniai kompiuteriai, nešiojamieji kompiuteriai ir mobilieji įrenginiai, apsaugą. Galiniai taškai tarnauja kaip prieigos prie įmonės tinklo taškai ir sukuria įėjimo taškus, kuriuos gali išnaudoti kenksmingi veikėjai.“ (Mark S. Kadrich, 2007)

Apibendrinant galima konstatuoti, kad buvo išskirtos pagrindinės kibernetinio saugumo bankų rizikų valdymui priemonės: draudimas nuo kibernetinių rizikų, klaidų aptikimo programos, technologinės priemonės. Taip pat išanalizuoti pagrindiniai metodai: nuspėjamoji analitika, atsarginių duomenų kopijų kūrimas, SLA garantijos, kibernetinio saugumo sąmoningumas ir mokymai, BYOD sprendimai, nepageidaujamo masinio el. pašto prevencija.

2. KIBERNETINIO SAUGUMO PRIEMONIŲ IR METODŲ TAIKYMO BANKŲ VEIKLOS RIZIKŲ VALDYMUI PASAULIO PATIRTIES ANALIZĖ

2.1. „Bank of America“ atvejo analizė (JAV)

Amerikos bankas (ang. „Bank of America“) – „prieš 240 metų iš daugelio šaltinių susibūrėme tam, kad būtume tokie, kokie esame šiandien: Bendrovė, vienijanti mūsų tikslą, kad naudodamasi kiekviena jungtimi galėtume pagerinti finansinį gyvenimą. „Bank of America“ atstovauja bankines paslaugas žmonėms ir įmonėms. Tai apima vartotojus ir smulkųjį verslą, privatų banką orientuotą į bendroves (pasaulinė komercinė bankininkystė, pasaulinės transakcijų paslaugos, verslo bankininkystė, didmeninis kreditas ir įmonių bankininkystės dalys).“

„Bank of America“ įvardija pagrindines saugumą didinančias priemones: 20 CC. „Projektas buvo inicijuotas 2008 m. pradžioje reaguojant į didžiulius duomenų praradimus, kuriuos patiria organizacijos JAV gynybos pramonės bazėje. Iš pradžių leidinį sukūrė SANS institutas. Tuomet nuosavybės teisė buvo perduota Kibernetinio saugumo tarybai (CCS) 2013 m., o po to - 2015 m. perduota interneto saugumo centrui (CIS). Iš pradžių ji buvo vadinama Konsensuso audito gairėmis ir dar vadinama CIS CSC, CIS. 20, CCS CSC, SANS Top 20 arba CAG 20.“ Žiūrėti į 2 lentelę:

2 lentelė. Ypač svarbios efektyviai kibernetinei gynybai saugumo kontrolės priemonės

Nr.	SAUGUMĄ DIDINANTI PRIEMONĖ	APRAŠYMAS
1.	„Tinklo įrenginių, kuriems leidžiama naudotis institucijos tinklo paslaugomis, identifikavimas (angl. Inventory of Authorized and Unauthorized Devices)“	Veiksmingai valdyti (inventorizuoti, stebėti ir šalinti) visus tinklo įrenginius, siekiant užtikrinti, kad tik tie įrenginiai, kuriems leidžiama tai daryti, galėtų pasinaudoti tinklo teikiamomis paslaugomis, o nežinomi ir nevaldomi įrenginiai būtų aptikti, jiems nebūtų leista dalyvauti tinklo veikloje.
2.	„Leistinos ir neleistinos naudoti programinės įrangos identifikavimas (angl. Inventory of Authorized and Unauthorized Software)“	Veiksmingai valdyti (inventorizuoti, stebėti ir šalinti) programinės įrangos naudojimą tinkle, siekiant užtikrinti, kad būtų įdiegta ir galėtų veikti tik leistina programinė įranga, o aptikta draudžiama naudoti programinė įranga būtų blokuojama.
3.	„Techninės ir programinės įrangos saugios konfigūracijos mobiliuosiuose įrenginiuose, darbo vietos ar tarnybinėse stotyse numatymas (angl. Secure Configurations for	Sukurti, pritaikyti ir veiksmingai valdyti (stebėti, tikslinti bei rengti ataskaitas) nešiojamųjų įrenginių, darbo vietos ar tarnybinių stočių techninės ir programinės įrangos saugumo konfigūraciją (saugumo nustatymo parametrus), siekiant užkirsti kelią pasinaudoti sistemų pažeidžiamumu.

	Hardware and Software on Mobile Devices, Laptops, Workstations and Servers)“	Konfigūracijų pokyčiai turi būti griežtai stebimi ir valdomi.
4.	„Nenutrūkstamas sistemų pažeidžiamumo vertinimas ir saugumo spragų taisymas (angl. Continuous Vulnerability Assessment and Remediation)“	Nuolat rinkti ir vertinti informaciją, susijusią su programinės įrangos pažeidžiamumu ir saugumo spragų ištaisymu. Neatidėliojant veikti pagal pateikiamas rekomendacijas, norint sumažinti galimybes piktavaliams pasinaudoti saugumo spragomis.
5.	„Naudojimosi administratoriaus teisėmis kontrolė (angl. Controlled Use of Administrative Privileges)“	Kurti procesus ir naudotis priemonėmis, skirtomis stebėti ir kontroliuoti, kaip naudojamasi administratoriaus teisėmis. Tokių teisių konfigūravimas ir suteikimas kompiuteriuose, tinkle ar programinėje įrangoje turi būti griežtai kontroliuojamas ir leidžiamas tik esant būtinybei.
6.	„Audito žurnalų įrašų stebėjimas, analizė ir saugojimas (angl. Maintenance, Monitoring and Analysis of Audit Logs)“	Audito įrašų, galinčių padėti aptikti ir suprasti vykstančias kibernetines atakas, atkurti sistemos veiklą įvykus saugumo incidentui, fiksavimas, valdymas ir analizė.
7.	„Elektroninio pašto ir naršyklių apsauga (angl. Email and Web Browser Protections)“	Mažinti galimybes piktavaliams manipuliuoti el. pašto ir interneto sistemų naudotojų elgsena.
8.	„Apsauga nuo kenkimo programų (angl. Malware Defenses)“	Kenkimo programų atsiradimo organizacijoje stebėjimas, jų plitimo ir veikimo organizacijos tinkle kontrolė. Apsaugos sistemų automatizavimas ir optimizavimas, norint sparčiai atnaujinti apsaugos priemones, efektyviai surinkti informaciją apie įvykius ir veiksmingai reaguoti į incidentus.
9.	„Tinklo prievadų, protokolų ir paslaugų naudojimo apribojimai (angl. Limitation and Control of Network Ports, Protocols and Services)“	Veiksmingai valdyti (stebėti, kontroliuoti ir riboti) tinklo prievadų, protokolų ir paslaugų tinklo įrenginiuose naudojimą, norint sumažinti galimybes piktavaliams rengti kibernetines atakas.
10.	„Duomenų atkūrimo pajėgumas (angl. Data Recovery Capability)“	Taikyti procesus ir priemones, skirtas itin svarbių duomenų atsarginėms kopijoms daryti. Metodika turi būti išbandyta ir užtikrinti patikimą duomenų atkūrimą reikiamu laiku.
11.	„Saugios tinklo įrenginių, tokių kaip saugasienės, maršruto parinktuvai, komutatoriai, konfigūracijos numatymas (angl. Secure Configurations for Network Devices such as Firewalls, Routers and Switches)“	Nustatyti, taikyti ir veiksmingai valdyti (stebėti, tikslinti bei rengti ataskaitas) tinklo įrenginių saugumo konfigūraciją, laikantis griežtai apibrėžtos konfigūracijos valdymo ir pokyčių kontrolės proceso tvarkos, siekiant užkirsti kelią piktavaliams pasinaudoti paslaugų ir įrenginių nustatymo parametrų pažeidžiamumu.

12.	„Tinklo perimetro apsauga (angl. Boundary Defense)“	Aptikti, stabdyti bei valyti potencialiai pavojingą duomenų srautą, keliaujantį tarp skirtingo patikimumo lygio tinklo segmentų.
13.	„Duomenų apsauga (angl. Data Protection)“	Taikyti procesus ir priemones, skirtas apsisaugoti nuo tikslinio duomenų rinkimo ir informacijos nutekinimo (eksfiltravimo), užtikrinti neskelbtinos informacijos vientisumą ir konfidencialumą.
14.	„Prieigos kontrolė, paremta principu „būtina žinoti“ (angl. Controlled Access Based on the Need to Know)“	Taikyti procesus ir priemones, skirtas stebėti ir kontroliuoti, kad prieiga prie itin svarbių išteklių (informacijos, sistemų ir pan.) būtų suteikiama tik esant motyvuotam poreikiui. Suteikiant prieigą, remtis iš anksto numatyta politika, kuriems kompiuteriams, programoms ar darbuotojams tai yra reikalinga.
15.	„Belaidės prieigos kontrolė (angl. Wireless Access Control)“	Taikyti procesus ir priemones, skirtas belaidžių tinklų, prieigos taškų ir belaidžių sistemų saugumui užtikrinti bei kontroliuoti, kad belaide prieiga naudotųsi tik teises tai daryti turintys naudotojai (neviršydami jiems suteiktų teisių).
16.	„Naudotojų paskyrų stebėjimas ir kontrolė (angl. Account Monitoring and Control)“	Aktyviai kontroliuoti sistemų ir taikomųjų programų naudotojų paskyras visą jų gyvavimo (kūrimo, naudojimo, laikino stabdymo, naikinimo) ciklą, siekiant sumažinti piktavalių galimybes išnaudoti sistemos saugumo spragas.
17.	„Saugumo srities gebėjimų vertinimas ir reikiamų mokymų numatymas (angl. Security Skills Assessment and Appropriate Training to Fill Gaps)“	Identifikuoti specifinių įgūdžių ir žinių, būtinų norint užtikrinti organizacijos informacinių sistemų apsaugą, poreikį (prioritetai teikiami ypač svarbiems veiklos procesams ir jų saugumui užtikrinti). Įvertinus poreikį didinti kibernetinį sąmoningumą, taikant veiklos planavimo priemones ir remiantis saugumo politika, sukurti ir pritaikyti darbuotojų gebėjimų tobulinimo planą.
18.	„Taikomųjų programų saugumas (angl. Application Software Security)“	Valdyti visos sukurtos ar įgytos programinės įrangos saugumo gyvavimo ciklo elementus. Siekti užkirsti kelią piktavalių planams pasinaudoti galimomis saugumo spragomis; stengtis jas aptikti ir ištaisyti.
19.	„Reagavimas į incidentus ir jų valdymas (angl. Incident Response and Management)“	Organizacijos informacijos ir reputacijos apsaugos užtikrinimas, diegiant reagavimo į incidentus infrastruktūrą (veiklos planai, vaidmenų paskirstymas, mokymai, komunikacija, valdymas) tam, kad būtų greitai aptinkamos

		vykstančios atakos, efektyviai suvaldoma žala, aptinkami įsilaužėliai ir panaikinami jų veiklos padariniai, atkuriamas tinklo ir sistemų vientisumas.
20.	„Bandymai įsilaužti ir „raudonųjų komandų“ pratybas (angl. Penetration Tests and Red Team Exercises“	Visapusiškai išbandyti organizacijos gynybos galimybes (technologijas, procesus, personalą), imituojant piktavalio veiksmus ir tikslus.

Šaltinis: sudaryta pagal Nacionalinio kibernetinio saugumo centro www.kam.lt duomenis, 2019

Abibendrinant galima teigti, kad „Bank of America“ remiasi 20 CC ir juos įvardija kaip pagrindiniais kibernetinio saugumo metodais ir priemonėmis tai ypač svarbios efektyviai kibernetinei gynybai saugumo kontrolės priemonės.

2.2. „Bank of China“ atvejo analizė (Kinija)

„Kinijos bankas yra vienas iš keturių didžiausių valstybinių komercinių bankų Kinijoje. Tai antras seniausias iki šiol gyvuojantis žemyninės Kinijos bankas. Jo būstinė yra Xicheng rajone, Pekine. 2009 m. gruodžio 31 d. jis buvo antras pagal dydį skolintojas Kinijoje ir penktas pagal dydį bankas pasaulyje pagal rinkos kapitalizacijos vertę. 2017 m. pabaigoje jis buvo ketvirtas pagal dydį bankas pasaulyje pagal turtą, užimdamas reitingą po kitų trijų Kinijos bankų.“

„Bank of China“ įvardija, vieną svarbiausių kibernetinio saugumo metodų ir priemonių bankų veiklos rizikų valdyme: dviejų faktorių autentifikavimą. Oficialiame banko internetiniame puslapyje (www.bochk.com) rašoma, kad „Siekdama padidinti internetinio saugumo lygį, klientams teikia platų dviejų veiksnių autentifikavimo priemonių asortimentą, skirtą apsaugoti nurodytas operacijas ir nurodytas investavimo operacijas, kurias klientai vykdo naudodamiesi internetine / mobiliąja bankininkyste.“

- **Dviejų veiksnių autentifikavimo priemonių tipai:**

Taip pat „Bank of China“ pristato kas yra „Mobilusis prieigos raktas“, tai įmontuota „BOCHK Mobile Banking“ funkcija. Suaktyvinus „Mobilusis prieigos raktą“ neteks rūpesčių nešiojant atskirą fizinį „saugos įrenginį“, kad iš tikrųjų galėtumėte mėgautis patogia ir saugia banko veikla. Suaktyvinę „Mobilųjį prieigos raktą“ suderinamame mobiliajame įrenginyje, galite patvirtinti nurodytas mobiliosios bankininkystės operacijas arba nurodytas investavimo operacijas naudodami iš anksto nustatytą kodą arba naudodami „Biometrinę autentifikaciją“. Be to, naudodami „„Mobilusis

prieigos raktą“, galite patvirtinti nurodytas internetinės bankininkystės operacijas arba Software Security)“.

Išskiriamos šios funkcijos:

3 lentelė. Dviejų faktorių autentifikavimo funkcijos

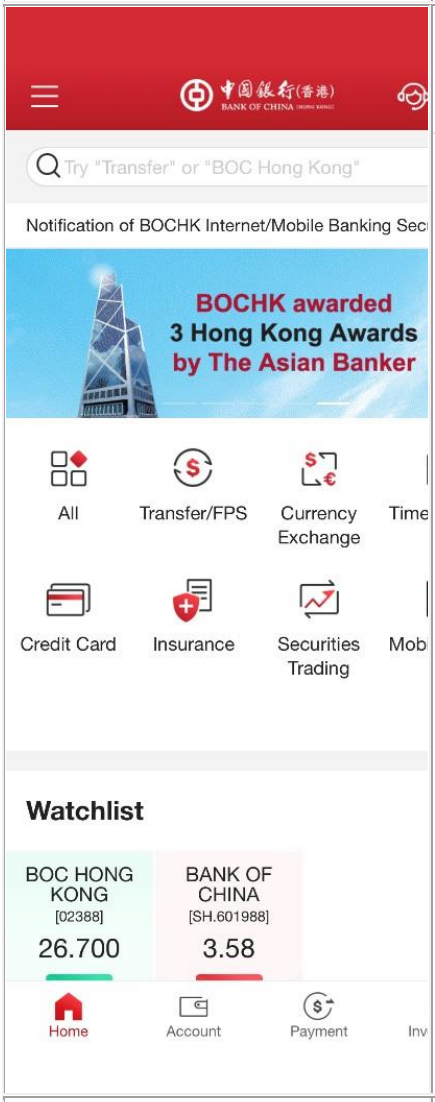
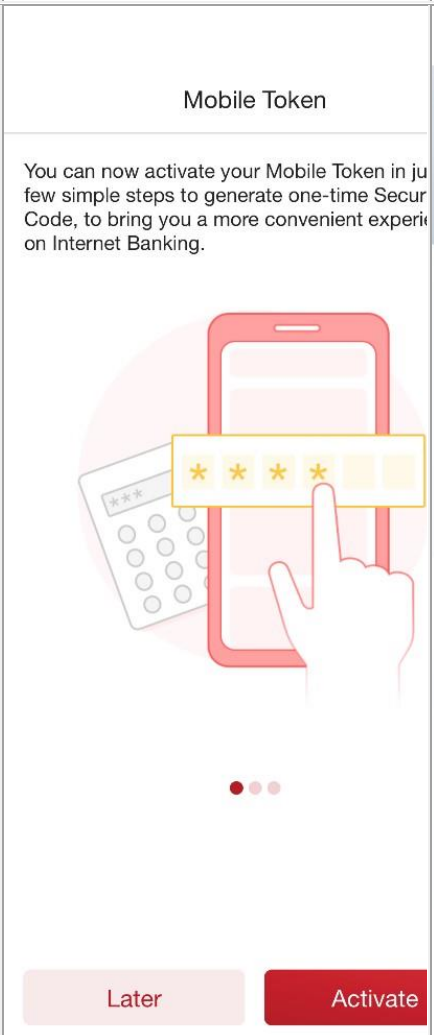
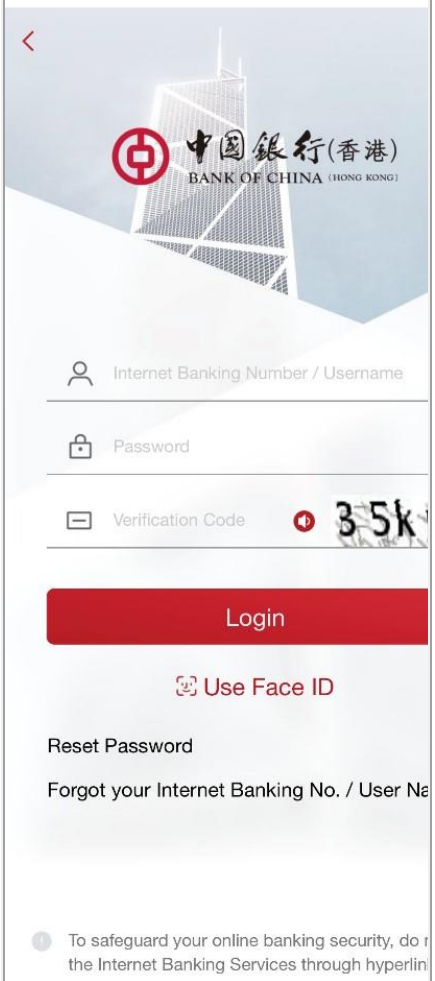
Patogiau	**Paprasčiau**	**Saugiau**
Nereikia be vargo nešiotis atskiro fizinio „saugos įrenginio“	Patvirtinkite įvairius sandorius, tokius kaip trečiųjų šalių lėšų pervedimas, investicinės operacijos ir kita	Naudokite „Biometrinį autentifikavimą“ (pirštų atspaudas / veido ID) arba iš anksto nustatytas leidimo kodas, kad būtų galima įjungti mobilųjį prieigos raktą

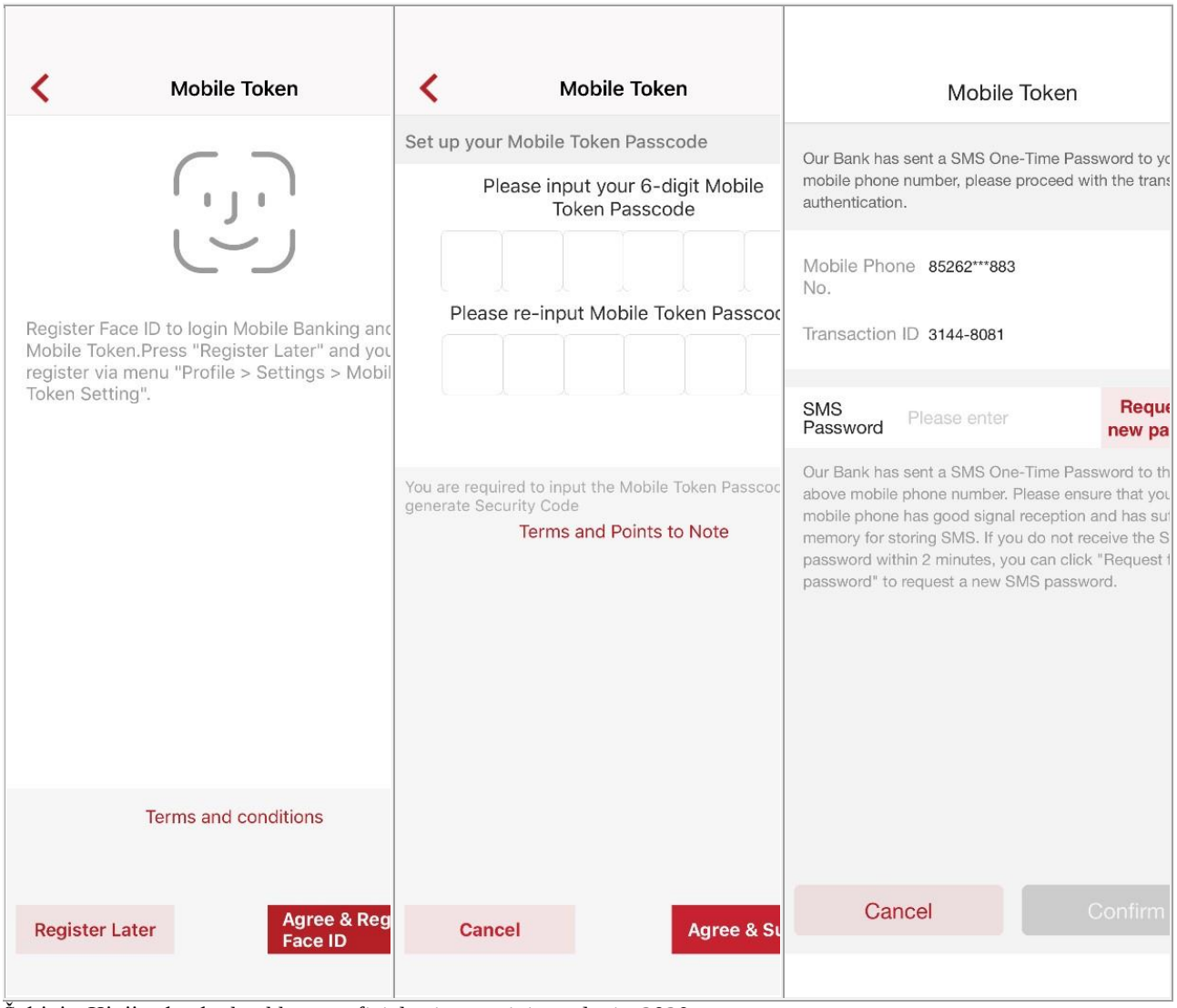
Šaltinis: Kinijos banko www.bochk.com oficialus internetinis puslapis, 2020

