MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

INDRĖ DAUBARAITĖ

ASMENS TAPATYBĖS NUSTATYMAS INTERNETE: GRĖSMĖS PINIGŲ PLOVIMO RĖŽIMUI

Magistro baigiamasis darbas

Vadovas

Doc. Dr. Marius Laurinaitis

Vilnius, 2023

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

ASMENS TAPATYBĖS NUSTATYMAS INTERNETE: GRĖSMĖS PINIGŲ PLOVIMO RĖŽIMUI

Kibernetinio saugumo valdymo magistro baigiamasis darbas
Studijų programa 6211LX066

Vadovas

Doc. Dr. Marius Laurinaitis

2023 04 ...

Atliko

I. Daubaraitė KSVvmis20-1 stud.

2023 04 ...

Vilnius, 2023

1. TURINYS

LENTELĖS

PAVEIKSLAI

SANTRUMPŲ SĄRAŠAS

FNTT – Finansinių nusikaltimų tyrimo tarnyba

RRT – Ryšių reguliavimo tarnyba

LR – Lietuvos Respublika

PPTFPĮ - Pinigų plovimo ir teroristų finansavimo prevencijos įstatymo

eIDAS – 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EC.

CDD (angl. Csutomer De dilligence) - Deramas kliento tikrinimas

HTTPS (angl. HyperText Transfer Protocol Secure) - Hiperteksto perdavimo protokolas

HTTP (angl. HyperText Transfer Protocol – Saugus Hiperteksto perdavimo protokolas

HSM (angl. Hardware security model) - aparatinis saugumo modelis

TLS ((angl. Transport Layer Security) - transporto sluoksnio saugumas

SSL (angl. Secure Sockets Layer) – saugaus lizdo sluoksnis

ECPSA (angl. Elliptic Curve Digital Signature Algorithm) - elipsinės kreivės skaitmeninio parašo algoritmas

RSA (angl. Rivest-Shamir-Adleman) - viešojo rakto kriptosistema

RASP (angl. Runtime Application Self-Protection) - Vykdymo laiko programų savisauga Technologija

FAFT (angl. Financial Action Task Force) - Finansinių veiksmų darbo grupės

AML (angl. Anti Money Laundering) pinigų plovimo prevencija

ĮVADAS

Darbo aktualumas. Elektroninė erdvė yra neatsiejama kiekvienos dali, ir vertinant ją finansinių paslaugų atžvilgiu reikšmė tik didėja. Elektroninės bankininkystės atsiradimas davė postūmį mažinti operacijas su grynaisiais pinigais, o elektroninių pinigų įstaigų atėjimas į rinką dar labiau sumažino atsiskaitymus grynaisiais pinigais. Šis būdas buvo pakeistas atsiskaitymą be kontaktinėmis kortelėmis, telefonais, išmaniaisiais laikrodžiais ir t.t. Kartu su besikeičiančiais vartotojų poreikiais, turėjo keistis ir finansinės institucijos bei plėstis elektroninė bankininkystė. Lietuvoje veikiantys bankai pradėjo siūlyti siūlyti sąskaitų atidarymą internetu (privačių konsultacijų metu), tuo tarpu elektroninių pinigų įstaigose sąskaitą galima atsidaryti vos keliais paspaudimais. Beveik visi Lietuvoje veikiantys bankai ir elektroninių pinigų įstaigos turi savo mobiliąsias programėles, kurių pagalba galima prisijungti prie savo sąskaitos akimirksniu. Tačiau siekis maksimaliai viską supaprastinti vartotojui, kelia ir tam tikrų iššūkių – klientui prisijungti prie sąskaitos paprasčiau, tačiau lygiai taip pat padidėja rizikos susijusios su tapatybės nustatymų ir paskyrų autentifikavimu internete. Netinkamas vartotojo tapatybės nustatymas internete kelia grėsmes pinigų plovimo rėžimui. Tarptautinės organizacijos (e.g.: „Financial Action Task Force“), Europos sąjungos institucijos ir Lietuvoje veikiančios institucijos tobulina esamus įstatymus ir gaires siekiant padėti finansinėms institucijoms suvaldyti kylančias rizikas. Tuo tarpu bankai ir elektroninių pinigų įstaigos pastoviai investuoja į priemones padedančia saugiai/ tinkamai nustatyti kliento tapatybę nuotoliniu būdu. Nepaisant visų dedamų pastangų, naudojamose sistemose/ metoduose, nustatyti kliento tapatybę jam gyvai nedalyvaujant, galima aptikti pažeidžiamumų, kurie sustiprina rizikas susijusias su pinigų plovimu. Todėl labai svarbu išanalizuoti esamą situaciją ir atlikti tolimesnius tyrimus siekiant įvertinti ar Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų naudojami tapatybės nustatymo internete būdai maksimaliai sumažina minėtas grėsmes

Darbo problema. Kaip suvaldyti asmens tapatybės internete nustatymo keliamas grėsmes pinigų plovimo rėžimui?

Darbo objektas. Asmens tapatybės nustatymo internete metodai

Darbo dalykas. Asmens tapatybės nustatymo internete metodai Lietuvos bankuose ir elektroninių pinigų įstaigose

Darbo tikslas. Atskleisti Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų naudojamus metodus asmens tapatybės nustatymui bei įvertinti jų keliamas grėsmės pinigų plovimo prevencijos rėžimui

Darbo uždaviniai:

1. Nustatyti bankuose ir elektroninių pinigų įstaigose naudojamus asmens tapatybės nustatymo metodus internete
2. Atlikti naudojamų tapatybės nustatymo internete metodų ir paskyrų autentifikavimo būdų veiksmingumo analizę ir išskirti aukščiausius standartus atitinkančias priemones

3. Ištirti pagrindines pinigų plovimo prevencijai grėsmes kylančias iš neteisėtos sąskaitos atsidarymo/ naudojimo
4. Įvertinti Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų naudojamų tapatybės nustatymo internete būdų patikimumą bei išanalizuoti jų keliamas grėsmes pinigų plovimo prevencijos rėžimui
5. Pasiūlyti tapatybės nustatymo internete ir paskyros autentifikavimo metodą, kuris Lietuvoje padėtų sumažinti grėsmes pinigų plovimo prevencijos rėžimui.

Duomenų rinkimo ir analizės metodai:

1. Mokslinės literatūros analizė.
2. Dokumentų analizė;
3. Statistinių duomenų analizės metodas
4. Lyginamoji duomenų analizė.
5. Atvejo analizė
6. *Teisės aktų analizė*
7. Oficialiuose finansinių įstaigų/ institucijų puslapiuose pateiktos informacijos analizė

Darbo struktūra

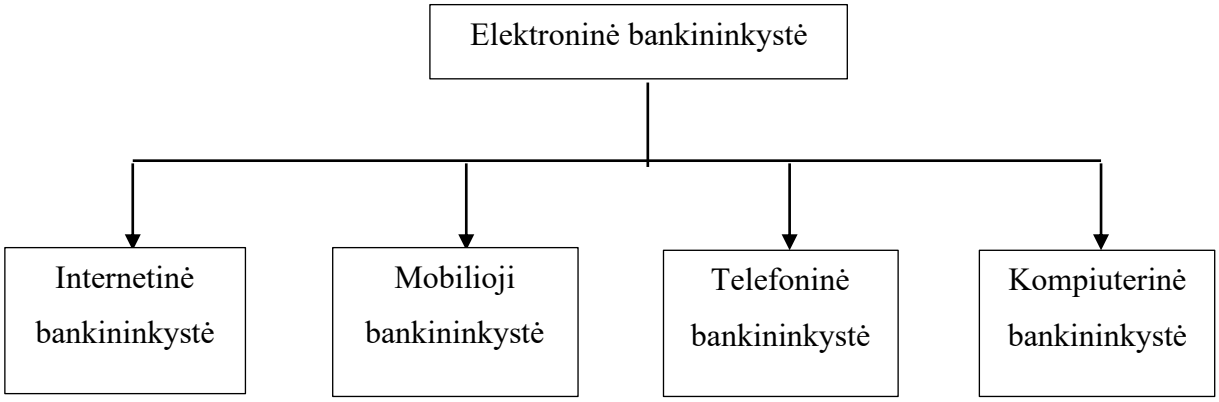
Magistro darbą sudaro keturios dalys. Magistro baigiamajame darbe analizuojamos asmens tapatybės nustatymo internete ir paskyrų autentifikavimo priemonės, bei jų keliamos rizikos pinigų plovimo prevencijos rėžimui. Atlikta lyginamoji analizė parodė, kad Lietuvoje finansinių institucijų naudojamos priemonės kelia tas pačias rizikas pinigų plovimo rėžimui, kai ir užsienyje. Pirmoje darbo dalyje nagrinėjama elektroninės bankininkystės rūšys, kliento tapatybės nustatymo internete ir vartotojo paskyros autentifikavimo būdai. Antroje dalyje analizuojamas finansinių įstaigų naudojamų, tapatybės nustatymo internete ir paskyros autentifikavimo būdai. Pateikiam atvejo analizė analizuojant Danijos karalystės, Jungtinės Karalystės bankų ir ne Lietuvoje registruotų elektroninių pinigų įstaigų naudojamų būdų patikimumą. Trečioje dalyje nagrinėjamos, asmens tapatybės internete ir paskyrų autentifikavimo būdų, keliamos grėsmės pinigų plovimo prevencijos rėžimui. Ketvirtoje dalyje atliekamas tyrimas išsiaiškinti Lietuvoje veikiančių finansinių įstaigų naudojamų, tapatybės nustatymo internete ir paskyrų autentifikavimo būdų, grėsmės pinigų plovimo rėžimui. Tyrime išvadose yra pasiūlomas saugiausias iš nagrinėtų būdų kuris galėtų būti pritaikytas Lietuvoje