„Bank of China“ išskiria šį biometrinį autentifikavimą, bei jo naudojimą:

- „„Biometrinį autentifikavimą“ (pvz.: pirštų atspaudus, veido ID) mobiliajame įrenginyje galite užregistruoti šioms paslaugoms, kai suaktyvinote „Mobilųjį prieigos raktą“:
- Prisijungdami mobiliojoje bankininkystėje įgalinkite „Mobilųjį prieigos raktą, kad patvirtintumėte nurodytas mobiliosios bankininkystės operacijas arba nurodytas investicines operacijas.
- Įgalinkite „Mobilųjį prieigos raktą“ ir sugeneruokite vienkartinį „Apsaugos kodą“ / „Operacijų patvirtinimo kodą“, kad patvirtintumėte nurodytas internetinės bankininkystės operacijas ar nurodytas investicines operacijas.“

„Mobiliojo prieigos rakto“ suaktyvinimas

1. Pagrindiniame puslapyje pasirinkite „Mobile Token“ piktogramą	2. Pasirinkite „Suaktyvinti“	3. Prisijunkite prie mobiliosios bankininkystės
		
4. Užregistruokite „Biometrinį autentifikavimą“ (galimybė registruotis vėliau)	5. Nustatykite „Mobile Token“ kodą	6. Iš banke užregistruoto mobiliojo telefono numerio gausite „SMS vienkartinį slaptažodį“ (OTP), įveskite OTP, kad užbaigtumėte aktyvaciją



Šaltinis: Kinijos banko bochk.com oficialus internetinis puslapis, 2020

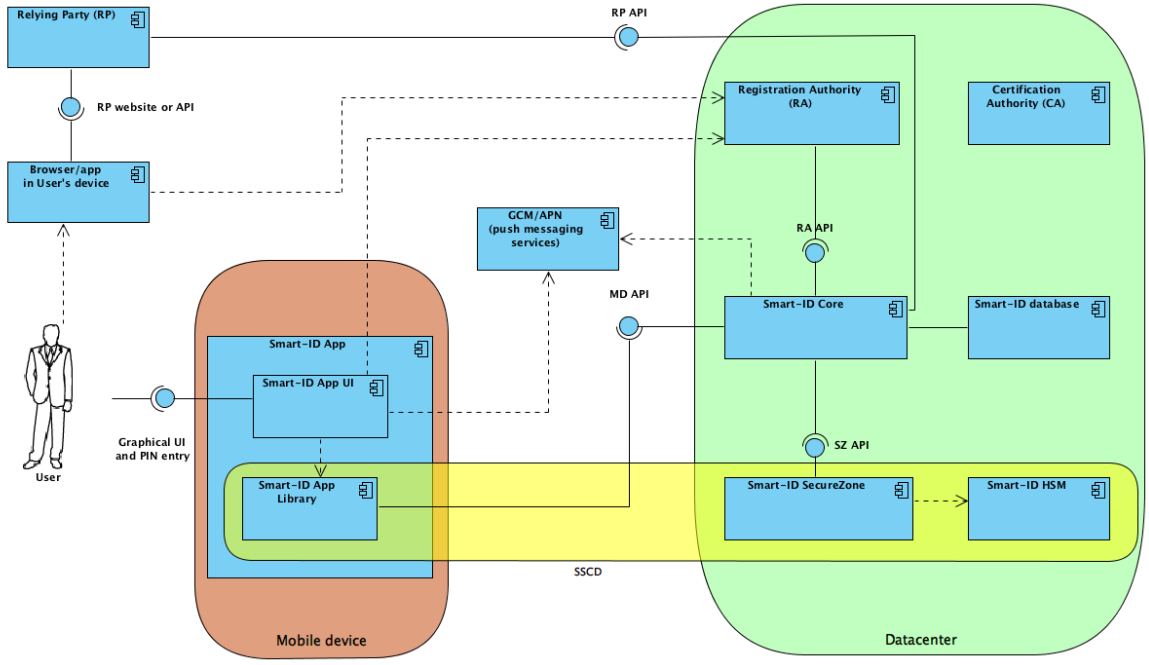
3 pav. Dviejų faktorių autentifikavimas

Apibendrinant galima teigti, kad „Bank of China“ (Kinijos) atvejo analizės metodu buvo analizuojamas - dviejų faktorių autentifikavimas. Siekdama padidinti internetinio saugumo lygį, „Bank of China“ klientams teikia platų dviejų veiksnių autentifikavimo priemonių asortimentą, skirtą apsaugoti nurodytas operacijas ir nurodytas investavimo operacijas, kurias klientai vykdo naudodamiesi internetine / mobiliąja bankininkyste. Naudodajant prieigos raktą, galima patvirtinti nurodytas internetinės bankininkystės operacijas arba nurodytas investavimo operacijas, sukurdami vienkartinį „apsaugos kodą“ arba „operacijos patvirtinimo kodą“.

2.3. Baltijos šalys

2.3.1. „Smart-ID“ atvejo analizė (Estija)

Saudardas P. (2016) nagrinėja kibernetinio saugumo istoriją, analizuodamas, kad „pirmųjų kibernetinių atakų Baltijos šalyse pradžia siejama su Bronzinio kario skulptūros perkėlimo istorija 2007 m., kada buvo paralyžiuotas Estijos valdžios institucijų, politinių partijų, bankų, žiniasklaidos priemonių interneto svetainių veikimas, taip pat Bendrojo pagalbos centro darbas.“ (Saudargas P., 2016) Taip pat jis teigia, Lietuva taip pat yra patyrusi atakų „2008 m. Seimui kriminalizavus sovietinių simbolių naudojimą, buvo įsilaužta į daugiau nei 300 interneto tinklalapių. Daugiausia tai buvo privačių kompanijų serveriai. Tuo tarpu valstybės institucijų informacinės sistemos atlaikė dėl geresnių apsaugos priemonių.“ (Saudargas P., 2016) To pasekoje buvo tobulinamos ir kuriamos įvairios kibernetinio saugumo priemonės. Viena iš jų - „Smart-ID“, tai „naujasis patogus asmens tapatybės nustatymo sprendimas. Ji yra paprasta bei lengva naudoti ir tai yra puiki alternatyva bankų kodų kortelėms. Naudodamiesi „Smart-ID“, galime jungtis prie elektroninių paslaugų ir patvirtinti operacijas bei susitarimus.“ (žr. 4 pav.)



Šaltinis: „Smart-ID“ techninė apžvalga, 2019 (www.github.com)

4 pav. „Smart-ID“ veikimo schema

„Smart-ID“ techninėje apžvalgoje (2019) yra išskiriamos šios sudėtinės dalys (žr. 4 pav.):

1. „Smart-ID App Lib“ – Šis komponentas „Smart-ID“ programėlėje tvarko visas su kriptografija, paskyros valdymu ir serverio ryšiais susijusias užduotis.
2. „Smart-ID App UI“ – Šis komponentas tvarko UI ir naudotojo sąveikas.
3. „Smart-ID App“ - „Android/IOS“ programėlė, kurią Naudotojas įdiegia savo mobiliajame įrenginyje, kad užregistruotų „Smart-ID“ paskyrą ir patvirtintų savo tapatybę RP (išteklių teikėjo) tarnyboms bei suteiktų skaitmeninius parašus.
4. GCM/APN – Aktyviųjų pranešimų platforma, tokia kaip „Google Cloud Messaging“ ir „Apple Push Notification“, perduoda pranešimus iš „Smart-ID Core“ į „Smart-ID App“ kopijas.
5. „Smart-ID Core“ – Šis komponentas įgyvendina verslo logiką, tvarko duomenų bazę ir teikia API mobiliesiems įrenginiams, RP (išteklių teikėjui) ir RA (registracijos institucijai). Jis taip pat tarpininkauja perduodant pranešimus tarp „Smart-ID App Lib“ ir „Smart-ID SecureZone“ komponentų.
6. „Smart-ID SecureZone“ – Tai yra komponentas, kuris tvarko kriptografijos užduotis ir raktinių porų generavimą serverio pusėje. „SecureZone“ taip pat prašo kriptografinių operacijų iš „Smart-ID HSM“.
7. RA – Registracijos įstaiga. Tai komponentas, įgyvendinantis registracijos procesus ir atliekantis registracijos įstaigos pareigas. Yra kelios RA, kad atitiktų skirtingus registracijos proceso variantus, pvz., registracija darbų vietoje su darbuotojais, kurie patvirtina savo tapatybę, ir savitarnos registracijos portaluose, kurie naudojasi trečiųjų šalių autentifikavimo paslaugomis.
8. CA – išduoda X.509 sertifikatus autentifikavimui ir parašo raktines poras. Yra kelios CA, atitinkančios skirtingus „Smart-ID“ paskyrų lygius, pvz., „Smart-ID Basic“ paskyrų sertifikatai yra išduodami iš skirtingų CA.
9. QSCD – kvalifikuotas parašo kūrimo įrenginys. Tai yra loginis komponentas, kurį sudaro „Smart-ID App Lib“, „Smart-ID SecureZone“ ir „Smart-ID HSM“ komponentai ir kuris teikia tokias pačias paslaugas, kaip ir išmaniosiomis kortelėmis paremti QSCD įrenginiai. Į jį atsižvelgiama atliekant saugumo analizę ir bendrųjų kriterijų įvertinimą.

„Smart-ID“ saugumo priemonė susideda iš šių komponentų:

1. Naudotojo autentiškumo nustatymas
2. Skaitmeninis naudotojo parašas
3. Vartotojo registracija
4. „Smart-ID“ paskyros valdymas

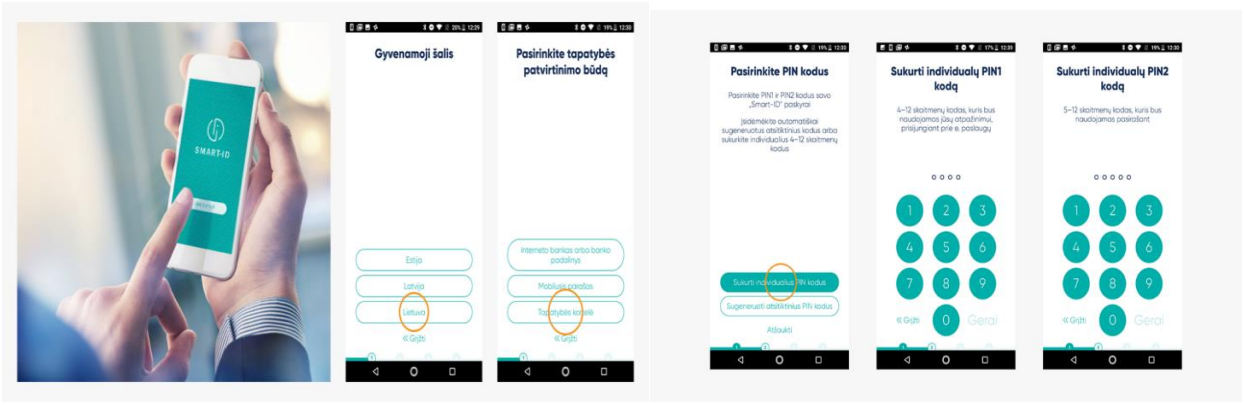
Plačiau apie trečiąją (Vartotojo registracija) dalį bus nagrinėjama toliau, kur naudojantis banko „Swedbank“ pateikta atmintine, kaip naudotis „Smart – ID“ (žr. 4 lentelė) bus aptariami visi žingsniai.

4 lentelė. Kaip pradėti naudotis „Smart-ID

Kaip pradėti naudotis „Smart-ID
„Reikia išmaniojo telefono su „Android 4.1“ (ar vėlesnės versijos) arba „iOS 8.0“ (ar vėlesnės versijos) operacine sistema ir dabartinės prisijungimo prie interneto banko priemonės.“
„Į telefoną atsisiųsti nemokamą „Smart-ID“ programėlę.“
„Telefone susikurti „Smart-ID“ paskyrą.“
„Aktyvinsti ją su dabartine prisijungimo priemone.“
„Jeigu turite tik kodų kortelę, aktyvuoti „Smart-ID“ paskyrą artimiausiame padalinyje.“

Šaltinis: sudaryta autorės pagal www.swedbank.lt ir pateiktą informaciją, 2020

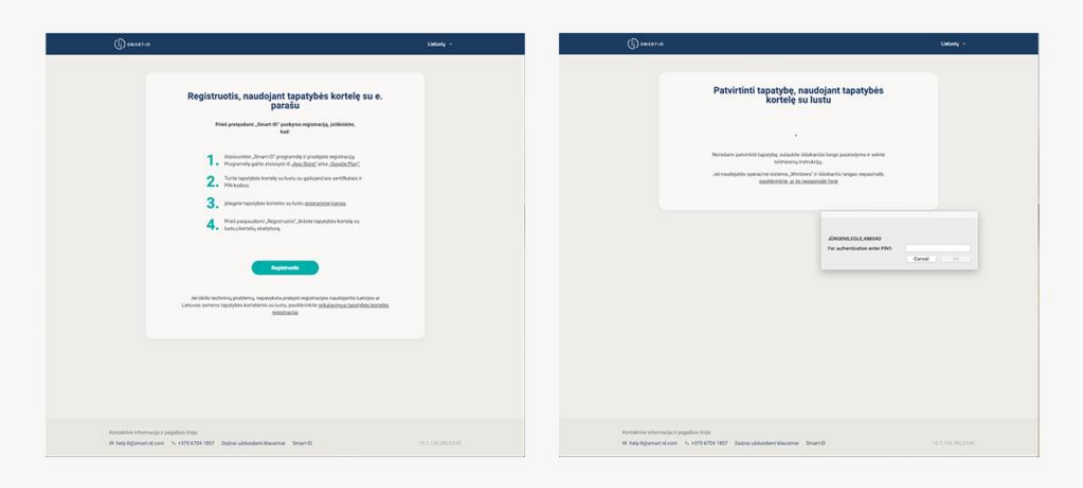
Vartotojams nurodoma, kad „išmaniajame įrenginyje atidarykite „Smart-ID“ programą (spustelėkite ją) ir pasirinkite „Registruotis“. Reikės pasirinkti gyvenamąją vietą savo šalyje ir tapatybės patvirtinimo būdą (pasirinkite „Tapatybės kortelė“).“ *(www.smart-id.com)* Tuomet rašoma, kad „Pasirinkite PIN kodus, kuriuos norite naudoti „Smart-ID“ programai. Atminkite, kad „Smart-ID“ PIN kodai negali būti atkurti ar nustatyti iš naujo, todėl svarbu pasirinkti tokius PIN kodus, kuriuos lengvai įsimintumėte, tačiau jų negalėtų atspėti kiti.“ *(www.smart-id.com)*



Šaltinis: nuotrauka iš https://www.smart-id.com

5 pav. 1-2 veiksmai: atidarykite „Smart-ID“ programą savo išmaniajame įrenginyje ir pasirinkite PIN kodus

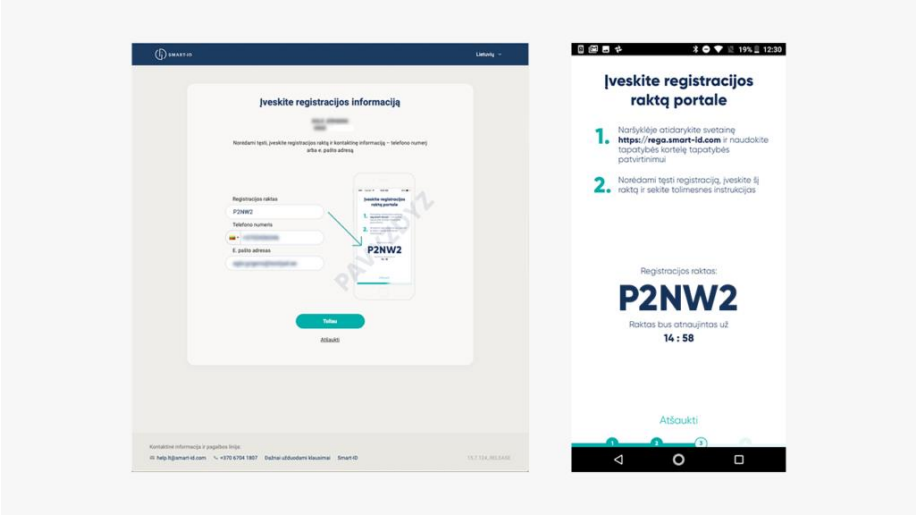
Atlikę šiuos veiksmus, turime „Pasirinkus PIN kodus, išmaniajame įrenginyje esanti „Smart-ID“ programa paprašys tęsti registraciją naudojant tapatybės kortelę ir atidaryti interneto naršyklę kompiuteryje. Atidarykite interneto svetainę https://rega.smart-id.com kompiuterio naršyklėje ir prisijunkite naudodami tapatybės kortelę.“ *(www.smart-id.com)*



Šaltinis: nuotrauka iš https://www.smart-id.com

6 pav. 3 veiksmas: tęskite registraciją kompiuteryje

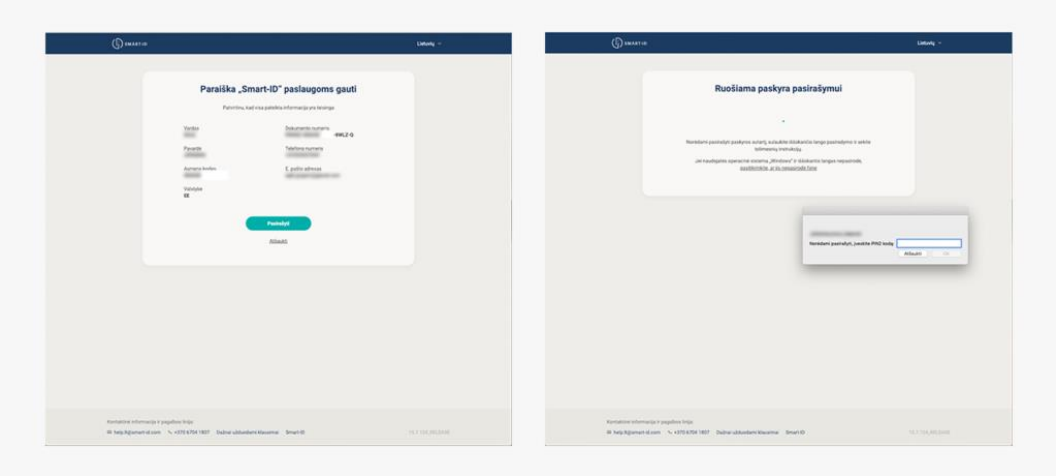
Tuomet „„„Smart-ID“ portale – svetainėje, prie kurios ką tik prisijungėte – bus užduota keletą paprastų klausimų. Atsakius į juos, reikės įvesti „Smart-ID“ registracijos kodą. Šis kodas bus pateiktas „Smart-ID“ programoje telefone arba planšetiniame kompiuteryje.“ *(www.smart-id.com)*



Šaltinis: nuotrauka iš https://www.smart-id.com

7 pav. 4 veiksmas: užpildykite duomenis kompiuteryje

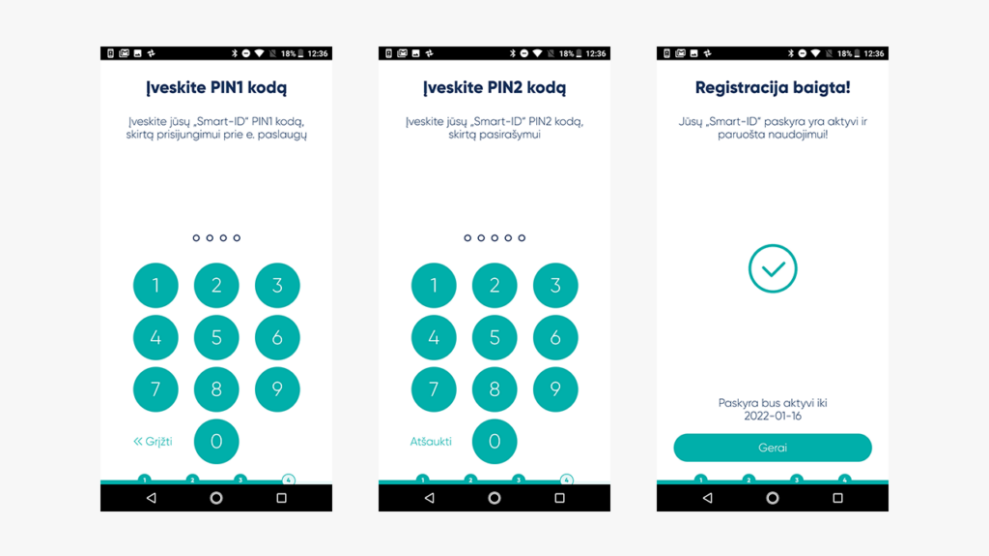
„Jei registracijos kodas, naudojamas „Smart-ID“ programoje, atitinka kompiuteryje įvestą kodą, automatiškai būsite nukreipti atlikti kitą veiksmą, kad patvirtintumėte registraciją. Vadovaukitės ekrane pateiktais nurodymais, kad užbaigtumėte registraciją.“ *(www.smart-id.com)*



Šaltinis: nuotrauka iš https://www.smart-id.com

8 pav. 5 veiksmas: patvirtinkite savo „Smart-ID“ paskyrą kompiuteryje

Tada „patvirtinę registraciją kompiuteryje, pamatysite pranešimą, kuriame nurodoma tęsti registraciją išmaniajame įrenginyje. Toliau nebereikės naudoti kompiuterio registracijos procesui atlikti. Paskutinis „Smart-ID“ registracijos etapas yra patvirtinti, kad atsimenate „Smart-ID“ PIN 1 ir PIN 2 kodus. Atlikę visus šiuos prieš tai išvardintus veiksmus jau galime naudotis e.paslaugomis, pvz.: elektronine bankininkyste.“ (žr. 6 pav.) *(www.smart-id.com)*



Šaltinis: nuotrauka iš https://www.smart-id.com

9 pav. 6 veiksmas: užbaikite registraciją savo išmaniajame įrenginyje

Apibendrinant galima konstatuoti, kad Smart-ID buvo sukurta Estijoje iš devynių sudėtinių pagrindinių dalių, norint ja naudotis reikia atlikti tik šešis veiksmus. Lietuvos bankų asociacija teigia, kad „Lietuvos statistikos departamento 2018 m. duomenimis, net 79,7 proc. 16–74 metų amžiaus šalies gyventojų naudojasi internetu, o 60,6 proc. jų – apie 1,27 mln. – internetinės bankininkystės paslaugomis. Vadinasi, jau beveik 80 proc. Lietuvos gyventojų prie savo interneto banko paskyrų jungiasi naudodami programėlę „Smart-ID““. **„Smart-ID“ trūkumai:** pastaruoju metu susilaukia vis daugiau kritiškos nuomonės, kad ši priemonė yra nesaugi, kad į ją lengva įsilaužti (atvejis, kai 2019 m. liepą, Estijoje buvo įvykdyta tapatybės vagystė pasinaudojant Smart-ID ir socialine inžinerija, (Kamaravcevas V., 2019)). Po pastarųjų įvykių „Smart-ID“ papildomai informuoja vartotojus laiškais apie naujai sukurtas paskyras, kad taip būtų galima išvengti kenkėjiško klonavimo. Ar „Smart-ID“ galėtų būti kibernetinio saugumo pavyzdys ne tik Baltijos šalyje, bet ir pasaulyje išsiaiškinta atlikus kokybinę ekspertinę apklausą (žr. 3 skyrių).

2.3.2. Kibernetinio saugumo dokumentų analizė (Lietuva)

„Stiprinant kibernetinį saugumą, buvo priimtas Kibernetinio saugumo įstatymas, kuriuo nustatytas kibernetinio saugumo organizavimas, valdymas ir kontrolė, taip pat įkurtas Nacionalinis kibernetinio saugumo centras, užtikrinantis kritinės informacinės infrastruktūros ir valstybės informacinių išteklių apsaugą. Krašto apsaugos ministerijai pavaldus centras atlieka daugybę uždavinių. Taip pat buvo sustiprinti CERT-LT pajėgumai.“ (Saudargas P., 2016)

Nacionalinis kibernetinio saugumo centras www.nksc.lt rekomenduoja sudaryti svarbiausių veiksmų sąrašą, kuris naudojamas bankų veiklos rizikų valdymui.

1. „Sudaryti leistinos naudoti programinės įrangos sąrašus (angl. *application whitelisting – CC 2*).“
2. „Naudoti standartizuotos, saugios konfigūracijos sistemas (angl. *use of standard, secure system configuration – CC 3*).“
3. „Skubiai (ne vėliau kaip per 48 val. nuo naujinių išleidimo) diegti naudojamos programinės įrangos naujinius (angl. *patch application software within 48 hours – CC 4*).“
4. „Skubiai (ne vėliau kaip per 48 val. nuo naujinių išleidimo) diegti naudojamos operacinės sistemos naujinius (angl. *patch system software within 48 hours – CC 4*).“
5. „Griežtai riboti naudotojų, turinčių administratoriaus teises, skaičių (angl. *reduce the number of users with administrative privileges – CC 3 ir CC 5*).“ *(www.nksc.lt)*

Teisinių dokumentų analizės praktinis reikšmingumas bankų veiklos rizikų valdymui: Ambrasas T., (2019) teigia, kad „Dėl naujų kibernetinių grėsmių nuolat keičiama ir pildoma teisinio reguliavimo praktika, o kasmet finansinių paslaugų sektoriuje sukuriamas duomenų kiekis sparčiai didėja.“ Taip pat jis pabrėžia, kad „Kibernetinis saugumas liečia ne tik finansų institucijas plačiąja prasme, bet ir pačius reguliuotojus.<...> Naujos kibernetinės grėsmės verčia keisti ir vystyti teisinio reguliavimo praktiką.“ (Ambrasas T., 2019) Todėl buvo išanalizuoti šie teisiniai dokumentai: LR Valstybės saugumo departamento ataskaitos (2011 - 2018 m.), LR Nacionalinio saugumo pagrindų įstatymas ir atlikta LR Nacionalinio saugumo strategijos analizė.

LR Valstybės saugumo departamento ataskaitų analizė

Analizuojant 2011 – 2018 metų Lietuvos Respublikos Valstybės saugumo departamento ataskaitas galima teigti, kad ne visose ataskaitose buvo minimas kibernetinis saugumas (paminėta 2011, 2012 ir 2016 metais).

Nagrinėjant www.vsd.lt 2011 metų ataskaitą, kibernetinio saugumo sąvoka buvo paminėta, įžanginiame direktoriaus žodyje. VSD generalinio direktoriaus, Gedimino Grinos, įžangos žodis: „Pažeidžiamas dėl asmeninių savybių ar kompromituojančios informacijos asmuo yra lengvai pasiekiamas taikinys valstybių žvalgybos ir saugumo tarnyboms. Dalyvavimas įvairiomis formomis kibernetinėje erdvėje asmens privatumą itin sumažina.“ (LR Valstybės saugumo departamento metinė ataskaita, 2011) Nėra paminima kokių prevencinių priemonių buvo imtasi, ar iš vis buvo imtasi. Tiesiog kaip ir kiekvienam aišku, pasakoma tai, kad asmens saugumas yra svarbus ir virtualiame pasaulyje bendrauti nėra saugu.

2012 metų ataskaitoje Lietuvos Respublikos gyventojai supažindinami plačiau su kibernetiniu saugumu, taigi kibernetinis saugumas jau užima didesnę vietą. Išskiriama kibernetinio saugumo sąvoka/apibrėžimas, įvardijama kas gali būti kibernetinio šnipinėjimo objektai, prieš ką gali būti vykdomos kibernetinės atakos, ko siekiama jas vykdant. Įdomu tai, kad atskleidžiama, kad Valstybės saugumo departamentas „kartu su Antruoju operatyvinių tarnybų departamentu identifikavo Lietuvos valstybės institucijų, verslo kompanijų ir privačių asmenų kompiuteriuose išplitusį užsienio valstybėje sukurtą kompiuterinį virusą, skirtą šnipinėti“, deja neįvardijamas pavadinimas, bei kokioje valstybėje virusas buvo sukurtas: „Kibernetinis saugumas: Kibernetinės atakos, kai siekiama pagrobti įslaptintą informaciją ar asmens duomenis, sutrikdyti informacinių sistemų veiklą, yra sparčiai auganti grėsmė Lietuvos nacionaliniam saugumui. Svarbiausi kibernetinio šnipinėjimo objektai gali būti su NATO ir Europos Sąjunga susijusi informacija, Lietuvos valstybinio ir privataus sektoriaus duomenys. Kibernetinės atakos gali būti vykdomos prieš Lietuvos informacines sistemas, elektroninėje erdvėje teikiamas viešas paslaugas ir kitas interneto funkcijas, siekiant sutrikdyti jų veiklą.“ (LR Valstybės saugumo departamento metinė ataskaita, 2012) Taip pat rašoma, kad „VSD identifikavo Lietuvos valstybės institucijų, verslo kompanijų ir privačių asmenų kompiuteriuose išplitusį užsienio valstybėje sukurtą kompiuterinį virusą, skirtą šnipinėti. Jis plinta per vartotojų naudojamas išorines duomenų laikmenas ir elektroniniu paštu. Virusas iš užkrėsto kompiuterio siunčia ten esančius duomenis ir naudojamus slaptažodžius šnipinėjimo programos valdytojui ir leidžia jam nuotoliniu būdu stebėti ir valdyti užkrėstą kompiuterį.“ (LR Valstybės saugumo departamento metinė ataskaita, 2012)

2014 metų ataskaitoje jau galime išvysti užsienio valstybių pavadinimus kalbant apie propagandą. Buvo paminėta 2014 metais vykusi Rusijos agresija prieš Ukrainą. „2014 m. po Rusijos pradėtos agresijos prieš Ukrainą Maskva suaktyvino savo propagandinę veiklą, todėl priešiška Rusijos informacinė politika išliko viena svarbiausių grėsmių Lietuvos nacionaliniam saugumui.“ (LR Valstybės saugumo departamento metinė ataskaita, 2014) Tačiau konkrečiai apie kibernetinį saugumą, ataskaitoje nebuvo kalbama lyginant prieš tai buvusius metus, kur dėmesys buvo gana didelis.

2016 metų ataskaitoje kibernetinis karas minimas tik įžanginiame direktoriaus, Dariaus Jauniškio žodyje: „Užtikrinant nacionalinį saugumą – būtiniausią ir pamatinę visavertiško Valstybės ir Tautos gyvavimo sąlygą – Lietuvos žvalgybai tenka ir visada teko svarbus, o kartais ir pagrindinis, vaidmuo. Ypač dabar, kai gyvename laikais, kuomet tampa neįmanoma preciziškai nustatyti karo lauko ribų ar veikėjų ketinimų, kai ginklu – tiek puolimo, tiek gynybos – tampa paprasčiausias kompiuteris, kai kaunamasi ne tik dėl teritorijos, bet ir dėl žmonių sąmonės.“ (LR Valstybės saugumo departamento metinė ataskaita, 2016)

2018 metų ataskaitoje kibernetinis „veiklos ataskaitoje pateikiama tik ta informacija, kurios atskleidimas nepakenks vykdomiems tyrimams ar Lietuvos Respublikos nacionalinio saugumo interesams.“ (LR Valstybės saugumo departamento metinė ataskaita, 2018) Todėl visiškai nėra kalbama apie kibernetinį ar informacinį saugumą.

Išanalizavus visas Lietuvos Respublikos Valstybės saugumo departamento ataskaitas, **apibendrinant galima teigti**, kad kibernetiniam saugumui galėtų būti skiriamas didesnis dėmesys, taip būtų informuojama visuomenė, vyktų socialinė inžinerija. Dažniausiai buvo paminėta, kad toks karas tiesiog vyksta ir kibernetinėje erdvėje nėra saugu, tačiau šios temos neplėtojant. Taip pat ne visose ataskaitose buvo minimas kibernetinis saugumas (paminėta 2011, 2012 ir 2016 metais). „Nors bankai pakankamai gerai valdo ir nuolat tobulina savo gebėjimus tvarkytis su kibernetinėmis grėsmėmis (brandi rinka, daugiau gali investuoti į prevenciją ir t.t.), ir jas nuolat mažina, tarptautiniai reguliuotojai šioje srityje tampa vis aktyvesni ir reikalavimų sąrašas ne tik bankams bet ir kitiems finansinių paslaugų industrijos žaidėjams didėja.“ (Ambrasas T., 2019) Taip pat labai svarbu informuot ir šviesti visuomenę kibernetinio saugumo klausimais bankų veiklos rizikų valdymui, „Akivaizdu, kad kibernetinis saugumas yra svarbi reguliavimo darbotvarkės dalis, ir priežiūros institucijos ateityje bus vis mažiau tolerantiškos toms įmonėms, kurios atsilieka nuo atitikties reikalavimų įgyvendinimo ir yra netinkamai pasiruošusios kibernetinių rizikų valdymui. Kibernetinės atakos paprastai išnaudoja trūkumus procesuose ir žmonėse, todėl reikia tinkamai naudotis tiek regioniniais, tiek tarptautiniais reguliavimo standartais, gerąja praktika ir apmokyti personalą.“ (Ambrasas T., 2019)

LR Nacionalinio saugumo pagrindų įstatymo analizė

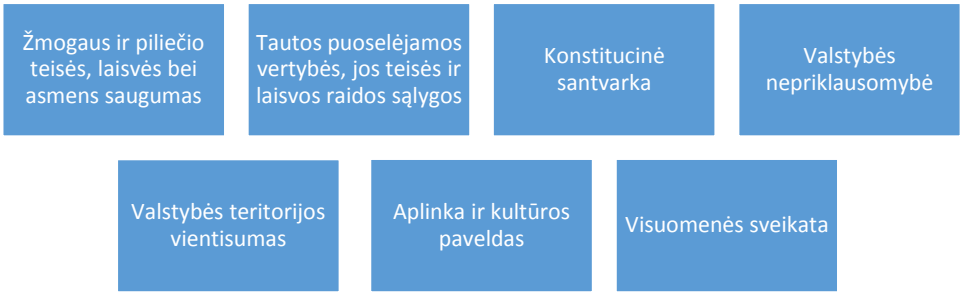
1996 m. gruodžio 19 d. Lietuvoje paskelbtas Nacionalinio saugumo pagrindų įstatymas (Įsigalioja nuo 1997 m. sausio 8 d.).

Šio įstatymo pagrindinė paskirtis yra užtikrinti Lietuvos nacionalinį saugumą „Lietuvos nacionalinio saugumo užtikrinimas – tai Tautos ir valstybės laisvos ir demokratinės raidos sąlygų sudarymas, Lietuvos valstybės nepriklausomybės, jos teritorinio vientisumo ir konstitucinės santvarkos apsauga ir gynimas. (Lietuvos Respublikos Nacionalinio saugumo pagrindų įstatymas, 1997).

Nacionalinio saugumo užtikrinimo objektai: „Lietuvos nacionalinį saugumą užtikrina LR piliečiai, jų bendrijos ir organizacijos, Respublikos Prezidentas, Seimas, Vyriausybė, kariuomenė, policija, Valstybės saugumo departamentas, kitos šiam tikslui valstybės įsteigtos institucijos,

vadovaudamiesi Konstitucija ir įstatymais bei vykdydami savo pareigas ir funkcijas nacionalinio saugumo sistemoje.“ (Lietuvos Respublikos Nacionalinio saugumo pagrindų įstatymas, 1997).

Pagrindiniai nacionalinio saugumo objektai:



Šaltinis: Sudaryta autorės remiantis LR Nacionalinio saugumo pagrindų įstatymu, 1996

10 pav. Pagrindiniai nacionalinio saugumo objektai

Įstatyme įvardijamas nacionalinio saugumo tikslas: „Sutelktomis valstybės ir piliečių pastangomis plėtoti ir stiprinti demokratiją, užtikrinti Tautos saugų būvį ir valstybės vidaus bei išorės saugumą, atgrasyti kiekvieną potencialų užpuoliką, ginti Lietuvos valstybės nepriklausomybę, teritorijos vientisumą ir konstitucinę santvarką.“ (Lietuvos Respublikos Nacionalinio saugumo pagrindų įstatymas, 1997).

5 lentelė. Nacionalinio saugumo užtikrinimo būdai

VALSTYBĖ	PILIEČIAI
– „prognozuodama (numatydama) iššūkius saugumui, rizikos veiksnius, pavojus bei galinčias kilti grėsmes“ – „vykdydama rizikos veiksnius, pavojus ir grėsmes mažinančią vidaus ir užsienio politiką“ – „patikimai kontroliuodama valstybės sausumos ir jūros sienas bei oro erdvę“ – „garantuodama pasirengimą besąlygiškai gynybai ir visuotiniam pilietiniam pasipriešinimui agresijos atveju“ – „stiprindama nacionalinio saugumo bei gynybos institucijas ir tobulindama jų veiklą“	- „saugodami tautines vertybes ir ugdydami pasiryžimą ginti Lietuvos laisvę“ - „rengdamiesi visuotiniam pilietiniam pasipriešinimui“ - „plėtodami visuomenės institutus, piliečių susivienijimų ir draugijų veiklą“

– „rengdama gynybai kariuomenę ir jos mobilizacinį rezervą pagal nacionalinius ir NATO kolektyvinės gynybos planus“ – „rengdama ir vykdydama ilgalaikes valstybines saugumo stiprinimo programas“ – „integruodamasi į Europos Sąjungą (EU) ir Šiaurės Atlanto sutarties organizaciją (NATO) bei kaip visateisė narė aktyviai dalyvaudama šiose organizacijose“	

Šaltinis: Sudaryta autorės remiantis LR Nacionalinio saugumo pagrindų įstatymu, 1996; https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/vDAPGooxLN

Lietuvos Respublikos Nacionalinio saugumo pagrindų įstatyme teigiama, kad „Nacionalinio saugumo institucijos veikia ir plėtojamos, saugumo stiprinimo priemonės rengiamos ir vykdomos vadovaujantis demokratinės kontrolės principais. Valstybės institucijų vykdomas nacionalinio saugumo priemones nustato šis įstatymas, Nacionalinio saugumo strategija, ilgalaikės valstybinės saugumo stiprinimo programos bei kiti teisės aktai.“ (Lietuvos Respublikos Nacionalinio saugumo pagrindų įstatymas, 1997). (LR Nacionalinio saugumo pagrindų įstatymas, 1996)

Svarbiausios nacionalinio saugumo užtikrinimo priemonės:

Šaltinis: Sudaryta autorės remiantis LR Nacionalinio saugumo pagrindų įstatymu, 1996 *https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/vDAPGooxLN*

11 pav. Svarbiausios nacionalinio saugumo užtikrinimo priemonės

LR Nacionalinio saugumo įstatyme „Nacionalinį saugumą užtikrinančios institucijos išskiriamos į vadovaujančias ir vykdomąsias: **Vadovaujančios institucijos:** Valstybės aukščiausiosios vadovaujančios institucijos, kurios vadovauja nacionalinio saugumo užtikrinimui, yra Seimas, Respublikos Prezidentas ir Vyriausybė. **Vykdomosios ir kitos institucijos:** Valstybės

gynimo taryba; Užsienio reikalų ministerija; Krašto apsaugos ministerija ir kitos krašto apsaugos ministrui pavaldžios krašto apsaugos sistemos institucijos; kariuomenė; Vidaus reikalų ministerija, policija, Valstybinė sienos apsaugos tarnyba ir kitos ministerijos valdymo sričiai priklausančios viešąjį saugumą užtikrinančios įstaigos; Valstybės saugumo departamentas; Specialiųjų tyrimų tarnyba; kitos ministerijos ir valstybės bei savivaldybių institucijos pagal savo kompetenciją.“ (LR Nacionalinio saugumo pagrindų įstatymas, 1996)