1. ELEKTRONINĖ BANKININKYSTĖ

1.1. Elektroninės bankininkystės rūšys

Internetinė bankininkystė pasaulyje pradėta naudoti nuo 1995 m., o Lietuvoje ši paslauga pradėta tiekti nuo 2000 m. Pirmasis internetinės bankininkystės paslaugą pristatė AB bankas „Snoras“, tačiau kiti Lietuvoje veikiantys bankai (pvz.: Šiaulių bankas, Swedbank) pasekė tuo pačiu keliu ir įsidiegė sistemas reikalingas teikti internetinės bankininkystės paslaugas. Technologijoms sparčiai vystantis ir nuolat tobulėjant, elektroninė bankininkystė šiuolaikiniam pasaulyje tapo neatsiejamo daugumos gyventoju gyvenimo dalis. Pavyzdžiui, remiantis Lietuvos bankų asociacijos (2022) užsakytu tyrimu, elektronine bankininkyste Lietuvoje naudojasi 90 proc. šalies gyventojų.

Nagrinėjant bankų teikimas paslaugas internetu svarbu suprasti kas yra elektroninė bankininkystė. Remiantis įvairiais šaltiniais (T. Parker ir M. Parker 2008, L. Sodžiūtė ir V. Sūdžius 2006) elektroninę bankininkystė galima išskirti į keturias pagrindines rūšis (žr. 2 pav.). Verta pažymėti, kad LR ryšių reguliavimo tarnyba (toliau RRT) (2023) išskiria mokėjimo korteles kaip elektroninės bankininkystės paslaugą/ sritį, tačiau dauguma kitų autorių (pvz. L. Sodžiūtė ir V. Sūdžius 2006) mokėjimo korteles priskiria prie elektroninių atsiskaitymų. Įvertinus tai, kad RRT apibrėžia mokėjimo korteles kaip atsiskaitymo negrynaisiais pinigais priemonę, mokėjimo kortelės šiame darbe nebus priskiriamos prie elektroninės bankininkystės sričių.



1 pav. Elektroninės bankininkystės rūšys

Šaltinis: sudaryta autorės remiantis T. Parker ir M. Parker 2008, L. Sodžiūtė ir V. Sūdžius 2006

Internetinę bankininkystę galima apibrėžti kaip banko paslaugų teikimą internetu, naudojantis specialiai tam sukurtu tinklapiu (LR ryšių reguliavimo tarnyba, 2023). Dažnai internetinė bankininkystė gali būti maišoma su kompiuterine bankininkyste, tačiau šių sąvokų nereikėtų tapatinti. Internetinei

bankininkystei reikalinga tik prieiga prie interneto, o tuo tarpu kompiuterinei bankininkystei reikia dar ir papildomų kompiuterinių programų.

Mobilioji bankininkystė dažniausiai siejama su mobiliojo ryšio priemonėmis/ išmaniaisiais telefonais kurių pagalba galima kontroliuoti savo sąskaitą it atlikti įvairias operacijas. Pastarąjį dešimtmetį mobilioji bankininkystė sparčiai augo, pvz. 2016 m. Swed Bankas pranešė apie rekordinį mobiliosios bankininkystės šuolį, nes išmaniosios banko programėlės naudotojų skaičius augo 83 proc. Įvertinus mobiliosios bankininkystės augimą galima teigti, kad ši sritis yra viena iš populiariausių, tačiau nereiktų pamiršti, kad finansinių įstaigų teikiamos paslaugos per programėlę gali skirtis nuo teikiamų paslaugų per internetinę bankininkystę (Paysera 2022).

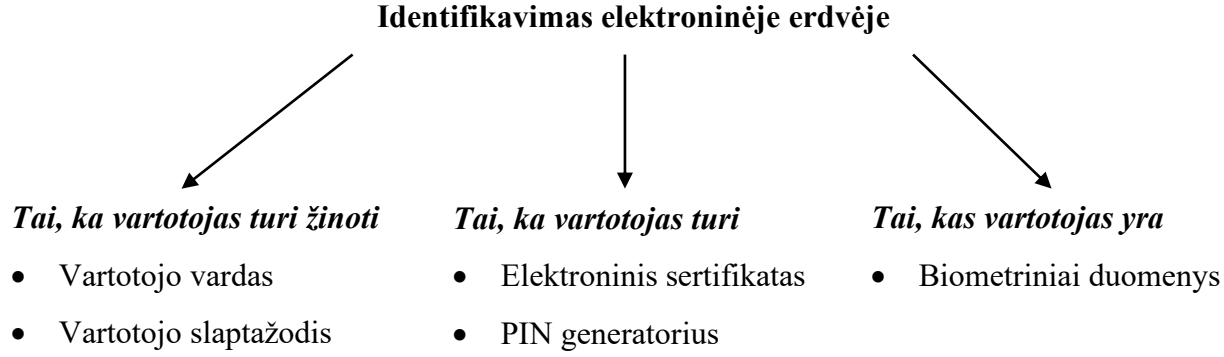
Telefoninė bankininkystė tai banko paslaugų teikimas telefonu. Galima išskirti dvi šios bankininkystės rūšis: automatizuotos paslaugos (bendraujama su automatu, kuris valdomas telefono mygtukais) ir banko specialisto paslaugos (LR ryšių reguliavimo tarnyba, 2023). Dauguma paslaugų teikiamų per telefoninę bankininkystę galima gauti kitais būdais (internetinė ir/ ar mobilioji bankininkystė), tačiau tam tikrais atvejais telefoninė bankininkystė gali būti vienintelė alternatyva. Pvz. praradus bankinę kortelę ir neturint galimybės jos užblokuoti interneto banke ar išmanioje programėlėje, su finansine institucija galima susiekti telefonu ir užblokuoti prarastą mokėjimo kortelę. Pažymėtina, kad finansinės institucijos šią funkciją stengiasi automatizuoti (pvz. Revolut nurodytas numeris yra automatizuotas). Atsižvelgiant į tai, kad telefoninė bankininkystė nėra laikoma pagrindine/ populiariausi elektroninės bankininkystės rūšimi, ji nebus plačiau analizuojama tolimesniuose šio darbo etapuose.

Kompiuterinė bankininkystė yra apibrėžiama kaip elektroninės bankininkystės rūšis, kai veiksmai (sąskaitos likučio stebėjimas, kitos finansinės operacijos) yra atliekami naudojant asmeninį kompiuterį su specialia kompiuterine programa ir slaptažodžiais (L. Hitt ir F. Frances, 2002). Seniau ši rūšis buvo paplitusi tarp verslo klientų (reikalingas intranetas), tačiau šiuo metu ji yra naudojama vis rečiau dėl atsiradusios patogesnės alternatyvos, t. y. internetinės bankininkystės. Dėl šios priežasties kompiuterinė bankininkystė nebus plačiau nagrinėjama.

Įvertinus pagrindines elektroninės bankininkystės rūšis galima teigti, kad jos suteikia platesnes galimybes vartotojui naudotis banko teikiamomis paslaugomis. Didesnis paslaugų prieinamumas turi įtakos kliento pasitenkinimui, tačiau būtina įvertinti su tuo susijusias rizikas ir kylančia grėsmes. Viena iš pagrindinių rizikų susijusi su elektronine bankininkyste yra kliento tapatybės nustatymas.