Apibendrinant galima daryti išvadas, kad šie elementai yra svarbūs bankų veiklos rizikų valdymui: „Tautos ir valstybės laisvos ir demokratinės raidos sąlygų sudarymas, Lietuvos valstybės nepriklausomybės, jos teritorinio vientisumo ir konstitucinės santvarkos apsauga ir gynimas.“ (LR Nacionalinio saugumo pagrindų įstatymas, 1996) Kitas svarbus saugumo elementas „<..>užtikrinti Tautos saugų būvį ir valstybės vidaus bei išorės saugumą, atgrasyti kiekvieną potencialų užpuoliką, ginti Lietuvos valstybės nepriklausomybę, teritorijos vientisumą ir konstitucinę santvarką.“ (LR Nacionalinio saugumo pagrindų įstatymas, 1996) Šiuo įstatymu remiantis galima teigti, kad „vien tik izoliuotų nacionalinių įstatymų ir institucijų nepakanka, ypač finansinių paslaugų sektoriuje. Reikia turėti pajėgumus organizacijos viduje ar išorės ekspertus.“ (Ambrasas T., 2019)

LR Nacionalinio saugumo strategijos analizė

Lietuvos Respublikos Nacionalinio saugumo strategijoje rašoma, kad Lietuva įsipareigoja dalyvauti „stiprinant NATO pasirengimą atsakyti į hibridines grėsmes, taip pat prisidėti prie NATO pajėgumų saugumo iššūkiams energetinio, kibernetinio, informacinio saugumo srityse atremti plėtojimo.“ Lietuvos Respublikos Seimo tinklalapyje, 2017 m. sausio 17 d. pranešime žiniasklaidai, rašoma, kad Lietuvos Respublikos „Strategijoje apibrėžiamos pagrindinės nacionalinio saugumo politikos prielaidos; Lietuvos Respublikos nacionalinio saugumo interesai; grėsmės, pavojai, rizikos veiksniai; įvardijami nacionalinio saugumo politikos prioritetai ir uždaviniai.“ (Lietuvos Respublikos Nacionalinio saugumo strategija, 2002)

Nacionalinio Saugumo politikos prioritetuose ir uždaviniuose kibernetinio saugumo srities plėtojamas yra įtrauktas kaip vienas iš pagrindinių: „dalyvaus stiprinant NATO pajėgumų saugumo iššūkiams energetinio, kibernetinio, informacinio saugumo srityse atremti plėtojimo; skatins NATO ir ES įgyvendinti kovos su hibridinio karo iššūkiais priemones, siekiant apsaugoti NATO ir ES valstybių narių politines sistemas nuo Rusijos Federacijos pastangų daryti įtaką politinėmis, finansinėmis, informacinėmis, kibernetinėmis ir kitomis priemonėmis“. (Lietuvos Respublikos Nacionalinio saugumo strategija, 2002)

Šaltinis: sudaryta autorės remiantis Lietuvos Respublikos Nacionalinio saugumo strategija

12 pav. Kibernetinio saugumo stiprinimo veiksmai

Apibendrinant galima konstatuoti, kad Lietuvos Respublikos Nacionalinio saugumo strategijoje smulkiai aprašomi Lietuvos Respublikos kibernetinio saugumo stiprinimo veiksmai, kurie yra svarbus elementas bankų veiklos rizikų valdymui. Vienas svarbiausių – „stiprinti nacionalinius gebėjimus nustatyti kibernetinio saugumo incidentus, bei likviduoti jų padarinius.“ Taip pat „Stiprinti visuomenės švietimą kibernetinio saugumo klausimais.“ Tai vienas svarbiausių kibernetinio saugumo metodų bankų veiklos rizikų valdymui (žr. 3 skyrių).

2.4. Pasaulio šalių kibernetinio saugumo priemonių ir metodų taikymo bankų veiklos rizikų valdymui lyginamoji analizė

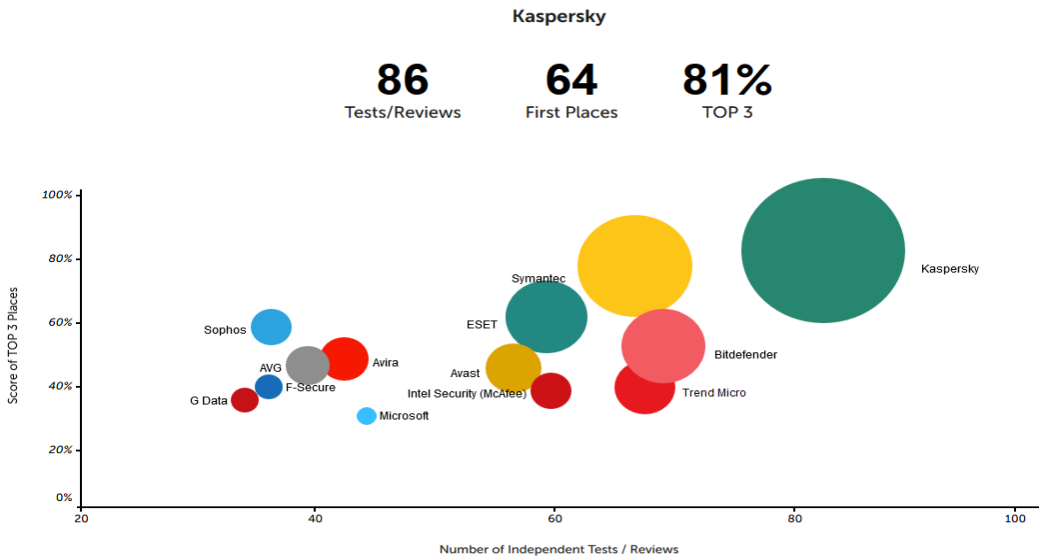
Antivirusinės programos

„Kaspersky Internet Security“

„„Kaspersky Internet Security“ tikrina, ar nėra pasikėsinimų į vagystę. Ji apsaugo nuo duomenų vagystės atakų, saugodama nuo grėsmingų interneto svetainių. Be to, nepriklausomos laboratorijos šiai antivirusinei programai skiria aukščiausius kenkėjiškų programų aptikimo balus.

„Kaspersky Internet Security“ privalumai:

- Efektyvus kenkėjiškų programų aptikimas ir antivirusinė apsauga
- Daugiau nei 400 milijonų apsaugotų vartotojų visame pasaulyje
- Apsauga realiuoju laiku
- Reklaminių skelbimų blokavimas“ (B. Athira, Neethu Babu ir M. Soumya Krishnan, 2017)



Šaltinis: nuotrauka iš https://www.kaspersky.com/top3

13 pav. Nepriklausomų testų / apžvalgų skaičius

Pagal 13 pav. matome, kad antivirusinė programa „Kaspersky“ atlieka daugiausiai nepriklausomų testų bei apžvalgų. Šią programą sukūrė „J.V. Kasperskis, Rusijos kibernetinio saugumo ekspertas ir „Kaspersky Lab“, IT apsaugos bendrovės, turinčios 4000 darbuotojų, generalinis direktorius. Jis kartu su „Kaspersky Lab“ įkūrė 1997 m. Ir padėjo nustatyti vyriausybės remiamo kibernetinio karo atvejus kaip tyrimų vadovas. Jis yra tarptautinės sutarties, draudžiančios kibernetinį karą, šalininkas. Jo susidomėjimas IT saugumu prasidėjo, kai jo darbo kompiuteris buvo

užkrėstas Cascade virusu 1989 m. Ir jis sukūrė programą jam pašalinti. „Kaspersky“ padėjo augti „Kaspersky Lab“ plėtojant saugumo tyrimus ir pardavimus. (Ronald Russell, Alex Medvedev, 2017)

„Avast Antivirus“

„Su nemokama antivirusine programa „Avast Mobile Security“ galima apsaugoti savo mobiliuosius telefonus nuo iššokančiuose languose ir nepageidaujamuose skelbimuose esančių virusų ir kenkėjiškų programų. Ši antivirusinė programa siunčia įspėjimus į įrenginius, kai diegiate privatumą pažeidžiančias šnipinėjimo ir reklamines programėles, kurios siunčia jūsų asmeninius duomenis į savo serverius. Ji apsaugo nuo duomenų vagystės atakų iš el. pašto, telefono skambučių, užkrėstų interneto svetainių ar SMS pranešimų.“ (B. Athira, Neethu Babu ir M. Soumya Krishnan, 2017)

Avast antivirus puslapyje www.avast.com pateikiama, kad „1988 m. kaip kooperatyvą „Avast“ įkūrė Pavelas Baudišas ir Eduardas Kučera. Ji buvo privati įmonė nuo 2010 m., O savo IPO turėjo 2018 m. gegužę. 2016 m. liepą „Avast“ už 1,3 milijardo dolerių įsigijo konkurentą „AVG Technologies“. Tuo metu AVG buvo trečias antivirusinis produktas. Jis yra dvejopai kotiruojamas Prahos ir Londono vertybinių popierių biržoje ir yra FTSE 250 indekso sudedamoji dalis. Pagrindinis bendrovės produktas yra „Avast Antivirus“ kartu su tokiais įrankiais kaip „Avast“ saugi naršyklė ir „Avast SecureLine“ VPN.“

„AVG Antivirus“

„2017 („Virus Cleaner“), skirta „Android“ operacinei sistemai, padeda apsaugoti įrenginius nuo pavojingų virusų, kenkėjiškų ir šnipinėjimo programų, apgaulingų programų ir tekstinių pranešimų bei padeda saugiai laikyti jūsų asmeninius duomenis su programų užrakto ir nuotraukų saugyklos funkcija.“ (B. Athira, Neethu Babu ir M. Soumya Krishnan, 2017)

Antivirusinės programos puslapyje www.avg.com pateikiama ši informacija, kad „„„AVG Technologies“ 1990 m. įkūrė Tomáš Hofer ir Jan Gritzbach pavadinimu „Grisoft“ Brno mieste, Čekoslovakijoje. Iš pradžių „Grisoft“, be savo antivirusinių produktų, pardavinėjo ir IT įrangą bei trečiųjų šalių programinę įrangą. „Grisoft“ augo, kai šalis atlaisvino savo tarptautinės prekybos politiką, todėl galėjo keistis technologijomis su Europos įmonėmis.“

„Bitdefender Antivirus“

„Pagrindinė šios antivirusinės programos ypatybė – pašalinti bet kokią kenksmingą kompiuteryje esančią programinę įrangą ir neleisti kompiuteriui ateityje parsisiųsti išpirkos reikalaujančių programų, virusų, Trojos arklių ar kitų kenkėjiškų programų. „Bitdefender Antivirus

Plus 2017“ peržengia šias pagrindines funkcijas. Pagrindinės šios antivirusinės programos funkcijos: paprasta slaptažodžių tvarkytuvė, saugi finansinių operacijų naršyklė, saugus failų naikiklis ir naujoji aktyvi apsauga nuo išpirkos reikalaujančių virusų.“ (B. Athira, Neethu Babu ir M. Soumya Krishnan, 2017)

Bitdefender vartotojo instrukcijoje rašoma, kad „„Bitdefender“ yra Rumunijos kibernetinio saugumo ir antivirusinės programinės įrangos įmonė. Jį 2001 m. įkūrė Florinas Talpešas, kuris šiuo metu yra generalinis direktorius. „Bitdefender“ kuria ir parduoda antivirusinę programinę įrangą, interneto saugumo programinę įrangą, galinių taškų apsaugos programinę įrangą ir kitus kibernetinio saugumo produktus ir paslaugas. Nuo 2018 m. programinę įrangą naudoja apie 500 milijonų vartotojų visame pasaulyje.“

„Avira Antivirus“

„Avira Antivirus“ „su 2017 m. aukštą reitingą turinčia nemokama mobiliųjų įrenginių sauga ir antivirusine apsauga apsaugokite savo telefono turinį nuo šnipinėjimo programų, Trojano arklių ir kitokio tipo kenksmingų ar taikomųjų programų.“ (B. Athira, Neethu Babu ir M. Soumya Krishnan, 2017)

„„Avira Operations GmbH & Co. KG“ yra vokiečių tarptautinė kompiuterių apsaugos programinės įrangos įmonė, daugiausia žinoma dėl savo antivirusinės programinės įrangos „Avira Internet Security“. „Avira“ buvo įkurta 2006 m., tačiau nuo 1986 m. aktyviai plėtojama antivirusinė programa per jos pirmtakę bendrovę „H + BEDV Datentechnik GmbH“. Manoma, kad nuo 2012 m. „Avira“ programinė įranga turi daugiau nei 100 milijonų klientų. 2012 m. birželio mėn. „Avira“ užėmė šeštąją vietą OPSWAT antivirusinės rinkos dalies ataskaitoje.“

„Comodo Antivirus“

„„Always on“ apsauga nuo virusų ir skaitytuvas pagal poreikį saugo įrenginį nuo virusų ir nesaugių taikomųjų programų. Nuskaitykite įdiegtas programas realiuoju laiku ir stebėkite kiekvieną diegimo procesą.“

„Bendrovę 1998 m. Jungtinėje Karalystėje įkūrė Melih Abdulhayoğlu. 2004 m. persikėlė į JAV kur jos produktai yra skirti kompiuterių ir interneto saugai. Bendrovė turi sertifikatų tarnybą, išduodančią SSL sertifikatus ir siūlančią informacijos saugumo produktus įmonėms ir vartotojams.“ (B. Athira, Neethu Babu ir M. Soumya Krishnan, 2017)

6 lentelė. Efektyvumo bandymo sąlygos skirtingoms antivirusinėms programoms

	Kaspersky Antivirus (2017)	Avast Free Antivirus (2017)	AVG Antivirus Free (2017)	Bitdefender Antivirus Free Edition (2017)	Avira Antivirus (2017)	Comodo Antivirus 10
„Tordow“ nuskaitymas pagal poreikį (On-Demand Tordow Scan)	+	+	+	+	+	+
„Tordow“ nuskaitymas pagal prieigą (On-Access Tordow Scan)	+	+	+	+	+	+
Interneto svetainės reitingas (Website Rating)	+	+	+	-	+	-
Kenkėjiškų URL blokavimas (Malicious URL Blocking)	+	+	+	+	+	+
Apsauga nuo duomenų vagystės (Phishing Protection)	+	+	+	+	+	+
Elgesio stebėjimu paremtas aptikimas (Behaviour Based Detection)	+	+	+	+	-	+
Papildomas pažeidžiamumo nuskaitymas (Bonus Vulnerability Scan)	+	+	-	-	-	-

Šaltinis: „International Journal of Pure and Applied Mathematics“ Volume 114 No. 12 2017, p. 85

Analizuojant prieš tai pateiktą „International Journal of Pure and Applied Mathematics“ lentelę „Efektyvumo bandymo sąlygos skirtingoms antivirusinėms programoms“ buvo sudaryta kibernetinio saugumo priemonės „Antivirusinių programų panašumų, skirtumų, privalumų ir trūkumų“ analizės lentelė (žr. 7 lentelė).

7 lentelė. Antivirusinių programų panašumai, skirtumai, privalumai ir trūkumai

Panašumai	Skirtumai	Privalumai	Trūkumai
Visos nagrinėtos antivirusinės programos turi šias funkcijas: „Tordow“ nuskaitymas pagal poreikį (On-Demand Tordow Scan); „Tordow“ nuskaitymas pagal prieigą (On-Access Tordow Scan); Kenkėjiškų URL blokavimas (Malicious URL Blocking); Apsauga nuo duomenų vagystės (Phishing Protection);	Avira Antivirus (2017) skiriasi nuo visų nagrinėtų programų tuo, kad ji neatlieka Elgesio stebėjimu paremtas aptikimo (Behaviour Based Detection) funkcijos.	Kaspersky Antivirus (2017) ir Avast Free Antivirus (2017) atitinka visas funkcijas, todėl jos turi daugiausiai pranašumų.	Daugiausiai antivirusinių programų negali atlikti šios funkcijos: Papildomas pažeidžiamumo nuskaitymas (Bonus Vulnerability Scan) - AVG Antivirus Free (2017), Bitdefender Antivirus Free Edition (2017), Avira Antivirus (2017), Comodo Antivirus 10

Šaltinis: sudaryta autorės

Apibendrinant galima daryti išvadas, kad visos nagrinėtos kibernetinio saugumo priemonės bankų veiklos rizikų valdymui (antivirusinės programos) turi šias funkcijas: „Tordow“ nuskaitymas pagal poreikį (On-Demand Tordow Scan); „Tordow“ nuskaitymas pagal prieigą (On-Access Tordow Scan); Kenkėjiškų URL blokavimas (Malicious URL Blocking); Apsauga nuo duomenų vagystės (Phishing Protection). Pagrindinis išskiriamas trūkumas, tai kad daugiausiai antivirusinių programų negali atlikti šios funkcijos: Papildomas pažeidžiamumo nuskaitymas (Bonus Vulnerability Scan) - AVG Antivirus Free (2017), Bitdefender Antivirus Free Edition (2017), Avira Antivirus (2017), Comodo Antivirus 10.

3. KIBERNETINIO SAUGUMO PRIEMONIŲ IR METODŲ BANKŲ RIZIKŲ VALDYME TAIKYMO VERTINIMAS

3.1. Tyrimo metodologija

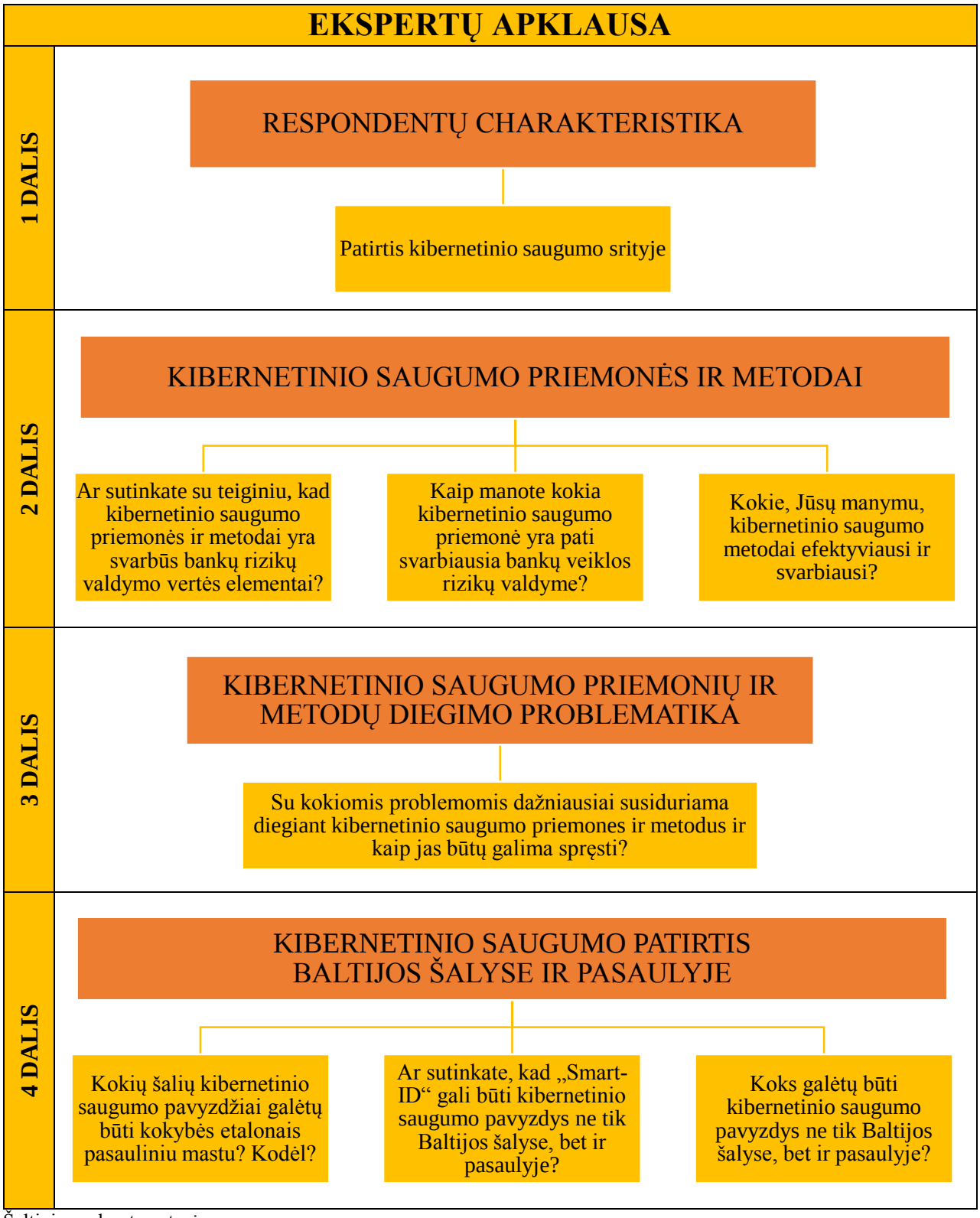
Remiantis Gulevičiūte G. (2013) ir Kardelio K. Mokslinių tyrimų metodologija ir metodais (2002) „tyrimui buvo pasirinktas kokybinis tyrimo metodas - ekspertų nuomonę norima išsiaiškinti standartizuoto interviu arba klausimyno forma. Kokybinių tyrimų taikytojai teigia, kad tokiu būdu gauti duomenys pateikia išsamesnę informaciją apie nagrinėjamą objektą, nei gauti kiekybiniais tyrimais (Tidikis, 2003).“ (Gulevičiūtė G., 2013)