1.2. Kliento tapatybės nustatymas internete

Prieš atsirandant elektroniniai bankininkystei norint atsidaryti sąskaitą finansinėje įstaigoje reikėdavo atvykti į padalinį ir pateikti asmens tapatybės dokumentą. Tačiau finansinėms įstaigoms pradėjus teigti paslaugas per elektroninę bankininkystę kliento identifikavimas ir jo tapatybės nustatymas buvo perkeltas į internetą. Žmogaus identifikavimas elektroninėje erdvėje pasižymi tuo, kad jis nėra susietas su konkrečia vieta ir jo identifikavimas yra nepriklausomas nuo geografinės vietos. Asmens identifikavimas elektroninėje erdvėje yra vykdomas pagal tris pagrindinius elementus. Remianti literatūra (Štitilis, Pakutinskas, Laurinaitis ir Dauparaitė, 2011; FATF 2020) ir žemiau pateikta lentele



2 pav. Identifikavimas elektroninėje erdvėje

Šaltinis: sudaryta autorės remiantis Štitilis, Pakutinskas, Laurinaitis ir Dauparaitė, 2011

(2 pav.) identifikavimas elektroninėje erdvėje yra skirstomas į tris dalis: tai, ka vartotojas turi žinoti, ką turi ir kas yra. Vartotojo vardas ir slaptažodis yra naudojami kaip atpažinimo priemonė siekiant prisijungti prie elektroninio pašto, socialinių tinklų, elektroninio pašto ir pan. Šio metodo saugumas priklauso nuo informacinės sistemos, kuria yra naudojamasi, patikimo/ saugumo lygio. Biometriniai duomenys yra suprantami kaip tai, kas vartotojas yra, nes biometriniai tapatybės elementai identifikuoja asmenį pagal jo turimas fiziologines arba elgesio charakteristikas. Elektroninėje bankininkystėje dažniausiai yra vartojami veido atvaizdas ir pirštų antspaudai, tačiau galima būtų svarstytu kitus metodus (akies tinklainės/ rainelės skanavimas, rankos geometrija ir pan.) Elektroninės bankininkystės kontekste „ką vartotojas turi“ yra elektroninės bankininkystės atpažinimo priemonės (pvz. kodų generatoriai), elektroninėje erdvėje pripažįstami dokumentai (pvz. asmens tapatybės kortelė) ir kiti duomenys (pvz. banko išduotos kortelės). Šios priemonės yra reguliuojamos valstybės/ tarptautinių institucijų ir turi atitikti įstatymų numatytas normas/ saugumo reikalavimus, dėl to, kas galima laikyti patikimomis.

Pagal Bazelio bankų priežiūros komiteto (angl. Basel Committee on Banking Supervision) paskelbtus Pagrindinius bankininkystės principus (2012) 29 principas numato, kad bankų priežiūros institucija turi užtikrinti, kad bankai/ elektroninių pinigų institucijos turi tinkamus vidinius procesus tarp

kurių yra griežtos išsamaus patikrinimo (angl. customer due diligence, CDD) taisyklės. Taip pat Finansinių veiksmų darbo grupės (angl. Financial Action Task Force, FATF) rekomendacijos (2012, atnaujintos 2023) nurodo, kad finansinės institucijos nustatyti ir patikrinti kliento tapatybę naudojantis patikimais dokumentais/ informacija. Tam, kad kliento tapatybės nustatymas atitiktų Lietuvos Respublikos keliamus standartus, reikalavimai šiam procesui yra nurodyti Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo (toliau PPTFPĮ) 11 str. Remiantis minėtu įstatymu kliento tapatybė gali būti nustatyta klientui fiziškai nedalyvaujant tik ***penkiais atvejais***.

(1) Trečiųjų šalių informacija apie klientą

Kliento tapatybė gali būti nustatoma jam fiziškai nedalyvaujant, naudojantis kitų subjektu/ trečiųjų šalių informacija. Verta pažymėti, kad trečioji šalis turi atitikti PPTFPĮ 13 str. keliamus reikalavimus, kurie pagrindine yra susiję su duomenų teikimu. Finansų įstaigai paprašius trečioji šalis nedelsiant turi pateikti visą prašomą informaciją ir dokumentus susijusius su kliento tapatybės nustatymu. Ne viena institucija nurodo tokią galimybę savo vidiniuose dokumentuose tvarkose (pvz. UAB , „Profitus“ Pinigų plovimo ir teroristų finansavimo prevencijos tvarka), tačiau reikia įvertinti ir tai, kad trečioji šalis gali nesutikti pateikti reikalaujamus duomenis dėl įvairių priežasčių (trūkstamų sutarčių teikti duomenis, baiminantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pažeidimo). Praktikoje galima aptikti susijusių pavyzdžių – teismo byloje (V. D. v institucija, 2017) kaltinamasis buvo pripažintas kaltu pažeidęs PPTFPĮ 13 str. 1 dalį dėl netinkamo klientų tapatybės nustatymo remiantis trečiųjų šalių informacija. Šis pavyzdys parodo, norint atitikti PPTFPĮ 13 str. keliamus reikalavimus reikalingas trečiųjų šalių bendradarbiavimas. Finansinės institucijos turėtų tai įvertinti ir pasirinkti šį būdą, tik tuo atveju jei gali užtikrinti keliamus reikalavimus.

(2) Europos Sąjungoje išduotos elektroninės atpažinties priemonės

Kliento tapatybę nuotoliniu būdu galima nustatyti naudojant Europos Sąjungoje (toliau ES) išduotas aukšto arba pakankamo saugumo užtikrinimo lygio elektroninės atpažinties priemones, veikiančias pagal schemas nustatytas ES reglamente Nr. 910/2014 (žinomu kaip eIDAS). Kaip viena iš pavyzdžių galiam paimti elektroninėje erdvėje pažengusią Baltijos šalį – Estijos Respubliką. Remiantis ES oficialiame leidinyje pateiktu sąrašu, nuo 2018 m. šešios Estijos elektroninės atpažinties priemonės (asmens tapatybės kortelė, „Digi-ID“, „e-Residency Digi-ID“, „Mobiil-ID“, diplomatinė asmens tapatybės kortelė) yra pripažįstamos ES ir atitinka minėtame reglamente nustatytus reikalavimus. Verta pažymėti, kad Estija šiuo atžvilgiu yra labiau pažengusi, nes nuo 2020 m. tik viena atpažinties priemonių naudojamų Lietuvoje (nacionalinė asmens tapatybės kortelė) yra pripažįstama ES.

(3) Kvalifikuotas elektroninis parašas

Elektroninis parašas laikomas kvalifikuotu, jei jis atitinka saugumo reikalavimus pateiktus eIDAS reglamente ir yra sukurtas kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų. Lietuvoje tokias paslaugas gali teikti Asmens dokumentų išrašymo centras prie LR vidaus reikalų ministerijos, Registrų centras ir Estijos įmonė „SK ID Solutions AS“ (platinami kartu su Smart-ID arba tam tikrų operatorių SIM kortelėmis). Pastebima, kad kvalifikuotas elektroninis parašas turi tokią pačią teisinę galią kaip ir ranka rašytas parašas. Šis tapatybės nustatymo būdas yra vienas iš populiariausių tarp finansinių institucijų/ bankų, dėl to labai svarbu suprasti kaip klientai naudojasi minėtu parašu. Remiantis RRT užsakytu tyrimu (2023) 2022 m. kvalifikuotas elektroninis parašas dažniausiai buvo naudojamas su Smart ID mobiliąja programėle (68 proc.), asmens tapatybės kortele (21 proc.) arba SIM kortele (16 proc.). Remiantis minėto tyrimo duomenimis, tolimesniame šio darbo etape (žr. skyrius 2) bus nagrinėjamos minėtos kvalifikuot elektroninio parašo priemonės.

(4) Tiesioginis vaizdo perdavimas (du būdai)

Kliento tapatybė patvirtinimas tiesioginio vaizdo perdavimo būdu turi atitikti techninius reikalavimus nurodytus Finansinių nusikaltimų tyrimo tarnybos (toliau FNTT) direktoriaus įsakymu Nr. V-314 (2016). Remiantis šiuo teisės aktu, vaizdas turi būti perduodamas tik nepertraukiami, tiesiogiai realiuoju laiku ir būti tokios kokybės, kuri leistų lengvai nuskaityti pateiktą informaciją. Tam finansinės institucijos turi naudoti specialias programas/ priemones, kurios užtikrintų keliamus reikalavimus. Tiesioginis vaizdo perdavimas gali būti naudojamas tapatybei nustatyti šiais dviem būdais:

1. *Užfiksuojant kliento tapatybės dokumento originalą* (asmens tapatybės kortelė, leidimas gyventi, pasas, vairuotojo pažymėjimas) *ir jį patvirtinant bent pažangiuoju parašu* ne vėliau nei per vieną valandą. Pažangusis parašas yra labai panašus į kvalifikuotą, tačiau turi žemesnius saugumo reikalavimus ir yra dažniau naudojamas įmonės vidinių ir trumpo saugojimo dokumentų pasirašymui. Įvertinus tai kad pažangusis parašas nėra plačiai naudojamas, galima teigti, kad šis tapatybės nustatymo būdas nėra labai populiarus
2. *Užfiksuojant kliento veido atvaizdą ir kliento parodytą tapatybės dokumento originalą*. Šį veiksmą galima atlikti tiesioginio vaizdo arba nuotraukos perdavimo metodais. Siekiant tapatybę patvirtinti kliento atvaizdą fiksuojant tiesioginio vaizdo perdavimu būtina užfiksuoti kliento veido atvaizdą iš priekio ir veido atvaizdą iš priekio kartu su tapatybės dokumento originalu. Vartotojui toks tapatybės nustatymas yra pateikiamas kaip reikalavimas pateikti asmenukę (angl. „selfie“) ir asmenukę laikant asmens tapatybės dokumentą (angl. „selfie with ID“). Tuo tarpu tapatybę nustatant tiesioginio nuotraukos perdavimu kliento veido atvaizdas iš priekio yra nufotografuojamas, bei klientas turi tiesiogiai pateikti tapatybės dokumento nuotrauką. Minėtas būdas yra labai dažnai naudojamas tarp finansinių institucijų ne tik Lietuvoje, bet ir užsienyje. Tarptautinė pinigų

pervedimo platforma Wise (anksčiau žinoma kaip TransferWise) naudoja tiesioginio vaizdo/ nuotraukos perdavimus metodus ir pateikia klientams instrukcijas kaip tinkamai pateikti prašomus dokumentus.

(5) Mokėjimo pavedimas ir tinkamai patvirtinta asmens tapatybės dokumento kopija

Kliento tapatybė gali būti nustatoma nuotoliniu būdu klientui į jo mokėjimo sąskaitą atlikus pavedimą iš kitos kredito įstaigos kliento vardu turimos sąskaitos. Kredito įstaiga iš kurios yra atliekamas pavedimas turi būti registruota ES valstybėje narėje arba trečioje valstybėje, nustačiusioje PPTFPĮ reikalavimams lygiaverčius reikalavimus. Tuo pačiu metu klientas turi paštu/ per kurjerį/ fiziškai pateikti patvirtintą popierinę tapatybės dokumento kopiją, atitinkančią reikalavimus pateiktus FNTT direktoriaus įsakymu Nr. V-131 (2017). Ši priemonė nereikalauja specialių įrenginių ir dėl to galėtų pasirodyti patraukli. Tačiau finansinė įstaiga, įpareigota nustatyti savo kliento tapatybę, negali užtikrinti tinkamo tapatybės nustatymo kitoje įstaigoje (iš kurios gautas mokėjimas). Taip pat, atsižvelgiant į tai kaip turi būti sudaryta ir pateikta asmens dokumento kopija, galima teigti, kad tapatybę nustatant minėtu būdu išnyksta tapatybės nustatymo klientui fiziškai nedalyvaujant esmė. Įvertinus minėtus reikalavimus galima įvertinti šia priemonę kaip nepatrauklią. Verta pažymėti, kad kai kurios institucijos (UAB „Credit Service", 2023) gali naudoti mokėjimo pavedimą kaip papildomą priemonę kliento tapatybės nustatymui.

Iš pateiktos PPTFPĮ 11 str. nurodytų kliento tapatybės nustatymo jam fiziškai nedalyvaujant būdų analizės galima pastebėti, kad populiariausi tapatybės nustatymo internete būdai yra kvalifikuotas elektroninis parašas ir tiesioginis vaizdo perdavimas užfiksuojant kliento veido atvaizdą ir kliento parodytą tapatybės dokumento originalą. Vertinant tapatybės nustatymo internete būdus pastebima, kad ne visi jie kelią vienodas grėsmes rizikas ir dėl šios priežasties tolimesniuose darbo etapuose didesnis dėmesys bus skiriamas populiariausių/ didžiausią riziką keliančių metodų analizei. Taip pat atkreiptinas dėmesys į tai, kad tapatybės nustatymas turi būti vykdomas ne tik prieš pradedant dalykinius santykius su klientu, tačiau ir jiems jau prasidėjus. Prasidėjus dalykiniams santykiams su klientu svarbu užtikrinti kad būtent jis naudojasi finansinės institucijos paslaugomis ir niekas kitas neturi prieigos prie jo paskyros. Pažymėtina vartotojo paskyros autentifikavimą galima iš dalies laikyti ir tapatybės patvirtinimo dalimi, dėl to tolimesniuose paskyrų autentifikavimas gali būti nurodamas kaip tapatybės patvirtinimas

1.3. Vartotojo paskyros autentifikavimas

Kiekviena finansinė institucija ne tik privalo nustatyti kliento tapatybę bet ir užtikrinti, kad sąskaita yra naudojama tik to paties anksčiau identifikuoto vartotojo ir taip patvirtini jo jau nustatytą tapatybę

Institucijos dažnai siekia supaprasti daugumą procedūra taip padarant savo paslaugas patrauklesnes klientui, tačiau tai gali sukelti papildomų grėsmių, kuria būtina įsivertinti. Bankai ir kitos finansinės institucijos investuoja į saugumą ir vykdo įvairias prevencines kompanijas siekdamos užtikrinti maksimalų paskyrų saugumą. Atkreiptinas dėmesys į tai, kad finansinės institucijos gali naudoti įvairias/ skirtingas priemones nustatant, kas jungiasi prie vartotojo paskyros. Dėl to analizuojant paskyrų autentifikavimą svarbu išskirti kaip klientai yra atpažįstami jungiantis pagrindinių finansinių institucijų, bankų ir elektroninių pinigų įstaigų paskyrų. Atkreiptinas dėmesį tai, kad šiame darbe minint vartotojo paskyrą, turima omenyje finansinės įstaigos vartojo paskyrą elektroninėje bankininkystėje

Populiariausi Lietuvoje veikiančių bankų elektroninių paslaugų teikimo būdai yra internetinė ir mobilioji bankininkystės. Pagrindinis skirtumas tarp šių dviejų būdų yra prisijungimo programa: internetinei bankininkystei reikalingas kompiuteris arba išmanusis įrenginys su įdiegta naršykle, o mobiliajai – mobilioji programėlė įrenginyje. Norint prisijungti minėtais būdais bankai dažniausiai prašo įvesti išduotą vartotojo atpažinimo kodą ir/ arba asmens kodą, specialų PIN kodą ar telefono numerį. Tolimesnis vartotojo paskyros autentifikavimo žingsnis priklauso nuo prisijungimo būdo ir gali skirtis priklausomai nuo elektroninės bankininkystės prisijungimo būdo. Pagal žemiau pateiktą lentelę (1 lentelė) galima pastebėti, kad ne visos prisijungimo prie paskyros priemonės yra prieinamos jungiantis

1 lentelė. Prisijungimo, prie elektroninės bankininkystės ir mobiliosios programėlės paskyrų, priemonės jungiantis pirmą kartą

Priemonė	Internetinė bankininkystė	Mobilioji programėlė
„Smart-ID:	+	+
„Mobile-ID“	+	+
Pin kortelė/ generatorius	+	+
Biometriniai duomenys	+	-
Asmens tapatybės kortelė	+	-

Šaltinis: sudaryta autorės remiantis finansinių institucijų internetiniuose puslapiuose/ aplikacijose pateikta informacija (2023)

prie banko paskyros per mobiliąja programėlę. Jungiantis prie internetinės bankininkystės su asmens tapatybės kortele yra reikalinga speciali įranga/ skaitytuvas nebent įrenginyje iš kurio yra jungiamasi yra integruotas kortelių skaitytuvas. Norint pasinaudoti biometriniais duomenimis nereikia specialaus skaitytuvo, bet reikalingas išmanusis įrenginys (telefonas/ planšetinis kompiuteris) turintis integruotą įrangą/ programą (veido atpažinimas, piršto antspaudo nuskaitymas). Verta paminėti, kad lentelėje pateikta informacija yra taikytina, kai prie mobiliosios programėlės yra jungiamasi pirmą kartą ar po ilgesnio neaktyvumo laikotarpio. Naudojant išmanųjį įrenginį pakartotinai jungiantis prie mobiliosios bankininkystės galima naudoti biometrinius duomenis ar savo susikurtą PIN kodą. Minėtų prisijungimo

prie elektroninės bankininkystės priemonių patikimumas bus analizuojamas antrame šio darbo skyriuje (žr. 2 skyrius).

Elektroninių pinigų įstaigos dažniausiai paslaugas teikia pasitelkiant internetinę ir mobiliąją bankininkystes, tačiau prisijungimas prie paskyros nesiskiria. Atsidarant sąskaitą elektroninių pinigų įstaigoje, klientai yra prašomi pateikti tam tikrus duomenis (elektroninis paštas, telefono numeris), kurie vėliau yra naudojami prisijungti prie paskyros. Verta paminėti, kad tarp elektroninių pinigų įstaigų yra atvejų, kai sąskaitą galima atsidaryti ir prie jos prisijungti, naudojanti trečiųjų šalių pagalba. Lietuvoje tokių atvejų aptikti neteko, tačiau tarptautinė pinigų pervedimo platforma Wise leidžia klientam atsidaryti sąskaitą ir prie jos prisijungti naudojantis trečiųjų šalių paskyromis (Facebook, Google, Apple). Jungiantis prie elektroninių pinigų įstaigų pakartotinai, yra naudojami biometriniai duomenys ar PIN kodas.