Tyrimui panaudota anketa buvo sudaryti remiantis Kardelio Mokslinių tyrimų metodologija ir metodais (2002):

- „Svarbi anketos apimtis: ilga anketa tiriamąjį atbaido, todėl galimi paviršutiniški atsakymai.
- Svarbus ir anketos apipavidalinimas, klausimų kompozicija – tai gali sušvelninti kilusias neigiamas nuostatas.
- Reikia vengti klausimų, kurie stumia respondentą į vieną atsakymą.
- Reikia vengti sudėtingų, erzinančių klausimų.“ (Kardelis K. 2002)

Vadovautasi Kardelio (2002) klausimų paruošimo rekomendacijomis:

- „Dėl klausimų turinio: ar reikalingas klausimas?
- Kuo jis bus naudingas?
- Ar reikalingi keli klausimai, ar tik vienas?
- Ar klausimas turi būti konkretus, susijęs su respondento patirtimi?
- Ar respondentas turi reikiamą informaciją, kad galėtų atsakyti į klausimą?
- Ar klausimas tikslus, ar nereikės papildomų klausimų?
- Ar gausime tą informaciją, apie kurią klausiame?“ (Kardelis K. 2002)



Šaltinis: sudaryta autorės

14 pav. Anketos struktūros loginė schema

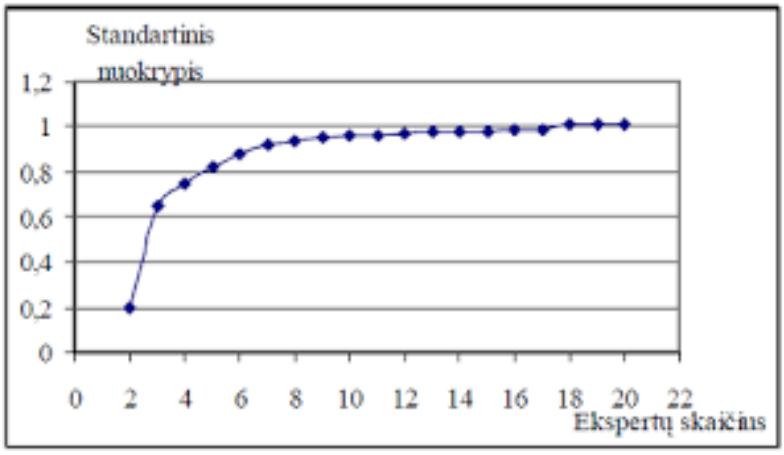
Pagal pateiktą schemą (14 pav.) galime matyti, kad klausimynas glaudžiai susijęs su kibernetinio saugumo priemonių ir metodų taikymu bankų rizikų valdyme Lietuvoje ir pasaulyje. Anketos klausimai buvo ruošiame remiantis teorija.

Kokybis tyrimas atliktas 2020 m. sausio 13 d. – vasario 12 d.

Šie septyni kibernetinio saugumo ekspertai dalyvavo tyrime: išlaikant konfidencialumą, jiems buvo suteikti kodai:

1) Ekspertas Nr. 1 *(atsakymai pateikti per elektroninę bankininkystę 2020-01-16)*
2) Ekspertas Nr. 2 *(interviu 2020-01-21)*
3) Ekspertas Nr. 3 *(interviu 2020-01-16)*
4) Ekspertas Nr. 4 *(atsakymai pateikti el. paštu 2020-01-17)*
5) Ekspertas Nr. 5 *(interviu 2020-01-16)*
6) Ekspertas Nr. 6 *(interviu 2020-01-16)*
7) Ekspertas Nr. 7 *(interviu 2020-02-06)*

Ekspertų skaičiaus nustatymas. Remianti Jegelavičiūte R., nustatant priimtiną ekspertų skaičių, buvo „vadovaujamasi metodologinėmis prielaidomis, suformuluotomis klasikinėje testų teorijoje, kurioje teigiama, jog agreguotų sprendimų patikimumą ir priimančių sprendimą (šiuo atveju ekspertų) skaičių sieja greitai gęstantis netiesinis ryšys. Įrodyta, jog agreguotų ekspertinių vertinimų moduliuose su vienodais svoriais nedidelės ekspertų grupės sprendimų ir vertinimų tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui (Rudzkienė, 2005).“ (Jegelavičiūte R., 2017)



Šaltinis: Rudzkienė, 2005 (http://lituka.com/wp-content/uploads/2017/03/ISSN-2424-3809-Nr-2-2017-03a.pdf)

15 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus

Tyrimo tikslas – išanalizuoti ekspertų nuomonę ir išskirti problemas taikant kibernetinio saugumo priemones ir metodus bankų veiklos rizikų valdymui; išskirti kibernetinio saugumo priemonių ir metodų pavyzdžius.

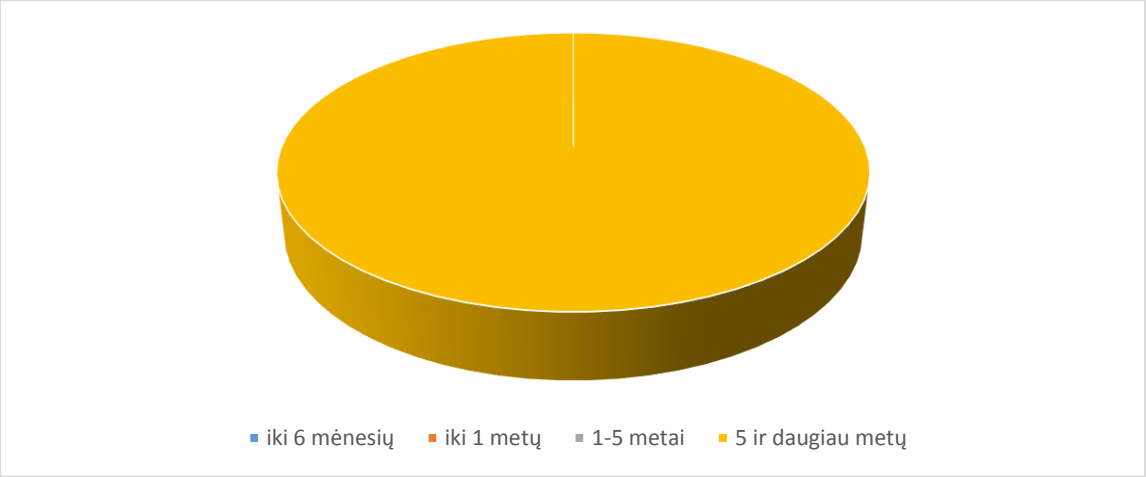
Tyrimo uždaviniai:

- Sužinoti ekspertų nuomonę ar kibernetinio saugumo priemonės ir metodai yra svarbūs bankų rizikų valdymo vertės elementai.
- Išsiaiškinti kokia kibernetinio saugumo priemonė yra pati svarbiausia bankų veiklos rizikų valdyme.
- Išsiaiškinti ar kibernetinis ir duomenų saugumas yra svarbiausias prioritetas finansinių paslaugų rinkoje.
- Sužinoti, kokie yra kibernetinio saugumo priemonės ir metodai efektyviausi ir svarbiausi.
- Sužinoti su kokiomis problemomis dažniausiai susiduriama diegiant kibernetinio saugumo priemones ir metodus ir kaip jas būtų galima spręsti.
- Sužinoti kokios šalys yra kibernetinio saugumo pavyzdžiai laikomi kaip kokybės etalonais pasauliniu mastu.
- Išsiaiškinti ar „Smart – ID“ galėtų būti kibernetinio saugumo pavyzdys ne tik Baltijos šalyse, bet ir pasaulyje.
- Išskirti kokie dar galėtų būti kibernetinio saugumo pavyzdžiai ne tik Baltijos šalyse, bet ir pasaulyje

Tyrimo objektas - Kibernetinio saugumo priemonės ir metodai bankų veiklos rizikų valdymui

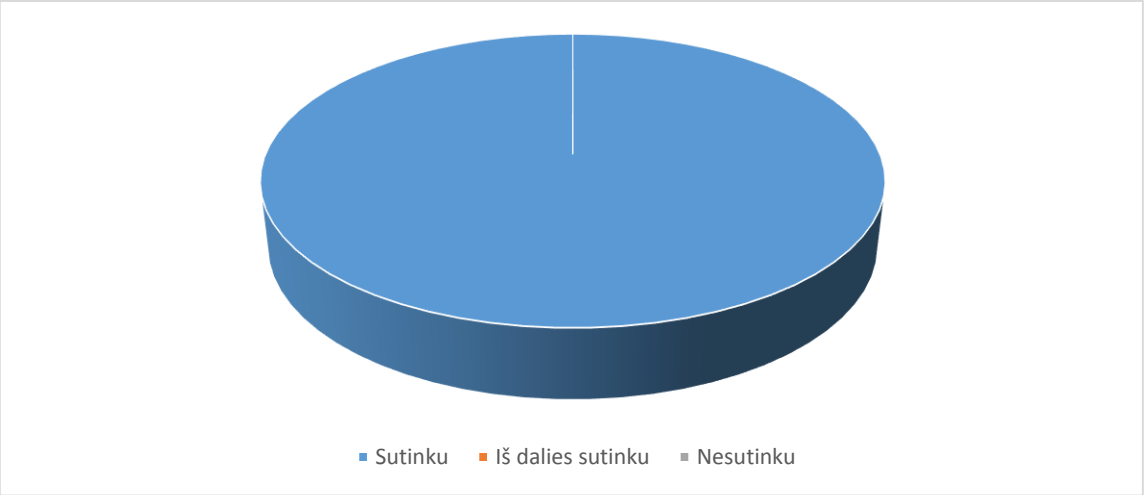
3.2. Tyrimo duomenų analizė

Atliekant tyrimą iš pradžių buvo išsiaiškinta kokia yra ekspertų darbo patirtis kibernetinio saugumo srityje. Visi ekspertai atsakė, kad dirba 5 ir daugiau metų kibernetinio saugumo srityje (žr. 16 pav.).



16 pav. Kibernetinio saugumo ekspertų patirtis

Atliekant tyrimą ekspertų buvo klausiama ar sutinka su teiginiu, kad kibernetinio saugumo priemonės ir metodai yra svarbūs bankų rizikų valdymo vertės elementai. Visi ekspertai atsakė, kad sutinka. Ekspertas Nr.2 atsakė kodėl sutinka: „Sutinku, todėl kad bankai iš esmės keičia savo pobūdį, seniau bankai būdavo fizinėse vietose, kurios turėjo savo adresus, kur galėjai nueiti, pamatyti banko darbuotoją, dabar bankų skyriai mažėja, jie keliasi į elektroninę erdvę, jie skatina pačius klientus atlikti operacijas, kurias anksčiau, kliento pageidavimo atlikdavo banko darbuotojai (pvz.: pavedimai, apmokėjimai už paslaugas ir kt.), dabar klientai turi įrankius, kuriuos suteikia bankai, todėl klientai viską daro elektroninėje erdvėje. Dėl šių priežasčių kibernetinis saugumas yra labai svarbus, nes jeigu tik kažkas kažkur nutinka, labai daug žmonių susirūpina. Jeigu paimtum ir mestum akmenį į minią žmonių, tai 99,9 proc., kad pataikytum į banko klientą, nes be banko sąskaitos, be mokėjimo kortelės šiais laikais yra pakankamai sudėtinga. Todėl kiekvienas iš mūsų susirūpina, nes kiekvienas iš mūsų turi pinigų banke ir sureaguoja žiniasklaida, kuri aprašinėja tokius dalykus.“ (žr. 17 pav.).



17 pav. Kibernetinio saugumo ekspertų nuomonė ar kibernetinio saugumo priemonės ir metodai yra svarbūs bankų rizikų valdymo vertės elementai?

Kokia kibernetinio saugumo priemonė yra pati svarbiausia bankų veiklos rizikų valdyme ekspertų nuomonės išssiskyrė, tačiau net

Ekspertas Nr.1 atsakė, kad „Išskirti vieną priemonę būtų neteisinga, svarbi jų visuma.“

Ekspertas Nr.2 atsakė, kad „Nėra vienos priemonės, nes viena priemonė negali apsaugoti banko klientų. Todėl negalėčiau įvardinti techninės priemonės. Ar tai būtų ugniasienė ar tai būtų antivirusinės programos.“

Ekspertas Nr.3 atsakė, kad yra pati svarbiausia kibernetinio saugumo priemonė bankų veiklos rizikų valdyme yra „Darbuotojų mokymai, prisijungimas prie elektroninės bankininkystės.“

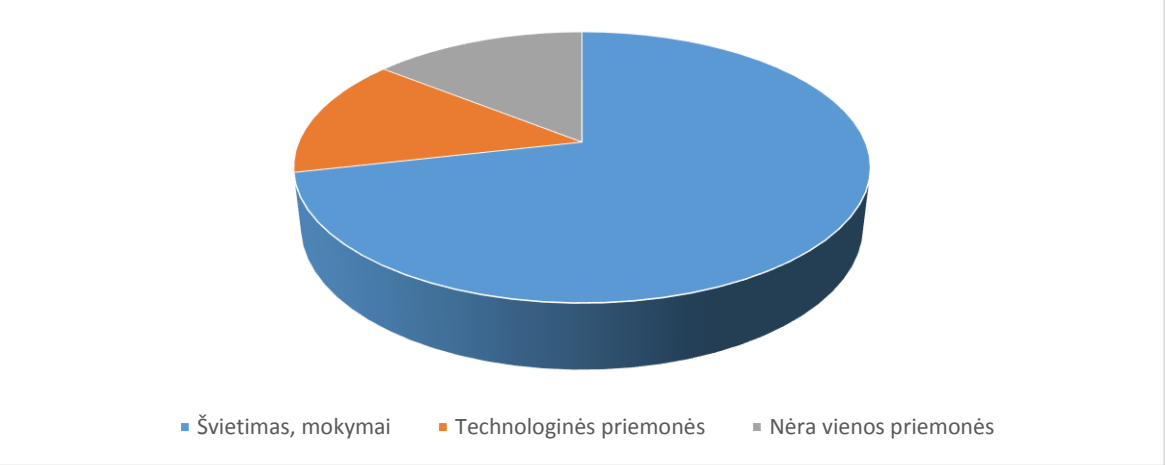
Ekspertas Nr.4 atsakė, kad „Mokymai (skaitmeninė higiena – o tiksliau visas personalo suvokimas ką galima daryti - ką ne, bei už saugumą atsakingų žmonių kompetencija).“

Ekspertas Nr.5 atsakė, kad „Reikia matyti rizikos vertinimą. Tarkim savi serveriai, kaip pavyzdys. Bankas turi užtikrinti informacijos vientisumą, kad sąskaitose esantys “skaičiukai” nebūtų pakeisti, antra konfidencialumas, kad informaciją nebūtų atskleista tretiems asmenims ir trečia prieinamumas, kad sąskaitos būtų pasiekiamos.“

Ekspertas Nr.6 atsakė, kad „Įgyvendinti Kibernetiniam saugumui techniniai ir organizaciniai reikalavimai, darbuotojų švietimas ir kompetencijos.“

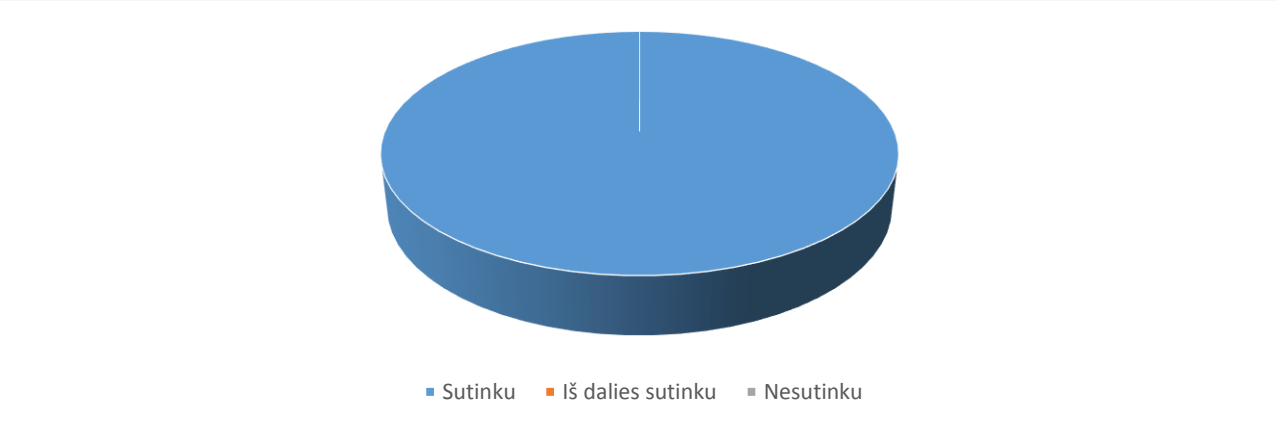
Ekspertas Nr.7 atsakė, kad „Technologinės priemonės, apsauga nuo įsilaužimų, duomenų bazių apsauga. Taip pat svarbu gyventojų ir darbuotojų švietimas.“

Dauguma ekspertų atsakė, kad svarbiausia kibernetinio saugumo priemonė yra švietimas, svarbu darbuotojų kompetencija ir sąmoningumas. (žr. 18 pav.).



18 pav. Kibernetinio saugumo ekspertų nuomonė kokia kibernetinio saugumo priemonė yra pati svarbiausia bankų veiklos rizikų valdyme

Ekspertai pritarė teiginiui, kad kibernetinis ir duomenų saugumas yra svarbiausias prioritetas finansinių paslaugų rinkoje. Visi pasirinko atsakymą „sutinku“. (žr. 19 pav.).



19 pav. Kibernetinio saugumo ekspertų nuomonė ar kibernetinis ir duomenų saugumas yra svarbiausias prioritetas finansinių paslaugų rinkoje

Kokie kibernetinio saugumo metodai efektyviausi ir svarbiausi ekspertų nuomone yra šie: Ekspertas Nr.1 atsakė, kad „Negalima išskirti vieno, svarbi jų visuma. Efektyvumas ir prioritetas (svarba) nebūtinai sutampa.“

Ekspertas Nr.2 atsakė, kad „Mokymai. Iš mano praktikos, kadangi silpniausia grandis yra bankinių paslaugų vartotojas arba banko darbuotojas, Jei tas žmogus nėra tinkamai apmokytas ir tinkamai

paruoštas darbui su kibernetinėmis rizikomis tai jis yra silpniausia grandis, nesvarbu kokias sistemas bankai naudoja, gali būti pačios naujausios, atnaujintos, per žmogų vis tiek bus galima sukompromituoti, jei jis nebus tinkamai apmokytas. Todėl svarbu, kad bankinių paslaugų vartotojas arba banko darbuotojas būtų apmokytas kaip tam tikrose situacijose elgtis.“

Ekspertas Nr.3 atsakė, kad „Žmogaus sąmoningumas ir švietimas, antivirusai, slaptažodžių keitimai.“

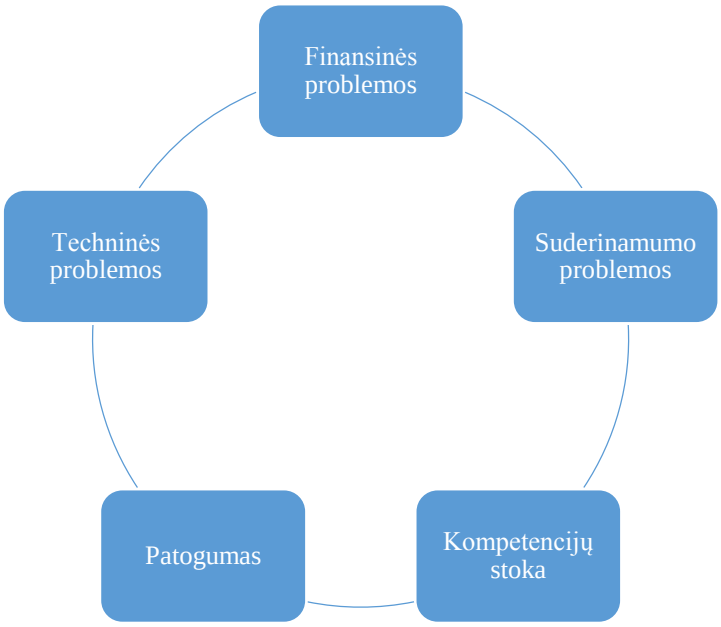
Ekspertas Nr.4 atsakė, kad „Mokymai, nuolatinis žinių ir naudojamų sprendimų tikrinimas bei tobulinimas. Jokia programinė įranga neapsaugos nuo klaidingų vartotojų veiksmų.“

Ekspertas Nr.5 atsakė, kad „Organizacinės ir techninės. Organizacinės priemonės yra greičiau ir lengviau įgyvendinamos, t.y. mokymai, tvarkos, procesai. Techninės priemonės yra brangesnės ir lėčiau įdiegiamos. Tiek organizacinės tiek techninės priemonės yra svarbios, nes tik organizacinėmis priemonėmis nepavyks pasiekti, vis tiek bus reikalingos techninės priemonės.“

Ekspertas Nr.6 atsakė, kad „Kolektyvinė kibernetinė apsauga“.