Ši paskyrų autentifikavimo apžvalga, leidžia suprasti kokios priemonės/ būdai yra naudojami siekiant užtikrinti, kad prie kliento paskyros jungiasi būtent jis. Nepaisant to, minėtos priemonės negali visiškai užtikrinti gaunamos informacijos patikimumo nes jos turi trūkumų/ pažeidžiamumų, kurie bus analizuojame kitame šio darbo skyriuje (žr. 3 skyrius).Turint omenyje, kad paskyrų autentifikavimas gali būti pažeidžiamas, svarbu išskirti pagrindines grėsmes. Kadangi tapatybės nustatymas internete yra glaudžiai susijęs su paskyrų autentifikavimu, susijęs grėsmės būtinai išnagrinėti kartu.

Apibendrinant, besivystant elektroniniai bankininkystei atsirado kelios skirtingos rūšys, tačiau labiausiai paplitusios yra tik dvi: internetinė ir mobilioji bankininkystės. Siekiant nustatyti klientų, besinaudojančių minėtomis elektroninės bankininkystės rūšimis, tapatybę internetu svarbu, kad šis veiksmas atitiktų keliamus standartus. PPTFPĮ numato penkis pagrindinius tapatybės nustatymo nuotoliniu būdu , tačiau finansinės institucijos dažniausia pasitelkia kvalifikuota elektroninį parašą ir/ arba tiesioginį vaizdo perdavimą užfiksuojant kliento veido atvaizdą ir kliento parodytą tapatybės dokumento originalą. Nustačius kliento tapatybę svarbu užtikrinti, kad prie paskyros jungiasi ir ja naudojasi klientas, kurio tapatybė anksčiau buvo patvirtinta. Nagrinėjant vartotojų paskyrų autentifikavimą buvo išskirti pagrindiniai skirtumai tarp skirtingų finansinių institucijų (bankų ir elektroninių pinigų įstaigų) ir tarp internetinės ir mobiliosios bankininkystės paskyrų atpažinimo. Visa ši informacija padėjo suprasti, kokius, asmens tapatybė ir paskyros autentifikavimo, būdus naudoja finansinės institucijos. Siekiant šiame darbe tinkamai įvertinti tapatybės internete ir paskyrų autentifikavimo pagrindines grėsmes pinigų plovimo prevencijos rėžimui, svarbu atlikti naudojamų priemonių ir jų patikimumo analizę.

2. TAPATYBĖS NUSTATYMO INTERNETE PRIEMONIŲ IR JŲ PATIKIMUMO APŽVALGA

2.1. Finansų įstaigose naudojamų, tapatybės nustatymo internete ir paskyros autentifikavimo priemonių patikimumas

Tapatybės nustatymas klientui tiesiogiai nedalyvaujant yra reglamentuos įstatymų, tačiau siekiant užtikrinti tinkama tapatybės nustatymą svarbu pasirinkti tinkamą priemonę ar jų kombinaciją. Tai turėtų būti daroma įvertinus rinkoje esamų priemonių prieinamumą ir jų patikimumą. Lietuvoje veikiančios finansinės institucijos tapatybei patvirtinti/ paskyrai autentifikuoti naudoja bent vieną iš šių būdų: „Smart-ID“, „Mobile-ID“, Pin kortele/ generatorius, Biometriniai duomenys, Asmens tapatybės kortelė, USB laikmena, elektroninis paštas, telefono numeris. Visi minėti būdai tam tikru metu prašo įvesti PIN kodą ar slaptažodį

„Smart-ID“ yra patogus, saugus ir išmanus būdas nustatyti ir patvirtinti tapatybę, kuriuo gali naudoti visi turintys išmanųjį įrenginį (telefoną, planšetinį kompiuterį). „Smart-ID“ yra dviejų tipų: „Smart-ID“ ir „Smart-ID Basic“. Pirmasis tipas suteikia visus kvalifikuoto elektroninio parašo privalumus ir yra rekomenduojamas visiems naudotojams, o tuo tarpu „Basic“ versija galima naudoti tik prisijungiant prie elektroninės bankininkystės. „Smart-ID“ paskyrą galima susikurti ir patvirtinti keliais būdais: tapatybės kortele, kurią galima naudoti elektroninėje erdvėje, „Mobile-ID“, biometrinių duomenų atpažinimas, banko sąsaja arba apsilankymas banko skyriuje. Remiantis „Smart-ID“ oficialiame internetiniame puslapyje pateikta informaciją, siekiant apsaugoti duomenų perdavimą tarp „Smart-ID“ programėlės ir serverio yra naudojamas HTTPS ryšys, kurio metu yra užtikrinamas duomenų šifravimas ir saugumas naudojant TLS/ SSL sertifikatais . „Smart-ID“ taip pat yra taikomi keli saugos faktoriai: PIN1 (naudojamas patvirtinti tapatybei) ir PIN2 (naudojamas elektroniniams parašams ir operacijoms patvirtinti), kurios žino tik paskyros savininkas, ir mobiliajame įrenginyje taikomų asmeninių raktų, naudojamų visoms „Smart-ID operacijoms atlikti, poros. Asmeninis raktas yra kriptografinis raktas, kuris slaptai saugomas ir naudojamas matematiniam skaitmeninių parašų generavimui. Asmeniniai raktai yra kombinuojami iš dalies saugomos „Smart-ID“ programėlėje, kuri yra apsaugota PIN kodais, ir dalies esančio „Smart-ID“ serveryje, kuri apsaugota naudojant aparatinį saugumo modelį (angl. Hardware security model, HSM). Norint suklastoti „Smart-ID“ elektroninį parašą, įsilaužėlis turėtų apeiti abiejų asmeninio rakto dalių apsaugą, o tai užtikrina aukštą apsaugos lygį. Toks tapatybės nustatymo būdas atitinka aukščiausio lygio saugumo reikalavimus pagal eIDAS ir nuo 2018 m. yra pripažįstamas kaip kvalifikuotas elektroninis parašas.

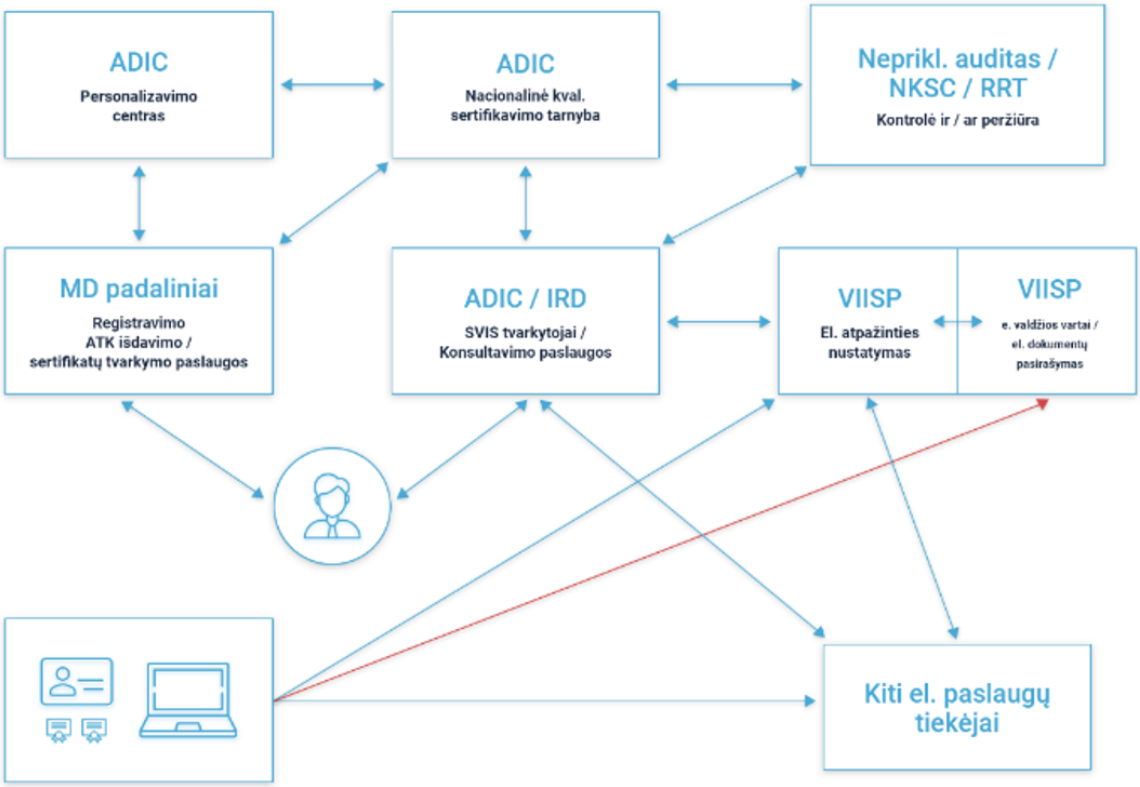
„Mobile-ID“ (anksčiau vadinamas mobilusis parašas) yra kvalifikuota elektroninio parašo ir asmens tapatybės atpažinimo/ nustatymo priemonė išduodama kartu su SIM kortelėmis. „Mobile-ID“

galima įsigyti kreipiantis į tam tikrus mobiliojo ryšio operatorius (UAB „Bitė Lietuva“, AB „Telia Lietuva“. UAB „Tele2“). Remiantis Lietuvoje išduodamų „Mobile-ID“ sertifikatų naudojimo sąlygomis (SK ID Solutions, 2022) „Mobile-ID“ yra taikomi sertifikavimo raktai (privatusis ir viešasis), kurie yra apsaugoti naudojant HSM. „Mobile-ID“ taip pat yra taikoma apsauga naudojant specialius kodus: PIN1 – skirtas tapatybei patvirtinti ir susidaro iš 4-8 skaitmenų kodo, PIN2 – naudojamas elektroniniams parašams ir operacijoms patvirtinti, PUK - skirtas atblokuoti PIN kodus. Iš pateiktos informacijos matyti, kad „Smart-ID“ ir „Mobile-ID“ veikia labai panašiai, tačiau žiūrint iš technologinės pusės, pagrindinis skirtumas tarp minėtų priemonių yra duomenų perdavimas. „Mobile-ID“ perduodi duomenis tarp SIM kortelės ir serverio naudoja HTTP ryšį („Smart-ID“ – HTTPS), kuriuo metu duomenys ir informacija nėra koduojama. Nepaisant minėto skirtumo, „Mobile-ID“ atitinka eIDAS reglamento standartus ir yra laikomas kvalifikuotu elektroniniu parašu.

Bankai taip pat siūlo alternatyvią tapatybės atpažinimo internete priemonę***, PIN kodų kortelę/ generatorių***, klientams, kurie neturi išmaniojo telefono ir nesinaudojo kitomis asmens tapatybės nustatymo ir prisijungimo prie banko sąskaitos. Nuo 2016 m. klientams, besinaudojantiems slaptažodžių kortelėmis, buvo įvesta papildoma saugumo priemonė. Norint prisijungti prie banko paskyros/ autentifikuoti paskyrą ar atlikti tam tikrus veiksmus, klientai turės suvesti ne tik kortelėje nurodyta kodą, bet ir papildomą, SMS žinute gautą, kodą. Nepaisant to, daugumą Lietuvoje veikiančių bankų tokios kliento atpažinimo priemonės atsisakė dėl saugumo spragų. RRT taip pat esant galimybei, vietoje slaptažodžių kortelės naudoti slaptažodžių generatorių. Kodų generatorius tai nedidelis elektroninis prietaisas, kuris generuoja vienkartinius/ unikalius prisijungimo kodus. Naudojant šį prietaisą tapatybė yra patvirtinama kai kliento įvesti duomenys (atpažinimo kodas/ vartotojo ID, nuolatinis slaptažodis ir kodų generatoriaus sugeneruotas slaptažodis) atitinka banko serveryje esančią informaciją.

USB laikmena yra kriptografinė laikmena išduodama Registrų centro, kurioje yra laikomas kvalifikuotas sertifikatas. gali būti naudojamas prisijungti prie internetinės bankininkystės. Šiam prisijungimo būdui reikalinga papildomą programinė įranga. Swedbankas siūlydama prisijungimą prie paskyros naudojant USB laikmeną ar asmens tapatybės kortelę rekomenduoja įdiegti „ID“ įskiepį. Siekiant prisijungti prie internetinės bankininkystės ir patvirtinti tapatybę su USB laikmeną reikia prijungti USB laikmeną prie kompiuterio ir įvesti žinomą slaptažodį. Tokios laikmenos dažniausiai yra naudojamos saugoti elektroniniams parašams/ sertifikatams, nes joms nėra lengva pritaikyti reversinės inžinerijos metodus. Tuo tarpu siekiant patvirtinti tapatybę jungiantis prie internetinės bankininkystės su asmens tapatybės kortele reikalingas specialus skaitytuvas (nebent įrenginyje iš kurioj jungiamasi skaitytuvas yra integruotas), speciali programinė įranga ir tapatybės kortelės elektroninio parašo PIN kodas. Asmens tapatybės kortelėje yra saugomi dvi viešojo rakto infrastruktūros, elektroninės atpažinties

sertifikatas ir kvalifikuotas elektroninio parašo sertifikatas, kurias sudaro viešojo ir privataus raktų poros. Remianti Lietuvos Respublikos vidaus reikalų ministerijos pateikta informacija (eid.lt, 2023), kortelėje yra įdiegta kriptografinio mikroprocesorinio lusto technologija pagrįsta tarptautiniu standartu EMV. Taip pat asmens tapatybės kortelėje yra naudojama elektroninėje erdvėje sukurta valstybės



3 pav. Asmens tapatybės kortelės valstybės valdomo Viešojo rakto infrastruktūros institucinė sandara ir internetinių paslaugų teikimo principinė schema

Šaltinis: sudaryta Lietuvos Respublikos vidaus reikalų ministerijos (eid.lt) (2023)

valdoma Viešojo rakto infrastruktūra (žr. 3 pav.). Tokia technologija atitinka aukščiausius saugumo standartus, yra laikoma kvalifikuotu elektroniniu parašu ir yra vienintelė Lietuvoje naudojama atpažinties priemonių kuri yra pripažįstama ES. Dėl minėtų technologinių sprendimų gali teigti, kad asmens tapatybės kortelėje įdiegta technologija daro ši tapatybės patvirtinimo/ atpažinimo būda atsparų kibernetiniams pažeidimams ir padirbinėjimui. Verta paminėti, kad keičiantis technologijoms keičiasi/ yra peržiūrimi ir saugumo reikalavimai. Dėl to buvo priimtas sprendimas, kad kortelės išduotos iki 2021 m. rugpjūčio 12 dienos nuo 2023 m. liepos mėnesio nebebus tinkamos naudoti kvalifikuotam parašui.

Biometrinis tapatybės nustatymas yra paremtas asmens fiziologinėmis savybėmis, kurios negali būti perduotos kitam žmogui, tokiomis kaip piršto antspaudais, veido atvaizdu, akie rainele ir pan. Štitilis, Pakutinskas, Laurinaitis ir Dauparaitė (2011) biometrinių duomenų sistema apibūdina dviem etapais. Pirmiausia vartotojo duomenys yra perkeliami į skaitmeninę formą ir taikant tam tikrus

algoritmus gautas rezultatas yra registruojamas. Jei duomenys sutampa, vartojo tapatybė yra patvirtinama. Vienas iš šios sistemos pažeidžiamumų yra neteisėtai gautų biometrinių duomenų klastojimas ir panaudojimas apeiti biometrinę apsaugą, pvz. padaromo veido atvaizdo kopija ir ji vėliau neteisėtai panaudojama. Siekiant suvaldyti šia riziką yra patirtina, biometrinius duomenis naudoti tapatybės nustatymui kartu su papildoma apsaugos priemone (slaptažodžiu, elektroniniu parašu ir pan.). Siekiant nustatyti finansinės įstaigos kliento tapatybę ar autentifikuoti jo paskyrą, biometriniai duomenys gali būti panaudoti *dviem tikslams*. Prieš pradedant dalykinius santykius, finansinės įstaigos prašo klientų pateikti įvairius duomenis/ dokumentus siekiant *nustatyti kliento tapatybę*. Dažnai yra prašoma kliento pateikti veido atvaizdą realiuoju laiku, tačiau siekiant šio būdo patikimumo, finansinės įstaigos turi naudoti patikimas dokumentų tikrinimo programas ir/arba kelti darbuotojų tikrinančių dokumentus kvalifikaciją. Siekiant papildomai įsitikinti, kad veido atvaizdo savininkas siekia patvirtinti savo tapatybę, yra prašoma pateikti veido atvaizdą realiuoju laiku kartu su asmens tapatybės dokumentu. Kitas atvejis kai yra naudojami biometriniai duomenys yra kliento paskyros autentifikavimas. Šis sprendimas yra įgyvendinamas išmaniųjų telefonų/ prietaisų pagalba, nes dauguma jų turi integruotus, tam tikrų biometrinių duomenų (piršto antspaudų, veido atpažinimo), skaitytuvus. Šiuo atveju paskyros autentifikavimas ir duomenų saugumas priklauso nuo telefonų gamintojo įdiegtų saugumo parametrų, dėl to svarbu įvertinti populiariausių telefonų gamintojus