Ekspertas Nr.7 atsakė, kad „Švietimas, pirma gynybos linija. Tik informuotas vartotojas galės apsiginti. Tema yra nauja ir specifinė, todėl informuotas vartotojas galės atpažinti grėsmę. Pvz.: elektroniniai sukčiai sukuria sistemas, bankų vartotojai turi gebėti jas atpažinti.“

Su kokiomis problemomis dažniausiai susiduriama diegiant kibernetinio saugumo priemones ir metodus ir kaip jas būtų galima spręsti, ekspertai išskyrė pačias svarbiausias problemas (žr. 20 pav.).



20 pav. Kibernetinio saugumo problematika dažniausiai susiduriama diegiant kibernetinio saugumo priemones ir metodus

8 lentelė. Kibernetinio saugumo problemos ir sprendimo būdai

Kibernetinio saugumo problemos ir sprendimo būdai
Dėl saugumo priemonių dažnai tenka apriboti patogumą ir jos reikalauja papildomų resursų. Reiktų ieškoti pusiausvyros tarp saugumo ir patogumo, tarp kaštų ir rizikos. *(1 E, interviu per el. bankininkystę, 2020-01-16)*
Kaštų klausimas ir patogumo klausimas. Tikriausiai būtų sunku surasti žmogų, kuris pakeltų ranką ir pasakytų, kad jam yra labai patogu ir lengva kas kartą suvedinėti dvylikos simbolių slaptažodį jungiantis prie bankinės sistemos. Kadangi kai nueini nuo kompiuterio jis užsirakina ir grįžus slaptažodį reikia vėl įvedinėti, tai tikrai niekam nėra patogu. Todėl nerastume žmogaus, kuriam tai būtų patogu, nes slaptažodis negali būti šiaip kažkoks žodis iš dvylikos simbolių, todėl skaičiai, mažosios, didžiosios raidės – neišvengiamai tai yra nepatogu. Kaip spręsti? Reikia ieškoti balanso tarp kaštų ir patogumo. *(2 E, asmeninis interviu, 2020-01-21)*
Finansinėmis, didinti finansavimą. *(3 E, asmeninis interviu, 2020-01-16)*
1. Problema atsakingiems asmenims paaiškinti ir pagrįsti tam tikrų ir pakankamai brangių priemonių reikalingumą. 2. Suderinamumo problemos ypač kai šiuolaikinės priemonės diegiamos pakankamai senose sistemose. 3. Darbuotojų mokymai siekiant užtikrinti sklandų darbą. *(4 E, interviu el. paštu, 2020-01-17)*
Susiduria su šiomis problemomis: 1. Su pinigų stoka 2. Su kompetencijų stoka. Jas spręsti būtų galima: 1. Skirti finansavimą 2. Pirkti paslaugas *(5 E, asmeninis interviu, 2020-01-16)*
Finansinėmis. Neatliekamas saugumo priemonių testavimas ar efektyviai jos veikia. Reikia subalansuoti kaštus ir saugumo priemonių efektyvumą. Naudotis gerąja pasauline praktika. *(6 E, asmeninis interviu, 2020-01-16)*
1. Diegiant kibernetinio saugumo priemones dažniausiai susiduriama su tai, kaip pasiekti vartotojų didelį kiekį, paaiškinti ganėtinai sudėtingą kibernetinio saugumo elementą. 2. Taip pat susiduriama su techninėmis problemomis – didelė įrangos kaina ir kompetencijų stoka. Kibernetinis saugumas yra labai dinamiškas ir gali kiekvieną dieną pasikeisti. Turime suspėti su („hakerių“) programišių greičiu. 3. Informacinės priemonės tampa labiau kompleksinės, jos sudėtingėja, duomenų bazės labai panašėja, daiktų internetas, kamerų įranga, susidaro daugiau pažeidžiamumo, kuriuos išnaudoja, todėl problematika lieka neišsprendžiama. *(7 E, asmeninis interviu, 2020-02-06)*

Šaltinis: sudaryta autorės

Atliekant kokybinį tyrimą buvo siekiama išsiaiškinti, kokių šalių kibernetinio saugumo pavyzdžiai galėtų būti kokybės etalonais pasauliniu mastu. (žr. 21 pav.).

Ekspertas Nr.1 atsakė, kad „Kibernetinis saugumas yra plati sąvoka ir galimi skirtingi etalonai priklausomai nuo vertinamos srities.“

Ekspertas Nr.2 atsakė, kad „Nėra tokios šalies, nes trūksta objektyvių priežasčių. Reikia atkreipti dėmesį į patį banką, kaip bankas sprendžia problemą jei yra prarandami pinigai ne dėl kliento kaltės.“

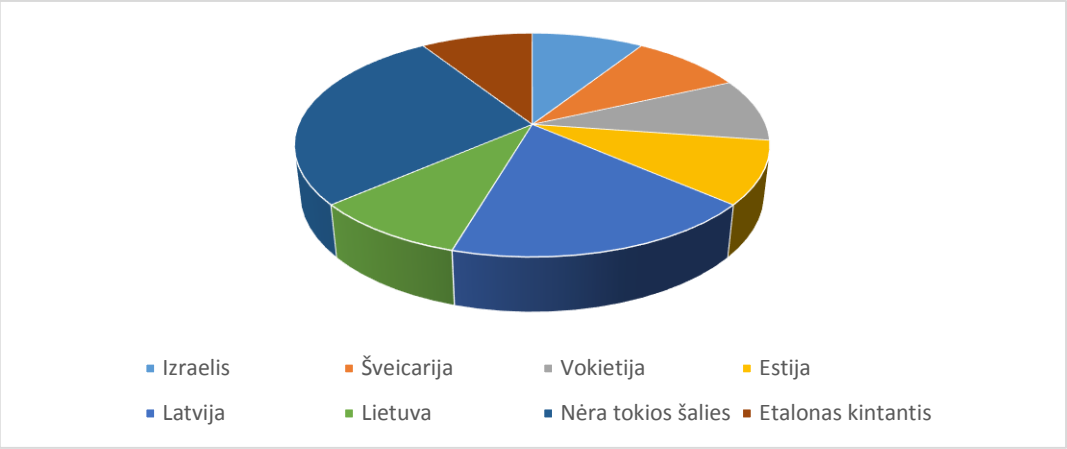
Ekspertas Nr.3 atsakė, kad „Šveicarija“.

Ekspertas Nr.4 atsakė, kad „Izraelis, labai daug kompanijų kurios orientuojasi į specifinius saugumo sprendimus, kibernetinio saugumo mokymams yra skiriamas labai didelis dėmesys ir tai atsiperka su kaupu.“

Ekspertas Nr.5 atsakė, kad „Reikia žiūrėti per standartų prizmę, kas nustato standartus. Bankininkystėje yra daug standartų (Kortelių aptarnavimo standartas, ISO ir t.t.) Tiesiogiai žiūrėti į šalis, JAV galėtų būti labai saugi, bet juk visai nesenai ten dar nebuvo „čipinių kortelių“, nes jie paskaičiavo, kad tai bus didelė vagysčių rizika, pinigai bus pavogiami nuskaitant įmagnetintą kodą ir tai bus vis tiek mažesni kaštai nei įdiegiant naują sistemą. Realiai sistema nesaugi, tačiau kaštai, kuriuos reikėjo įdiegti buvo per dideli. Dabar jau sistema yra įdiegta. Todėl etalonas yra kintantis.“

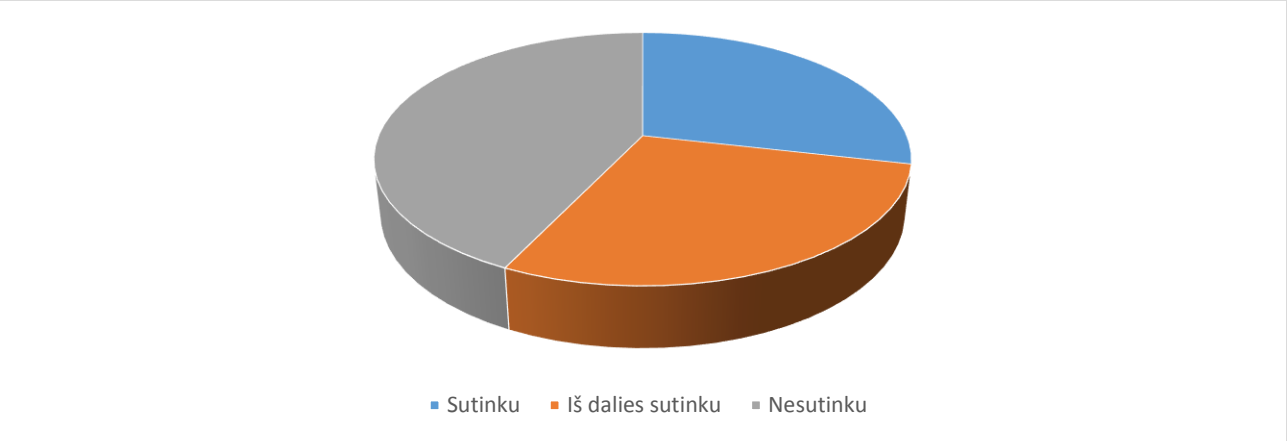
Ekspertas Nr.6 atsakė, kad „Lietuva, nes užimą 4 vietą, taip pat saugumo pavyzdžiais gali būti Estija, Vokietija, Latvija.“

Ekspertas Nr.7 atsakė, kad „Nėra vienos šalies, priežastis yra internetas, nes interneto tinklelis neturi ribų.Yra tik šalys, kurios kontroliuoja: Kinija, Rusija, Iranas, Arabų šalys turi specifines ugniasienes (firewall), šios šalys apriboja youtube.com, facebook.com ir kt. bei kontroliuoja piliečius.“



21 pav. Kibernetinio saugumo ekspertų nuomonė: šalys, kurios galėtų būti kibernetinio saugumo kokybės etalonais pasauliniu mastu

Kibernetinio saugumo ekspertų buvo klausiama apie „Smart-ID“, buvo norima sužinoti ar jie pritaria teiginiui: **„**Smart-ID“ gali būti kibernetinio saugumo pavyzdys ne tik Baltijos šalyse, bet ir pasaulyje“. Ekspertų nuomonės pasiskirstė taip: du ekspertai atsakė, kad sutinka, du ekspertai, kad iš dalies sutinka ir 3 ekspertai, kad nesutinka. (žr. 22 pav.).



22 pav. Kibernetinio saugumo ekspertų nuomonė, kad „Smart-ID“ gali būti kibernetinio saugumo pavyzdys ne tik Baltijos šalyse, bet ir pasaulyje

Ekspertai, kurie nesutiko su prieš tai buvusiu teiginiu, kad „Smart-ID“ gali būti kibernetinio saugumo pavyzdys ne tik Baltijos šalyse, bet ir pasaulyje išskyrė kitus pavyzdžius:
Mobilusis parašas galėtų būti kaip saugiausias ir patikimiausias saugumo pavyzdys ne tik Baltijos šalyse, bet ir pasaulyje *(3 E, asmeninis interviu, 2020-01-16).*
Pavyzdžių labai daug, geriausi pavyzdžiai yra „Fintech“ startuoliai kurie projektuoja savo produktus visų pirma atsižvelgdami į saugumo iššūkius, vietoj to, kad kurti produktą kuriam po to bando pritaikyti saugumo sprendimus *(4 E, interviu el. paštu, 2020-01-17).*
Nėra gerų pavyzdžių, nes viską galima „nulaužti“. Tačiau kelių kibernetinio saugumo priemonių komplektas yra geras *(5 E, asmeninis interviu, 2020-01-16).*
USB šifruotas nuotolinis prisijungimas (fincort.io) *(6 E, asmeninis interviu, 2020-01-16).*

Tyrimo išvados:

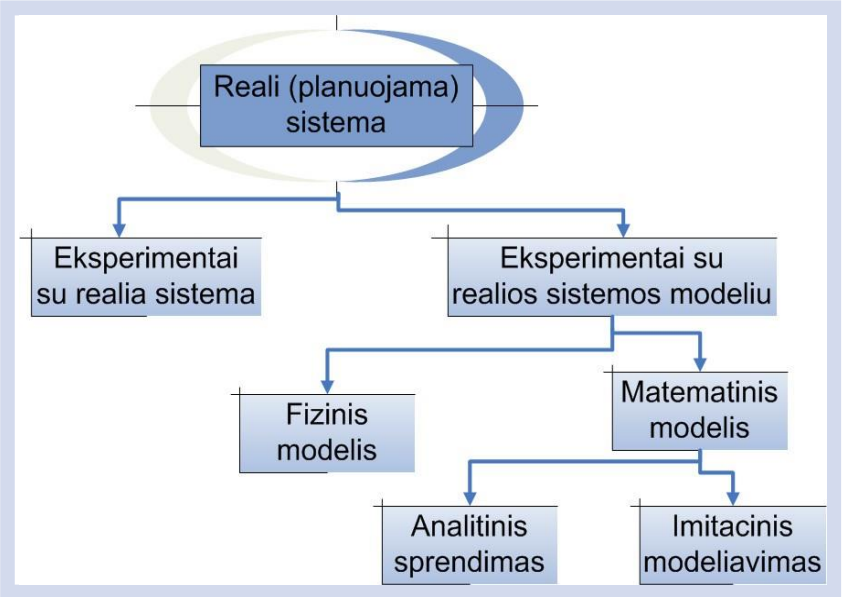
- Pasitelkiant ekspertų žinias, išsiaiškintos pagrindinės problemos, atsirandančias diegiant kibernetinio saugumo priemones ir metodus: finansinės, techninės, suderinamumo problemos, kompetencijų stoka, patogumo klausimas.
- Išskirti kibernetinio saugumo priemonių ir metodų pavyzdžiai: švietimas, mokymai, technologinės priemonės, kolektyvinė kibernetinė apsauga.

- Išsiaiškinta ekspertų nuomonė apie tai, ar kibernetinio saugumo priemonės ir metodai yra svarbūs bankų rizikų valdymo vertės elementai – visi ekspertai sutiko su šiuo teiginiu.
- Sužinota ekspertų nuomonė kokia kibernetinio saugumo priemonė yra pati svarbiausia bankų veiklos rizikų valdyme: švietimas, mokymai.
- Sužinota kokios šalys yra kibernetinio saugumo pavyzdžiai laikomi kaip kokybės etalonais pasauliniu mastu: Izraelis, Šveicarija, Vokietija, Estija, Latvija, Lietuva.
- Išsiaiškinta ar „Smart – ID“ galėtų būti kibernetinio saugumo pavyzdys ne tik Baltijos šalyse, bet ir pasaulyje: du ekspertai sutiko su šiuo teiginiu, du – iš dalies sutiko, trys ekspertai nesutiko.
- Išskirta kokie dar galėtų būti kibernetinio saugumo pavyzdžiai ne tik Baltijos šalyse, bet ir pasaulyje: Mobilusis parašas, USB šifruotas nuotolinis prisijungimas.

4. KIBERNETINIO SAUGUMO MODELIS: KOLEKTYVINĖS KIBERNETINĖS APSAUGOS PRIEMONIŲ, METODŲ IR SPRENDIMO BŪDŲ SUDERINAMUMAS BANKŲ VEIKLOS RIZIKŲ VALDYMUI

4.1 Modeliavimo metodologija

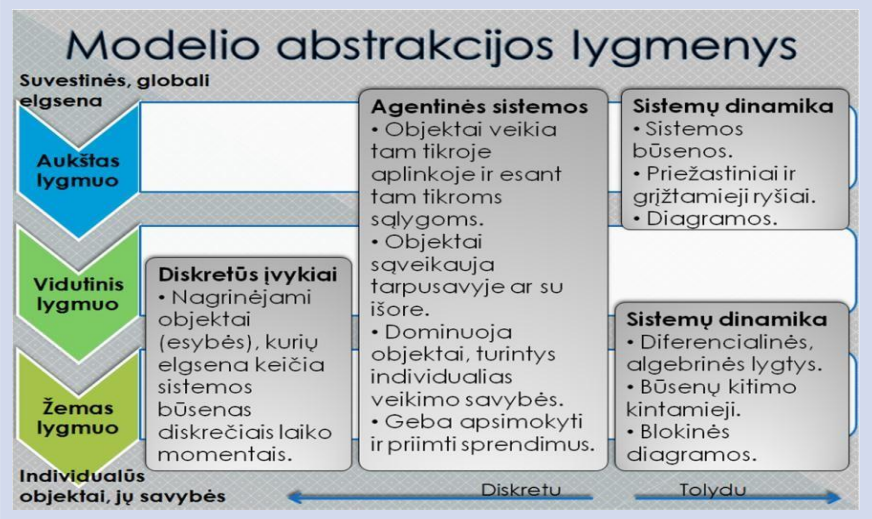
Pilakauskas V. (2011) teigia, kad modelis – tai abstrakti konstrukcija, kuria mėginama atkartoti kai kurias realios sistemos savybes. Modelio kūrimas įvardijamas kaip modeliavimas.



Šaltinis: Pilakauskas V. (2011)

23 pav. Modelių schema

Remiantis Pilakausko V. (2011) modelių schema, buvo sukurtas imitacinis modelis (žr. 25 pav.) Imitacinio modeliavimo metodas turi daug privalumų. Matematiškai sugebėti adekvačiai aprašyti realią sistemą yra pakankamai sudėtinga; o imitacinis modelis gali būti sudaromas bet kokiai realiai sistemai. Modeliuotojui gali reikėti daug žinių ir kompetencijos sprendžiant analitinio modelio lygtis. Manoma, kad mažiau laiko ir pastangų reikia sudarant imitacinį modelį. (Pilakauskas V., 2011)



Šaltinis: Vytautas Pilakauskas (2011)

24 pav. Modelio abstrakcijos lygmenys

Remiantis modelio abstrakcijos lygmenimis (žr. 24 pav.) yra skirtoma į tris lygmenis: žemas lygmuo, vidutinis lygmuo ir aukštas lygmui. Kibernetinio saugumo modelis bankų veiklos rizikų valdymui buvo kuriamas atsižvelgiant į aukšto lygmens suvestinės elgseną (Diskretūs įvykiai, Agentinės sistemos ir Sistemų dinamika).

Algeier S. ir kt. (2018) rašo, kad kibernetinio saugumo ekspertai visoje vyriausybėje ir pramonėje susiduria su bauginančia, bet rimta realybe, kuri pati nusižengia vien jau nebegali būti valdančioji praktika. Yra didelis poreikis apibrėžtos kolektyvinės gynybos.