- **iPhone** naudojami piršto antspaudai yra užkoduoti, saugomi tik telefone ir apsaugoti raktu, kuris yra prieinamas tik su atskira „Secure Enclave“ sistema. Veido atpažinimui (angl. Face ID“) yra naudojama „TrueDepth“ gylio kamera ir mašininiu mokymusi (angl. machine learning) siekiant pasiūlyti saugu autentifikavimo sprendimą. Įvertinus tai, kad iPhone telefonuose yra naudojamas duomenų kodavimas, galima teigti, kad šie išmanūs telefonai yra saugūs. Su šia nuomone sutinka ir Croft ir McNally (2023) teigdami, kad iPhone telefonai yra laikomi saugesniais nei Android operacinę sistemą turintys įrenginiai.
- **Samsung** savo tinklapyje teigia kad veido atpažinimo technologija yra mažiau saugi nei kiti telefono apsaugos būdai. Verta pažymėti, kad Samsung labiau orientuojasi į piršto antspaudų skanavimo saugumą ir patikimumą. Šiuo metu naujausiuose Samsung modeliuose yra naudojamas ultragarsinis piršto antspaudų skaitytuvas, kuris yra laikomas (Button 2023, Samsung for Business 2021, Petrovan 2019) saugiausiu skaitytuvu integruotu mobiliajame įrenginyje. Samsung įmonė šiuo metu vysto naują technologiją piršto antspaudus atpažinimo technologiją, kurios pagalba įrenginiai gebėtų nuskaityti kelis piršto antspaudus vienu metu (2022)

Lietuvoje veikiantys bankai tokio prisijungimo būdo netaiko, tačiau elektroninių pinigų įstaigos dažniausiai autentifikuoja vartotojo paskyrą pateikiant registracijos metu nurodytą ***elektroninį paštą ar***

telefono numerį bei suvedant paskyros slaptažodį. Be jokių papildomų apsaugos priemonių, toks prisijungimo būdas yra laikomas nesaugiu, tačiau elektroninės pinigų įstaigos dažniausiai taiko papildomas apsaugos priemones, pavyzdžiu kodo siuntimas į patvirtintą el. paštą/ telefono numerį. Tokia priemonė turėtų būti vertinama atsargiai, nes klientai dažniausiai naudojasi elektroninių pinigų įstaigų paslaugomis per programėlę, kuri yra įdiegta išmaniajame prietaise susietam su nurodytu telefono numeriu ar el. paštu. Praradus išmanųjį įrenginį, minėtas paskyros autentifikavimo būdas gali būti apeinamas trečiųjų asmenų, jei pačio įrenginio apsauga yra nepakankamai stipri (pvz. naudojami populiariausi slaptažodžiai). Dėl to naudojant elektroninį paštą/ telefono numerį autentifikuoti paskyrai svarbu užtikrinti išmaniojo įrenginio saugumą.

Pagrindiniai Lietuvoje veikiančių finansinių institucijų (bankų ir elektroninių pinigų įstaigų) naudojami tapatybės internete ir paskyrų autentifikavimo būdai yra laikomi saugiais, tačiau jie turi tam tikrų saugumo spragų. Saugumo spragos gali atsirasti naudojamo būdo pobūdžio ar jame esančio technologinio sprendimo. Nepaisant to, finansinės institucijos turi įvertinti esamas/ galimas saugumo spragas norint sumažinti jų keliamas grėsmes pinigų plovimo prevencijos rėžimui. Norint pasiūlyti saugiausią būdą, kuris padėtų sumažinti pinigų plovimo prevencijos rėžimui keliamas grėsmes, būtina išanalizuoti užsienio šalyse taikomus metodus. Siekiant tai padaryti, kuo tiksliau buvo pasirinktos šalys turinčio aukšta kibernetinio saugumo reitingą

2.1.1. Atvejo analizė: Danijos karalystė

Remiantis Jungtinės Karalystės saugumo tyrimų įmonės „Compritech“ duomenimis (2022), kad kelis metus iš eilės Danija pirmauja kibernetinio saugumo priemonių reitinge. Tam, kad pasiekti tokį aukštą kibernetinio saugumo lygį, reikėjo investuoti daug pastangų ir laiko, tačiau padėjo sustiprinti gyventojų saugumą kibernetinėje erdvėje. Tai įvertinus, galima teigti, kad Danijos elektroninės bankininkystės ir joje naudojamų vartotojo tapatybės internete ir paskyrų autentifikavimo internete priemonių analizė, gali sutelkti naudingų įžvalgų.

Danijoje veikiantys bankai norėdami patvirtinti asmens tapatybę, dažniausiai prašo pateikti asmens tapatybės dokumento kopiją, CPR numerį, adresą Danijoje patvirtinantį dokumentą ir įdarbinimą įrodanti dokumentą. Verta paminėti, kad dauguma Danijos bankų neleidžia sąskaitos atsidaryti internetu ir prašo atvykti į banko skyrių ar užsiregistruoti susitikimui internetu. Nagrinėjant pagrindiniu bankus (Danske, Nordea, Jysk bank, Sydbank) buvo pastebėta, kad tik Nordea leidžia sąskaitą atsidaryti nuotoliniu būdu, o norint atsidaryti sąskaitą „Danske“, „Jysk Bank“ ar „Sydbank“ būtina atvykti į banko skyrių. Toks tapatybės patvirtinimas yra vienas iš saugiausių ir sumažina netinkamą tapatybės nustatymo rizikas. Autentifikuojant kliento paskyrą, dažniausiai nereikia nerimauti dėl kliento tapatybės.

Autentifikuojant kliento sąskaitą internetinėje bankininkystėje ar mobiliojoje programėlėje yra visi bankai prašo pateikti tradicinius duomenis (vartotojo vardą, slaptažodį). Siekiant paskyrą patvirtini papildomų, Nordea siūlo kelis variantus papildomus patvirtinimo priemones: „Nordea ID“ mobiliąją programėlę ir “MitID“. MitID programėle naudoja daugumą Danijos bankų, tačiau yra siūloma ir alternatyvų: MitID vienkartinių kodų generatorius (kodas pateikiamas prietaiso ekrane arba balso komanda), MitID čipas/ mikroschema. Kodų generatorius ir čipas yra naudojamas kaip dviejų faktorių autentifikavimo priemonė, tačiau MitID programėlė yra kelių faktorių autentifikavimo prietaisas. Taip yra todėl, kad pačioje programėlėje yra naudojama du papildomi autentifikavimo faktoriai: tai ką klientas žino (PIN kodas) ir tai ką, klientas turi (programėlė taikomos apsaugos funkcijos). Nagrinėjant šios programėlės saugumą buvo pastebėti šie pagrindiniai parametrai/ technologijos/ saugumo elementai padedantys autentifikuoti vartotojo paskyrą:

- Naudojamas brokerio/ tarpininko modelis kurį taikant prieigą prie MitID saugomų duomenų turi tik patvirtintas/ sertifikuotas tarpininkas, o ne daugelis paslaugų tiekėjų.
- Naudojami autentifikavimo faktoriai yra pagrįsti tuo ką klientas žino (pvz.: PIN kodas), ką turi (MitID programėlė) ir kas yra (biometriniai duomenys). Pažymėtina, kad MitID nenaudoją nuosavybė pagrįstų autentifikavimo priemonių – biometriniai duomenys naudojami išmaniajame įrenginyje yra pasitelkiami tik atskleisti PIN kodui (ar kitą informaciją, kurią klientas turi žinoti)
- Technologinis sprendimas yra paremtas dvejais asimetriniais kriptografiniais algoritmais: elipsinės kreivės skaitmeninio parašo algoritmu (angl. Elliptic Curve Digital Signature Algorithm, ECDSA) ir viešojo rakto kriptosistema RSA.
- Duomenų perdavimas tarp programėlės ir serverio yra apsaugotas Vykdymo laiko programų savisaugos (angl. Runtime Application Self-Protection, RASP) technologija ir transporto sluoksnio saugumo (angl. Transport Layer Security, TLS) protokolu
- Prieš autentifikuojant paskyrą su MitID programėle nereikia suvesti slaptažodžio, nes jis įterptas į programėlę
- Siekiant vartotojus apsaugoti nuo atsitiktinio patvirtinimo, MitID programėlėje nėra naudojami „Push“ pranešimai kurių pagalba galima atsidaryti programėlę automatiškai. Jei klientas pats inicijavimo prisijungimą prie banko, jis pats turi atsidaryti programėlę.
- Papildoma apsauga siekiant apsisaugoti nuo netikrų tinklapių – jei yra jungiamasi prie internetinės bankininkystės, banko internetinio puslapio URL adresas visada turi baigtis MitID.dk (pvz. https://jyskebank.mitid.dk/)

Minėti saugumo sprendimai slypintys už MitID programėlės atitinka aukščiausius eIDAS standartus ir yra pripažįstama ES kaip aukšto lygio elektroninės atpažinties priemonė. Kuriant šią

programėlę buvo atsižvelgta į aktualias problemas rizikas ir įdiegti sprendimai padeda pinigų plovimo rizikas susijusias su paskyrų autentifikavimu (tapatybės vagystė, neteisėta prieiga prie paskyros)

2.1.2. Atvejo analizė: Jungtinė Karalystė

Remiantis Jungtinės Karalystės saugumo tyrimų įmonės „Compritech“ duomenimis (2022), Jungtinė Karalystė užima aštuntą vietą kibernetinio saugumo priemonių reitinge. Siekiant išanalizuoti šioje šalyje naudojamus kliento tapatybė internete ir paskyrų autentifikavimo, buvo pasirinkti keturi bankai: „HSBC“, „Lloyds“, „Roayl Bank of Scotland“ (toliau RBS), „Barclays“.