Štitilis D., Laurinaitis M. ir kt. (2017) teigia, kad „interneto ir kitų informacinės infrastruktūros paslaugų teikėjų teikiamos paslaugos dažnai neužtikrina paslaugų naudotojų saugos. Ekonominiu sunkmečiu elektroninės informacijos saugai (kibernetiniam saugumui) skiriama nepakankamai dėmesio ir informacinių išteklių, o taikant kolektyvinės saugos principą būtų veiksmingiau naudojami informaciniai ištekliai.“

Paulauskas A. (2016) pabrėžia, „kad Lietuvoje vis dar neveikia kolektyvinė kibernetinė gynyba, nes kibernetinio išpuolio atveju dalis institucijų, neprisijungusių prie saugaus duomenų perdavimo tinklo, negalėtų tinkamai funkcionuoti ir be trikdžių teikti paslaugas gyventojams. Lietuvoje šiandien turime situaciją, kai rūpinimasis kolektyvine kibernetine gynyba kol kas lieka tik kalbomis.“

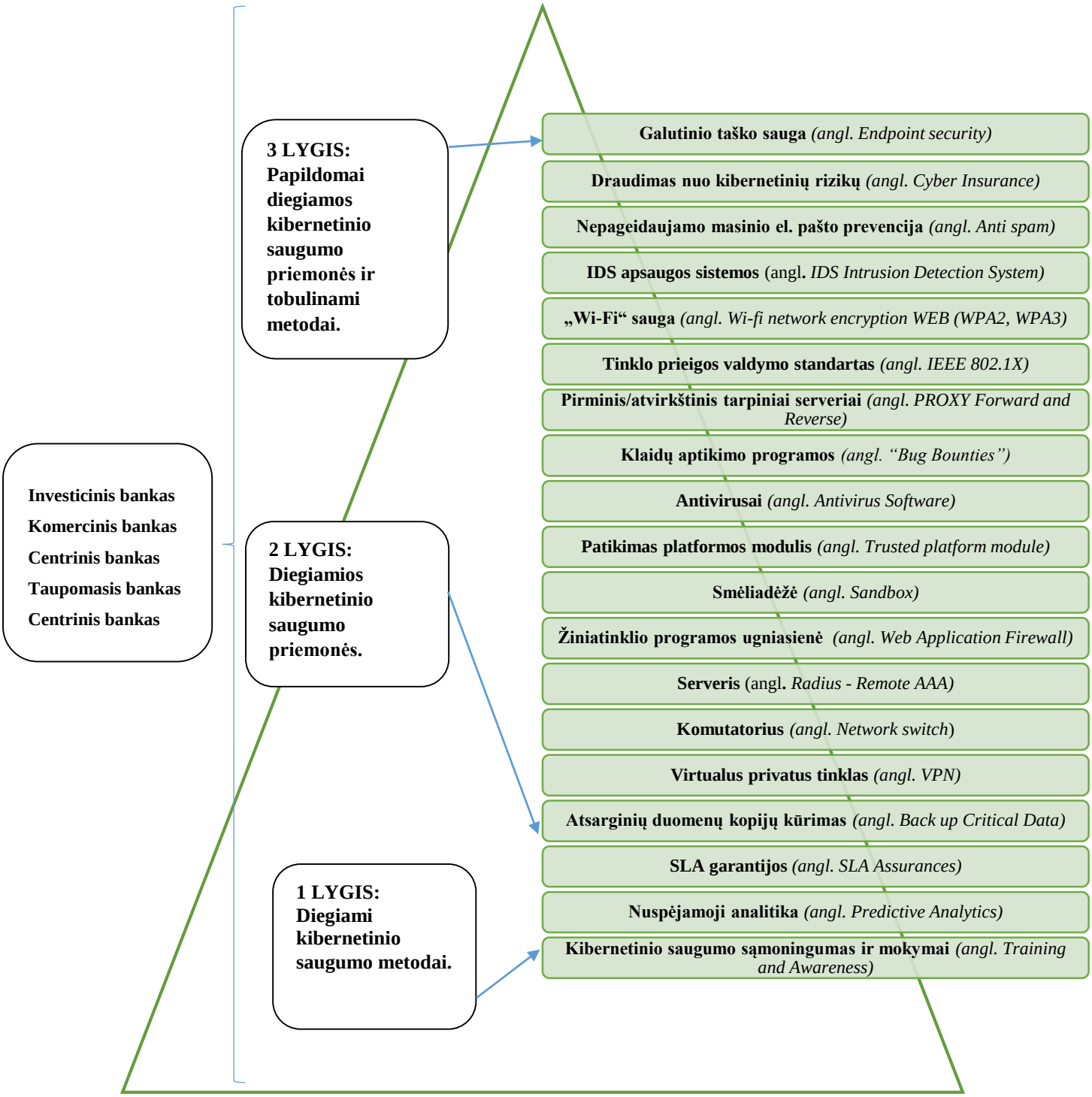
Taip pat Štitilis D., Laurinaitis M. ir kt. (2017) teigia, kad „kolektyvinės apsaugos principu tikslinga vadovautis ne tik nacionaliniu, bet ir tarptautiniu lygiu. Kompetentingų specialistų bendradarbiavimas, keitimasis turima informacija ir patirtimi yra būtina veiksmingo išankstinio perspėjimo ir prevencinės veiklos sąlyga.“

4.2 Modelio analizė

Kolektyvinės kibernetinės apsaugos modelio piramidė: kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų suderinamumas bankų veiklos rizikų valdymui (žr. 25 pav.) buvo sudaryta remiantis atlikta teorine analize, ekspertinės apklausos analize bei gerosios pasaulinės patirties analize. Modeliui buvo parinkti tarpusavyje derantys, svarbiausi bankų veiklos rizikų valdymui taikomi kibernetinio saugumo metodai, priemonės ir sprendimo būdai užtikrinantys kibernetinį saugumą.

Remiantis Wai O. (2019), kolektyvinė gynyba yra galinga ir sena idėja. Šią koncepciją galima pamatyti visose srityse, pradedant NATO įkūrimu ir baigiant 13 Amerikos kolonijų, susibūrusių kartu 1776 m. Dabar, šiandieniniame skaitmeniniame amžiuje, kas būtų, jei verslai suformuotų panašų kolektyvinės gynybos ar kolektyvinio saugumo aljansą prieš kibernetines grėsmes? Wai O. (2019), konstatuoja, kad tokio strateginio aljanso kibernetinėje erdvėje logika ir vertybė yra didžiulė - ypač kai atsižvelgiame į šių dienų grėsmių mastą ir sunkumą, bendradarbiavimo naudą ir santykinius individualių pastangų kibernetinėje gynyboje trūkumus. Nors dalijimasis informacija, siekiant geresnio kibernetinio saugumo, nėra nieko naujo, sėkmė ją įgyvendinant apima dvigubai daugiau klausimų, kaip praktiškai verslo aplinkoje iš tikrųjų turėtų atrodyti kibernetinio saugumo kolektyvinė gynyba.

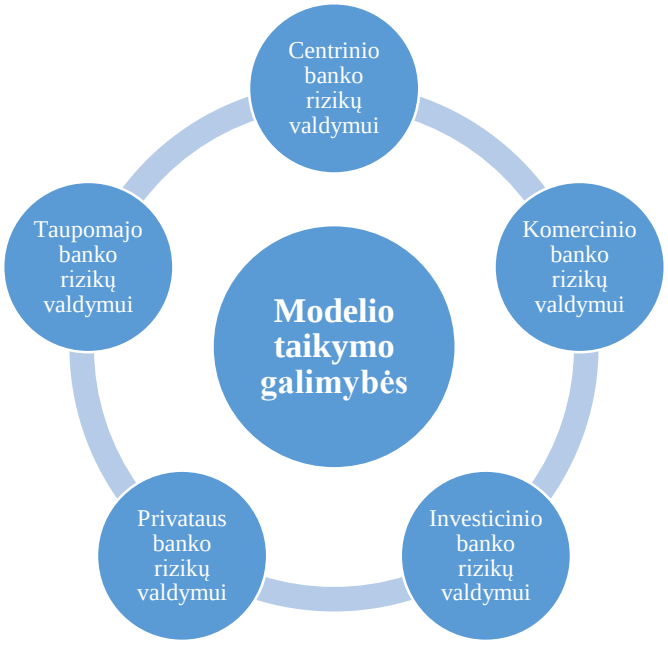
Kolektyvinės kibernetinės gynybos tikslas yra suburti kelias organizacijas kartu, o Kolektyvinės kibernetinės apsaugos modelio tikslas sujungti suderinamas kibernetinės apsaugos priemones bankų veiklos rizikų valdymui, metodus ir sprendimo būdus. (žr. pav. 25). Modelis skirtomas į tris etapus: pirmame etame yra diegiami kibernetinio saugumo metodai, piramidės apačioje: Kibernetinio saugumo sąmoningumas ir mokymai (angl. Training and Awareness), tai įvardijama kaip kibernetinio saugumo diegimo pagrindas. Vėliau yra išskiriama antroji dalis, kada yra diegiamos kibernetinio saugumo priemonės, pradedant nuo atsarginių duomenų kopijų kūrimo (angl. Back up Critical Data), tai ypač svarbu dėl duomenų pažeidimo ar neteisėto panaudojimo. Kylant piramide aukštyn yra įdiegiamos svarbiausios kibernetinio saugumo priemonės, kurios dera ir sąveikauja tarpusavyje. Trečioje dalyje papildomai diegiamos kibernetinio saugumo priemonės ir tobulinami metodai. Skiriamas dėmesys draudimui nuo kibernetinių rizikų, vykdoma nepageidaujamo masinio el. pašto prevencija.



Šaltinis: Sudaryta autorės

25 pav. Kolektyvinės kibernetinės apsaugos modelis: kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų suderinamumas bankų veiklos rizikų valdymui

4.3 Modelio taikymo galimybės



Šaltinis: Sudaryta autorės

26 pav. Modelio taikymo galimybės

Sukurtas modelis (žr. pav. 25) gali būti taikomas įvairių bankų (žr. pav. 26) veiklos rizikų valdymui. Įdiegiant kibernetinio saugumo metodus ir priemones nuo pirmojo iki trečiojo lygio. Iš pradžių diegiant metodus, o paskui prijungiant priemones. Procesų vienodumas ir jų taikymas leidžia greitai pastebėti esminius trūkumus. (Štitilis D., Laurinaitis M. ir kt., 2017). Kibernetinis saugumas yra kritiškiausias ir neatidėliotinas rūpestis bankams, jų klientams ir platesnei finansų sistemai. Finansų institucijos susiduria su kasdieniais kibernetinių užpuolimų atvejais, dėl kurių gali būti prarasti duomenys, turtas ir pasitikėjimas savimi, todėl plečiantis skaitmeninei bankininkystei yra neišvengiama naudoti tinkamą ir saugų kibernetinio saugumo modelį. (Grasshoff G., Bohmayr W. ir kt., 2018)

Bankai turi didelį klientų duomenų ir finansinio turto kiekį kas verčia juos tapti kibernetinių išpuolių taikiniais - beveik ketvirtadalis visų kibernetinių išpuolių yra nukreipti į juos. (Grasshoff G., Bohmayr W. ir kt., 2018)

Dabar bankai sustiprino savo galimybes aptikti išpuolius ir į juos greitai sureaguoti, tačiau daugumai jų reikia strategiškai permąstyti kokį tinkamą ir saugiausią modelį naudoti. Be strateginių investicijų, naujų technologijų ir darbo metodų visoje organizacijoje, reikalingas naujas kibernetinio saugumo modelis. Užduotis sudėtinga, tačiau prizas vertingas: saugi bankų sistema skaitmeniniam amžiui. (Grasshoff G., Bohmayr W. ir kt., 2018)

IŠVADOS IR PASIŪLYMAI

1. Magistro baigiamajame darbe buvo išanalizuoti kibernetinio saugumo priemonių ir metodų taikymo teoriniai aspektai. Teoriniai aspektai apima kibernetinio saugumo sąvoką; kibernetinio saugumo aktualumą bankuose, kibernetinio saugumo sprendimus (metodus ir priemones): nuspėjamoji analitika (norėdami veiksmingai pasipriešinti kibernetinėms atakoms, IT darbuotojai turi žinoti, kaip atrodo ataka, kada ji gali įvykti ir iš kur kildinama); Atsarginių duomenų kopijų kūrimas (bankams svarbu turėti parengtą atsarginių duomenų kopijų kūrimo planą); Draudimas nuo kibernetinių rizikų (dauguma įmonių įsigijo draudimo planus, kad apsisaugotų nuo galimų finansinių nuostolių); Klaidų aptikimo programos (tiek privačios įmonės, tiek vyriausybinės institucijos įgyvendino „klaidų aptikimo“ politiką, kad sustiprintų savo programinės įrangos saugumą); Mokymas ir sąmoningumas (darbuotojų mokymas apie naujausią sukčių naudojamą taktiką gali padėti sumažinti tikimybę, kad jie paspaus nuorodas į kenksmingą programinę įrangą). Išskirta kibernetinio saugumo problematika: DDoS atakos (per pastaruosius kelerius metus tapo viena ryškiausių kibernetinių nusikaltimų formų); Kenkėjiška programa (nuolat atsiranda vis naujų kenkėjiškos programinės įrangos formų, kurios kelia grėsmę organizacijoms ir asmenims); Duomenų vagystė („Verizon“ ataskaitoje nustatyta, kad žmonės šešis kartus dažniau spustelėjo ant suklastoto el. laiško nei ant įprastinio rinkodaros el. laiško); Vidinis piktnaudžiavimas (net geriausios kibernetinio saugumo priemonės gali tapti neveiksmingos, darbuotojams priėmus sprendimą piktnaudžiauti savo prieigos teisėmis).

2. Remiantis atvejo analizės metodu, išanalizuota pasirinktų šalių kibernetinio saugumo metodai ir priemonės: atlikus „Bank of America“ (JAV) atvejo analizę, buvo išsiaiškinta, kad „Bank of America“ remiasi 20 CC ir juos įvardija kaip pagrindiniais kibernetinio saugumo metodais ir priemonėmis tai ypač svarbios efektyviai kibernetinei gynybai saugumo kontrolės priemonės. „Bank of China“ (Kinijos) atvejo analizės metodu buvo analizuojamas - dviejų faktorių autentifikavimas. Siekdama padidinti internetinio saugumo lygį, „Bank of China“ klientams teikia platų dviejų veiksnių autentifikavimo priemonių asortimentą, skirtą apsaugoti nurodytas operacijas ir nurodytas investavimo operacijas, kurias klientai vykdo naudodamiesi internetine / mobiliąja bankininkyste. Naudodajant prieigos raktą, galima patvirtinti nurodytas internetinės bankininkystės operacijas arba nurodytas investavimo operacijas, sukurdami vienkartinį „apsaugos kodą“ arba „operacijos patvirtinimo kodą“. Baltijos šalių (Estijos ir Lietuvos) atvejo analizės metodu buvo analizuojamas – „Smart ID“ kibernetinio saugumo priemonių ir metodų taikymo galimybės. „Tai naujasis patogus asmens tapatybės nustatymo sprendimas. Jį yra paprasta bei lengva naudoti ir tai yra puiki alternatyva

bankų kodų kortelėms. Naudodamiesi „Smart-ID“, vartotojai gali jungtis prie elektroninių paslaugų ir patvirtinti operacijas bei susitarimus.“ Nors „Smart-ID“ pastaruoju metu susilaukia vis daugiau kritiškos nuomonės, kad ši priemonė yra nesaugi, kad į ją lengva įsilaužti (atvejis, kai 2019 m. liepą, Estijoje buvo įvykdyta tapatybės vagystė pasinaudojant „Smart-ID“ ir socialine inžinerija). Po pastarųjų įvykiu „Smart-ID“ papildomai informuoja vartotojus laiškais apie naujai sukurtas paskyras, kad taip būtų galima išvengti kenkėjiško klonavimo. Analizuojant Lietuvos Respublikos Nacionalinio saugumo strategijojoje smulkiai aprašytus Lietuvos Respublikos kibernetinio saugumo stiprinimo veiksmus buvo išskirtas vienas svarbiausių veiksmų: stiprinti nacionalinius gebėjimus nustatyti kibernetinio saugumo incidentus, bei likviduoti jų padarinius. Išanalizavus 2011 – 2017 metų Lietuvos Respublikos Valstybės saugumo departamento ataskaitos, galima teigti, kad ne visose ataskaitose buvo minimas kibernetinis saugumas (paminėta 2011, 2012 ir 2016 metais).

3. Pasitelkiant ekspertų žinias, išsiaiškintos pagrindinės problemos, atsirandančias diegiant kibernetinio saugumo priemones ir metodus: finansinės, techninės, suderinamumo problemos, kompetencijų stoka, patogumo klausimas. Išskirti kibernetinio saugumo priemonių ir metodų pavyzdžiai: švietimas, mokymai, technologinės priemonės, kolektyvinė kibernetinė apsauga. Išsiaiškinta ekspertų nuomonė apie tai, ar kibernetinio saugumo priemonės ir metodai yra svarbūs bankų rizikų valdymo vertės elementai – visi ekspertai sutiko su šiuo teiginiu. Sužinota ekspertų nuomonė kokia kibernetinio saugumo priemonė yra pati svarbiausia bankų veiklos rizikų valdyme: švietimas, mokymai. Sužinota kokios šalys yra kibernetinio saugumo pavyzdžiai laikomi kaip kokybės etalonais pasauliniu mastu: Izraelis, Šveicarija, Vokietija, Estija, Latvija, Lietuva. Išsiaiškinta ar „Smart – ID“ galėtų būti kibernetinio saugumo pavyzdys ne tik Baltijos šalyse, bet ir pasaulyje: du ekspertai sutiko su šiuo teiginiu, du – iš dalies sutiko, trys ekspertai nesutiko. Išskirta kokie dar galėtų būti kibernetinio saugumo pavyzdžiai ne tik Baltijos šalyse, bet ir pasaulyje: Mobilusis parašas, USB šifruotas nuotolinis prisijungimas.

4. Sukurtas Kolektyvinės kibernetinės apsaugos modelis: kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų suderinamumas bankų veiklos rizikų valdymui. Kolektyvinės kibernetinės apsaugos modelio piramidė buvo sudaryta remiantis atlikta teorine analize, ekspertinės apklausos analize, bei gerosios pasaulinės patirties analize. Modeliui buvo parinkti svarbiausi kibernetinio saugumo metodai, priemonės ir sprendimo būdai užtikrinantys kibernetinį saugumą. Kolektyvinės kibernetinės gynybos tikslas yra suburti kelias organizacijas kartu, o Kolektyvinės kibernetinės apsaugos modelio tikslas sujungti suderinamas kibernetinės apsaugos priemones, metodus ir sprendimo būdus.

Suformulavus išvadas ir papildomai akcentuojant atlikto empyrinio tyrimo rezultatus, galima pateikti tokius **pasiūlymus:**

- diegiant kibernetinio saugumo metodus ir priemones Lietuvoje, bankų veiklos srityje, siūlytina remtis pasaulinio mąsto etalonais stengiantis tarpusavyje sinchronizuotai suderinti šių pasaulio šalių kibernetinio saugumo valdymo gerosios patirties priemones ir metodus: Izraeliu (valstybės bei finansų institucijų tarpusavio bendradarbiavimu kibernetinio saugumo srityje), Šveicarija (greitai kintančiomis techninėmis ypatybėmis), Vokietija (kibernetinio saugumo pajėgomis), Baltijos šalimis (švietimu ir sąmoningumu);
- Pasiūlytas Kolektyvinės kibernetinės apsaugos modelis: kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų suderinamumas bankų veiklos rizikų valdymui (žr. pav. 25) gali būti rekomenduojamas Lietuvos bankų asociacijai kaip įrankis diegiant, kuriant bei stiprinant kibernetinio saugumo sritį.

LITERATŪROS SĄRAŠAS

Vadovėliai ir monografijos:

1. Mačerinskienė ir Baršauskienė, V. (2007). I. *Studijų darbų parengimo tvarka: mokomoji knyga.* Kaunas: Technologija.
2. William A., Carter D. (2019). *Crumpler Financial Sector Cybersecurity Requirements in the Asia-Pacific Region*.
3. Tidikis R. (2003). *Socialinių mokslų tyrimų metodologija*. Vilnius: Lietuvos teisės universiteto leidybos centras.
4. Kardelis K. (2002). *Mokslinių tyrimų metodologija ir metodai 2-asis leidimas*. Šiauliai. Prieiga per internetą: https://www.scribd.com/doc/37948910/K-Kardelis-Mokslini%C5%B3-tyrim%C5%B3-metodologija-ir-metodai
5. Lewis M. (2004). *Radius - Remote AAA Serveris, Trobleshooting Virtual Private Network*s.
6. Mark S. Kadrich. (2007). *Endpoint Security*.
7. Russell R., Medvedev A. (2017). *Eugene Kaspersky: Biography*.
8. Rudzkienė, V. (2005). *Socialinė statistika*, Vilnius.
9. Pilakauskas V. (2011). *Procesų modeliavimas ir nuotolinis valdymas. Mokomoji knyga.* Prieiga per internetą: http://www.esparama.lt/documents/10157/490675/Procesu_modeliavimas.pdf/4dc2f3a3-308f-41ab-a2fb-dcd98d14ef91

Mokslinės literatūros šaltiniai:

10. Limba T., Agafonov K., Damkus M., Paukštė L., Plėta, T. (2017). *Peculiarities of cyber security management in the process of internet voting implementation, Entrepreneurship and Sustainability Issues*.
11. Limba T., Plėta T., Agafonov K., Damkus M. (2017). *Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability Issues*.
12. Štitilis D. (2013). *Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos*.
13. Štitilis D., Laurinaitis M., Paulius Pakutinskas, Inga Malinauskaitė (2017). *Lietuvos kibernetinio saugumo strategijos modelis.* Prieiga per internetą: file:///D:/Users/Ieva/Downloads/Lietuvos_kibernetinio_saugumo_strategijos_modelis(galutinis)%20(1).pdf

14. Kirdeikis E. ir Kaklauskas L. (2015). *Įmonės tinklo saugos užtikrinimas naudojant fortigate ugniasienę*.
15. Žalimaitė M., Baležentis A. (2011). *Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas. Vadybos mokslas ir studijos – kaimo verslų ir jų infrastruktūros plėtrai*.
16. Podvezko V. (2005). *Ekspertų įverčių suderinamumas. Ūkio technologinis ir ekonominis vystymas*.
17. Athira B., Neethu Babu, Soumya Krishnan M. (2017). *An Inspective Mode to Find the Optimum Antivirus App for Defending the Latest Banking TordowInternational Journal of Pure and Applied Mathematics*, Vol.: 114, No. 12, 79-88.
18. Grincevičius R., (2019). *Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose* (daktaro disertacija).
19. Gulevičiūtė G. (2013). *E. verslo kokybinių kriterijų kūrimas ir taikymas: pasaulinė rinkos analizė.* (Magistro baigiamasis darbas, Mykolo Romerio universitetas, darbo vadovas – Limba T.), 2013.
20. Užkuraitytė G. (2013). *Kibernetinio saugumo valdymo užtikrinimas: pasaulinė patirtis ir Lietuvos perspektyva.* (Magistro baigiamasis darbas, Mykolo Romerio universitetas, darbo vadovas – Limba T.), 2015.
21. ANDRIUŠKA G., (2011) *Vartotojų identifikavimo sprendimai panaudojant RADIUS arba TACACS serverį*. (Mokslinis vadovas -AKLAUSKAS L.) Prieiga per internetą: https://www.slk.lt/sites/default/files/profesinis_bakalauras_2011.pdf#page=6
22. Depren O., Topallar M., Anarim E., Kemal Ciliz M. (2005). *An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks*, (p.713-722).
23. Jyh-Cheng Chen; Yu-Ping W. (2005). *Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience*, IEEE Communications Magazine, Vol.: 43 , Issue: 12, Dec.
24. Weeger A., Loose M., Gewald H. (2013). *BYOD – The Next Big Thing in Recruiting? Examining the Determinants of BYOD Service Adoption* Behavior from the Perspective of Future Employees. Prieiga per internetą: https://aisel.aisnet.org/amcis2013/EndUserIS/GeneralPresentations/12/
25. Segal R., Crawford J., Kephart J., Leiba B. (2004). *SpamGuru: An Enterprise Anti-Spam Filtering System.* Prieiga per internetą: http://internetmessagingtechnology.org/pubs/CEAS-2004-SpamGuru-Overview.pdf
26. Frank H. Katz (2009). *WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?*

27. Zehavi R., Trugman U., Drai D., Safruti I. (2012). *System combining a cdn reverse proxy and an edge forward proxy with secure connections,* US Patent App. 13/102,038.
28. Huston G., Ferguson P. (1998). *What is a VPN?* Prieiga per internetą: http://cpham.perso.univ-pau.fr/ENSEIGNEMENT/COMMUN/vpn_ferguson.pdf
29. Waldin R., Nachenberg C. (2000). *Antivirus accelerator for computer networks,* US Patent 6,094,731.
30. Urias W., Stout W., Watson J. L., Grim C., Liebrock L., Merza M. (2017). *Technologies to enable cyber deception*. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/8167793/authors#authors
31. Schreieck M., Finke R., Wiesche M., Krcmar H. (2017). *Sandbox vs. Toolbox–Analysis of Boundary Resources in B2B Software Platforms*. Prieiga per internetą: http://excell-mobility-il17.in.tum.de/wp-content/uploads/2017/11/2017-11-23-Sandbox-vs.-Toolbox.pdf
32. Bajikar S. (2002). *Trusted Platform Module (TPM) based Security on Notebook PCs*. Prieiga per internetą: http://ogobin.de/TCPA/Trusted_Platform_Module_White_Paper.pdf
33. Butrimas V. (2016). *Kenkėjiškos veiklos kibernetinėje erdvėje – grėsmės technologiniams visuomenės pagrindams*. Prieiga per internetą: http://apzvalga.eu/images/kibernetinis_saugumas.pdf
34. Telksnys L. (2016). *Kibernetinis saugumas.* Prieiga per internetą: http://apzvalga.eu/images/kibernetinis_saugumas.pdf
35. Saudargas P. (2016). *Kibernetinių atakų Lietuvoje atvejai ir kaip į juos reaguojama.* Prieiga per internetą: http://apzvalga.eu/images/kibernetinis_saugumas.pdf
36. Algeier S. ir kt. (2018) *Collective Defense: A Collaborative Perspective from the IT Sec.* Prieiga per internetą: https://www.it-scc.org/uploads/4/7/2/3/47232717/the_collective_defense_white_paper_12.19.pdf

Teisės aktai:

37. Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee
38. LR Valstybės saugumo departamento metinė ataskaita (2011). Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2017/03/Veiklos-ataskaita-2012.pdf
39. LR Valstybės saugumo departamento metinė ataskaita (2012). Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2017/03/Veiklos-ataskaita-2012.pdf
40. LR Valstybės saugumo departamento metinė ataskaita (2014). Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2017/03/Veiklos-ataskaita-2012.pdf

41. LR Valstybės saugumo departamento metinė ataskaita (2016). Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2017/03/Veiklos-ataskaita-2012.pdf
42. LR Valstybės saugumo departamento metinė ataskaita (2018). Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2019/06/VSD-2018-ataskaita.pdf
43. LR Nacionalinio saugumo pagrindų įstatymas (1996). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/vDAPGooxLN
44. LR Nacionalinio saugumo pagrindų įstatymas (1996). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/vDAPGooxLN
45. LR Nacionalinio saugumo strategija, pranešimas žiniasklaidai (2017). Prieiga per internetą: http://www.lrs.lt/sip/portal.show?p_r=25318&p_k=1&p_t=168480
46. LR Nacionalinio saugumo strategija (2002). Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.2627131DA3D2/LLwfQepmnD
47. NKSC būklės ataskaita (2020). Prieiga per internetą: https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf

Kita:

48. *Kibernetinio saugumo valdymas.* Prieiga per internetą: https://www.mruni.eu/lt/universitetas/fakultetai/ekonomikos_fakultetas/studijos/magistranturos-studijos/kibernetinio-saugumo-valdymas/ [Žiūrėta 2018-11-08].
49. *NKSC: Ypač svarbios efektyviai kibernetinei gynybai saugumo kontrolės priemonės.* Prieiga per internetą: https://www.nksc.lt/doc/NKSC%20plakatas%20(20cc)_1.pdf [Žiūrėta 2019-04-10].
50. *Ugniasienė.* Prieiga per internetą: https://searchsecurity.techtarget.com/definition/firewall [Žiūrėta 2019-04-10].
51. *Duomenų kopijos*. Prieiga per internetą: https://www.nksc.lt/doc/biuleteniai/2018-05-11%20NKSC%20saugumo%20atmintine%20keliaujantiems.pdf [Žiūrėta 2019-05-10].
52. Bloomberg. (2016). *How $81 Million Slipped Through Philippine Cracks: Timeline.* Prieiga per internetą: https://www.bloomberg.com/news/articles/2016-03-20/how-81-million-slipped-through-philippine-cracks-timeline [Žiūrėta 2019-05-10].
53. Swedbank. *„Smart-ID“ naudotojo atmintinė.* Prieiga per internetą: https://www.swedbank.lt/private/home/more/security?language=LIT [Žiūrėta 2020.01.15]
54. *„Smart-ID“ programa išmaniajame įrenginyje*. Prieiga per internetą: https://www.smart-id.com/lt/pagalba/duk/registracija/kaip-uzregistruoti-smart-id-paskyra-naudojant-asmens-tapatybes-kortele/ [Žiūrėta 2020.01.15]

55. Oficialiosios statistikos portalas. *Informacinių technologijų naudojimas namų ūkiuose.* Prieiga per internetą: https://osp.stat.gov.lt/naujienos?articleId=5808689 [žiūrėta 2020.01.15]
56. *Duomenų kopijos*. Prieiga per internetą: http://www.kompservis.lt/atsargines-kopijos-ir-duomenu-atstatymas/ [žiūrėta 2020.01.15]
57. *Antivirusinės programos.* Prieiga per internetą: http://acadpubl.eu/jsi/2017-114-7-ICPCIT-2017/articles/12/9.pdf [žiūrėta 2020.02.26]
58. *Nepriklausomų testų / apžvalgų skaičius*. Prieiga per internetą: https://www.kaspersky.com/top3 [žiūrėta 2020.02.26]
59. *„Smart-ID" naudojimas*. Prieiga per internetą: https://www.smart-id.com/lt/pagalba/duk/registracija/kaip-uzregistruoti-smart-id-paskyra-naudojant-asmens-tapatybes-kortele/ [žiūrėta 2020.01.15]
60. *Swedbank bankas*. Prieiga per internetą: https://www.swedbank.lt/private/home/more/security?language=LIT [žiūrėta 2020.01.15]
61. *Kinijos bankas*. Prieiga per internetą: https://www.bochk.com/en/security/2factorauthentication.html, [žiūrėta 2020.02.26]
62. *Bank of America*. Prieiga per internetą: https://www.pbs.org/wgbh/theymadeamerica/whomade/giannini_hi.html [žiūrėta 2020.01.13]
63. *The CIS Critical Security Controls for Effectice Cyber Defence*, Prieiga per internetą: https://www.us-cert.gov/bsi, [žiūrėta 2020.02.26]
64. *Report of Bank of China*, Prieiga per internetą: https://pic.bankofchina.com/bocappd/report/201106/P020110620680809691168.pdf [žiūrėta 2020.02.26]
65. *Web Application Firewall*, Prieiga per internetą: https://owasp.org/www-community/Web_Application_Firewall
66. *Komutatorius*. Prieiga per internetą: https://www.cisco.com/c/en/us/solutions/smallbusiness/resourcecenter/networking/network-switch-vs-router.html
67. *Avast Antivirus*. Prieiga per internetą: https://www.avast.com/en-eu/index#pc
68. *AVG Antivirus.* Prieiga per internetą: https://www.avg.com/en-us/homepage#pc
69. *Avira Antivirus.* Prieiga per internetą: https://antivirus.avira.com/en/acq/bundles/antivirus-optimization-prime-src-2?x-cchannel=SEM&xasource=Media&xamedium=SEM&xanetwork=Search&gclid=EAIaIQobChMIisWtKeN6AIVw8YYCh0G4wCtEAAYASAAEgISyPD_BwE
70. *Comodo Antivirus.* Prieiga per internetą:

https://www.comodo.com/home/internet-security/updates/vdp/database.php

71. US Senate. (1978). *Select Committee on Intelligence, 'Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard', Staff Report.* Prieiga per internetą: http://intelligence.senate.gov/pdfs/95nsa.pdf
72. BDO. (2017). *Cyber security in banking industry.* Prieiga per internetą: http://www.bdo.in/getmedia/b478e1ec-a9a3-4afe-997a-3aed7d190164/Cyber-Security-in-banking-industry.pdf.aspx?ext=.pdf&disposition=attachmen
73. Gyarmathy K. (2019). *Top Cybersecurity Problems and Solutions*. Prieiga per internetą: https://www.vxchnge.com/blog/cybersecurity-problems-and-solutions
74. *Bitdefender Antivirus Bitdefender mobile security and antivirus, User's guide*. Prieiga per internetą:https://books.google.lt/books?id=Dx1QDQAAQBAJ&pg=PA24&dq=Bitdefender+Antivirus&hl=lt&sa=X&ved=0ahUKEwj_gOqyp43oAhVUwsQBHUbfCxYQ6AEIJzAA#v=onepage&q=Bitdefender%20Antivirus&f=false
75. Jegelavičiūtė R. (2017). *Lyginamojo metodo pataisos kriterijų įtaka nekilnojamojo turto vertei.* Prieiga per internetą:http://lituka.com/wp-content/uploads/2017/03/ISSN-2424-3809-Nr-2-2017-03a.pdf
76. *„Smart-ID" naudotojų Lietuvoje – daugiau kaip 1 milijonas* (2020). Prieiga per internetą: https://www.lba.lt/lt/asociacijos-naujienos/2019/-smart-id-naudotoju-lietuvoje-daugiau-kaip-1-milijonas
77. Paulauskas A. (2016). *NSGK pirmininkas A.Paulauskas ragina pasirūpinti kibernetine gynyba.* Prieiga per internetą: https://www.respublika.lt/lt/naujienos/lietuva/lietuvos_politika/nsgk_pirmininkas_apaulauskas_ragina_pasirupinti_kibernetine_gynyba/,print.1
78. Wai O. (2019). *What a „Collective Defence" model can do for Cybersecurity"* Prieiga per internetą: https://ironnet.com/blog/what-a-collective-defense-model-can-do-for-cybersecurity/
79. Grasshoff G., Bohmayr W. ir kt. (2018). *Banking's Cybersecurity Blind Spot—and How to Fix It.* Prieiga per internetą: https://www.bcg.com/publications/2018/banking-cybersecurity-blind-spot-how-to-fix-it.aspx
80. *„Smart-ID" technical overview* (2019). Prieiga per internetą: https://github.com/SK-EID/smart-id-documentation/wiki/Technical-overview#smart-id-solution-components
81. Ambrasas T., *Kibernetinis ir duomenų saugumas – svarbiausias prioritetas finansų paslaugų rinkoje?* (2019). Prieiga per internetą: https://www.aaalaw.eu/lt/naujienos/kibernetinis-ir-duomenu-saugumas-svarbiausias-prioritetas-finansiniu-paslaugu-rinkoje/

Lelešienė L. Kibernetinio saugumo priemonių ir metodų bankų veiklos rizikų valdymui/ Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas Prof. dr. T. Limba. – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir verslo fakultetas, 2020. – 77 p.

ANOTACIJA

Magistro darbe buvo analizuojami kibernetinio saugumo taikymo teoriniai aspektai, kibernetinio saugumo metodai ir priemonės bankų veiklos rizikų valdymui pasaulio ir Baltijos šalyse. Buvo atliktas kokybinis tyrimas ir pateikta kibernetinio saugumo metodų ir priemonių bankų veiklos rizikų valdymui tyrimo rezultatai. Pirmame skyriuje analizuojami kibernetinio saugumo teoriniai aspektai: kibernetinio saugumo sąvoka ir raidos tendencijos, kibernetinio saugumo metodų ir priemonių analizė, kibernetinio saugumo metodų ir priemonių problematika ir sprendimo būdai. Antrame skyriuje nagrinėjama kibernetinio saugumo metodų ir priemonių taikymo pasaulinė analizė: JAV, Kinijos ir Baltijos šalių (Estijos ir Lietuvos) šalių kibenetinio saugumo metodų ir priemonių bankų veiklos rizikų valdymui atvejai. Trečiame skyriuje analizuojamas kokybinis tyrimas, kurio tikslas - pasitelkiant ekspertų žinias, išsiaiškinti kibernetinio saugumo bankų veiklos rizikų valdymui pagrindines problemas, atsirandančias diegiant kibernetinio saugumo priemones, išskirti pagrindinius kibernetinio saugumo metodų ir priemonių pavyzdžius. Ketvirtame skyriuje yra sukurtas Kolektyvinės kibernetinės apsaugos modelis: kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų suderinamumas.

Pagrindiniai žodžiai: kibernetinis saugumas, kibernetinio saugumo metodai, kibernetinio saugumo priemonės, kibernetinio saugumo metodų ir priemonių taikymas, kibernetinio saugumo modelis

Lelešienė L. Cyber Security Measures and Methods for Management of Banking Operational Risks/ Master's Thesis on Cyber Security Management. Supervisor Prof. Dr. T. Limba. – Vilnius: Mykolas Romeris University, Faculty of Economics and Business, 2020. – 77 p.

ANNOTATION

In master's thesis, after an introduction of theoretical aspects of cyber security application, analysis of cyber security methods and measures for management of banking operational risks throughout the world and in Lithuania, and after a qualitative study, a concept of cyber security and results of the study were presented. Primarily, the first part of thesis reviews theoretical aspects of cyber security, namely, a concept of cyber security and its development tendencies, analysis of cyber security methods and measures, problematicity and solutions of cyber security methods and measures. Further, the second part examines the global analysis of application of cyber security methods and measures: cases of the United States of America, China and the Baltic States (Estonia and Lithuania), regarding cyber security methods and measures for management of banking operational risks. The third part of thesis analyses a study carried out, whose aim is to find out, by using the expert knowledge, the main issues of cyber security in management of banking operational risks, arising when implementing cyber security measures, as well as to accentuate the major examples of cyber security methods and measures. A collective cyber security model is created in the fourth chapter: compatibility between collective cyber security measures, methods and ways of solution.

Key words: cyber security, cyber security methods, cyber security measures, application of cyber security methods and measures, cyber security model

Lelešienė L. Kibernetinio saugumo priemonių ir metodų bankų veiklos rizikų valdymui/ Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas Prof. dr. T. Limba. – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir verslo fakultetas, 2020. – 77 p.

SANTRAUKA

Magistro baigiamojo darbo tikslas - remiantis pasauline analize išanalizuoti kibernetinio saugumo metodus ir priemones bankų veiklos rizikų valdymui ir išanalizuoti kibernetinio saugumo teorinius aspektus.

Buvo atlikta mokslinė literatūros analizė kibernetinio saugumo srityje. Septyni kibernetnio saugumo ekspertai buvo apklausti kokybinio tyrimo metu. Ekspertų nuomonę siekiama sužinoti standartizuoto interviu arba klausimyno forma. Mokslinės literatūros analizė atlikta tam, kad galima būtų išanalizuoti kibernetinio saugumo priemonių ir metodų teorinius aspektus. Tyrimu siekta išsiaiškinti kibernetinio saugumo priemonių ir metodų taikymo bankų veiklos rizikų valdymo pagrindines problemas, išskirti populiariausias kibernetinio saugumo priemonių ir metodų pavyzdžius.

Keturios dalys sudaro baigiamąjį darbą: pirmoje dalyje analizuojamos kibernetinio saugumo priemonės ir metodai diegimo rizikų valdymui teoriniai aspektai: kibernetinio saugumo priemonių ir metodų savokos ir raidos analizė, kibernetinio saugumo priemonės ir metodai, kibernetinio saugumo priemonių ir metodų diegimo bankų veiklos rizikų valdymui problematika. Antroje dalyje analizuojama kibernetinio saugumo priemonių ir metodų taikymo bankų veiklos rizikų valdymui pasaulio patirties analizė. Trečioje dalyje analizuojamas atliktas kokybinis tyrimas, kuris - pasitelkiant ekspertų žinias, padeėjo išsiaiškinti kibernetinio saugumo priemones ir metodus naudojamus bankuose; pagrindines sąvokas ir problemas, atsirandančias diegiant kibernetinio saugumo priemones ir metodus; išskirti populiariausius kibernetinio saugumo priemonių ir metodų pavyzdžius. Ketvirtoje dalyje buvo sukurtas Kolektyvinės kibernetinės apsaugos modelis: kolektyvinės kibernetinės apsaugos priemonių, metodų ir sprendimo būdų suderinamumas. Darbo pabaigoje pateikiamos išvados ir rekomendacijos.

Lelešienė L. Cyber Security Measures and Methods for Management of Banking Operational Risks/ Master's Thesis on Cyber Security Management. Supervisor Prof. Dr. T. Limba. – Vilnius: Mykolas Romeris University, Faculty of Economics and Business, 2020. – 77 p.

SUMMARY

To begin with, the aim of the master's thesis is to analyse cyber security methods and measures for management of banking operational risks on the basis of global analysis. Also, it aims at analysing the theoretical aspects of cyber security.

In the master's thesis, a scientific literature review in the field of cyber security was carried out. Moreover, a qualitative study on the views of experts was conducted, during which 7 experts were interviewed. Opinion of experts was sought to be known through the form of standardized interview or questionnaire. In order to survey the theoretical aspects of cyber security methods and measures, a scientific literature review was applied in the thesis. The study pursued to reveal the main issues of application of cyber security methods and measures for management of banking operational risks, distinguish the most popular examples of cyber security methods and measures.

Furthermore, the master's thesis consists of three parts. The first part of thesis looks over the theoretical aspects of the cyber security measures and methods for managing implementation risks: concepts of cyber security measures and methods and their development tendencies, cyber security methods and measures, problematicity of implementing cyber security methods and measures for management of banking operational risks. The second part provides an analysis of the worldwide experience on applying cyber security measures and methods for management of banking operational risks. The third part examines a study carried out, which seeks to find out cyber security methods and measures used in banks, by invoking knowledge of experts; identify the main concepts and issues arising out of implementation of cyber security measures and methods; distinguish the most popular examples of cyber security methods and measures. A collective cyber security model is created in the fourth chapter: compatibility between collective cyber security measures, methods and ways of solution. Finally, conclusions and recommendations are provided at the end of this thesis.

Forma patvirtinta

Mykolo Romerio universiteto

Senato 2016 m. gegužės 9 d. nutarimu Nr. 1SN-44

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2020-04-21
Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

Ekonomikos ir verslo fakulteto, Kibernetinio saugumo valdymo programos
(fakulteto / instituto, programos pavadinimas)

studentė Lina Lelešienė,
(vardas, pavardė)

patvirtinu, kad šis magistro baigiamasis darbas

„Kibernetinio saugumo priemonės ir metodai bankų veiklos rizikų valdymui“
(*baigiamojo darbo pavadinimas*):

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už šiurkštų akademinės etikos pažeidimą.