Minėti bankai naudoją žemiau pateiktus duomenis (dažniausiai jų kombinaciją) siekiant nustatyti kliento tapatybę internetu:

- *Asmens tapatybės dokumentas* – Jungtinėje Karalystėje veikiantys bankai leidžia naudoti ne tik pasą/ asmens tapatybės kortelę bet ir valstybėje išduotą vairuotojo pažymėjimą. JK vairuotojų ir transporto priemonių licencijavimo agentūra (remiantis Mills 20218) teigia, kad vairuotojo pažymėjimas yra saugus dokumentas. Tačiau verta atkreipti dėmesį, JK naudojami asmens tapatybės dokumentai nėra pripažįstami ES kaip elektroninės atpažinties priemonės
- *Adresą/ pajamas patvirtinantys dokumentai.* Banko sąskaitos išrašas, sąskaita už komunalines sąskaitas, mokesčių deklaracijos ir panašūs dokumentai yra naudojami ne tik adresui/ pajamoms patvirtinti, bet ir tapatybei nustatyti. Dokumentų patvirtinimui ar tapatybės nustatymui internete, bank dažnai naudojasi papildomus paslaugomis/ programinėmis įrangomis. Pavyzdžiui „RBS“ nurodo kad klientų tapatybės nustatymui internete ir dokumentų patikrinimui yra naudojamasi „HooYu“ ir „DigiDocs“ paslaugomis. „HooYou“ sujungia tradicinį dokumentų patikrinimą (pvz.: duomenų bazės patikrinimas) su naujomis technologijomis (skaitmeninio pėdsako analizė, veido biometrinių duomenų analizė ir pan.). Toks metodas leidžia užtikrinti patikimą dokumentų patikrinimą
- *Trečiųjų šalių teikiama informacija*. Kai kurie JK veikiantys bankai siekdami patvirtinti kliento tapatybę internetu naudoja papildomą būdą, t.y. naudojasi kredito biurų paslaugomis. Pavyzdžiui „Barclays“ siekdamas patvirtinti kliento tapatybę internetu, proceso metu prašo atsakyti į kelis kredito biuro pateiktus klausimus. Jeigu patikros metu visa pateikta informacija sutampa ir kliento tapatybė nustatomo, jam leidžiama atsidaryti sąskaitą interneto banke. Pažymėtina, kad pasirinkus kelis kliento tapatybės atpažinimo būdus, galima užtikrinti sėkmingesnį tapatybės nustatymą.
-

Iš pateiktos informacijos, pastebima, kad JK bankai naudoja, kurie nėra labai paplitę tarp Lietuvoje veikiančių bankų (adresą/ pajams patvirtinantis dokumentas ir trečiųjų šalių teikiama informaciją).

2 lentelė. Jungtinėje Karalystė veikiančių bankų naudojami asmens tapatybės internete nustatymo ir paskyros autentifikavimo būdai naudojant internetinę bankininkystę ir mobiliąją programėlę

Bankas	Internetinė bankininkystė	Mobilioji programėlė
HSBC	Vartotojo vardas + *skaitmeninis saugos raktas* kodui gauti	Vartotojo vardas + *skaitmeninis saugos raktas* kodui gauti
Lloyds	Vartotojo vardas + slaptažodis + *dalis įsimintinos informacijos*	Vartotojo vardas + slaptažodis + *dalis įsimintinos informacijos* + *automatinis skambutis iš banko*
RBS	Vartotojo specialus numeris arba *bankinės kortelės numeris* + PIN kodas ir slaptažodis + vienkartinis kodas	Vartotojo specialus numeris + elektroninės bankininkystės PIN kodas ir slaptažodis + vienkartinis patvirtinimo kodas gaunamas į telefoną
Barclays	Kliento pavardė + vartotojui suteiktas numeris arba *bankinės kortelės numeris* arba *banko sąskaitos numeris* + patvirtinimas per mobiliąją programėlę arba sugeneruotas kodas per „PINsentry“ arba slaptažodis + *dalis įsimintinos informacijos*	Kliento vardas + *bankinės kortelės numeris* + vienkartinis patvirtinimo kodas gaunamas į telefoną + kortelės PIN kodas

Šaltinis: sudaryta autorės remiantis finansinių institucijų internetiniuose puslapiuose/ aplikacijose pateikta informacija (2023)

Nagrinėjant JK bankų naudojamus paskirų autentifikavimą būdus, pastebima daugiau skirtumų lyginant juos su Lietuvoje veikiančių bankų metodais. Žemiau pateiktoje lentelėje (2 lentelė) pateikiami būdai, kuriuos naudoja didžiausi JK veikiantys bankai, siekiant nustatyti tapatybę/ autentifikuoti vartotojo paskyrą. Naudojamas skaitmeninis saugos raktas ir „PINsentry“ yra mobilus kodu generatorius, kurio generuojami kodai yra dviejų faktorių autentifikavimo (angl. two factor autehntication, 2FA) dalis. Technologija, slypinti už šių įrankių, yra panaši į Lietuvoje naudojama Smart-ID ir yra laikoma saugia priemone autentifikuoti vartotojo paskyrą. Dalinės įsimintinos informacijos, kuri pateikiama atskantant į apsauginius klausimus, (pvz.: pirmos trys mamos vardo raidės). Vien tik šios priemonės naudojimas negali užtikrinti saugaus tapatybės internete ir paskyros patvirtinimo, nes atsakymą galima atspėti pasitelkus socialinius tinklus ir kitą informaciją, dėl to bankai šį būdą taiko kartu su kitais, labiau patikimais. Kitas Lietuvoje netradicinis būdas atpažinti vartotoją internete yra banko kortelės/ sąskaitos numerio pateikimas. Ši priemonė kartu su kitais paskyros saugumo užtikrinimo būdais gali sustiprinti paskyros autentifikavimo patikimumą.

2.1.3. Atvejo analizė: elektroninių pinigų įstaigos

Remiantis LR elektroninių pinigų ir elektroninių įstaigų įstatymu (2011) elektrinių pinigų įstaiga yra apibrėžiama kaip bendrovė (AB arba UAB) kuriai išduota atitinkama licencija ir suteikta teisė leisti elektroninius pinigus Lietuvoje arba ir/ar kitose valstybėse narėse. Tokios įstaigos nėra pririštos stipriai

prie vienos jurisdikcijos (priešingai nei bankai) ir gali lengviau vykdyti veiklą skirtingose šalyse. Lietuvos gyventojams yra prieinamos nemažai ES įmonių, kurios užsiima elektroninių pinigų pervedimu. Siekiant ištirti minėtų įstaigų būdus naudojamus patvirtinti tapatybei internetu ir autentifikuoti kliento paskyrą, pasirinktos trys labiau žinomos įmonės: „Wise Payments Limited“ (toliau „Wise“, „Monese Ltd“ (toliau „Monese“) ir „N26 AG“ (toliau N26).

Pagal žemiau pateiktą lentelę (3 lentelė) pastebima, kad visos pasirinktos institucijos naudoja anksčiau šiame darbe paminėtus, asmens tapatybės internete ir paskyrų autentifikavimo, būdus. Patvirtinti

3 lentelė. Elektroninių pinigų įstaigų naudojamos priemonės patvirtinti asmens tapatybę internetu ir autentifikuoti vartotojo paskyrą

Prašoma informacija	Wise	Monese	N26
Tapatybės patvirtinimas internete			
Asmens tapatybės dokumentas	+	+	+
Asmenukė arba asmenukė su dokumentu realiuoju laiku	+	-	+
Veido atvaizdo vaizdo įrašas realiuoju laiku	-	+	-
Paskyros autentifikavimas			
Telefono numeris su slaptažodžiu	-	+	-
El. pašas su slaptažodžiu	+	-	+
2FA	+	+	+
Socialinių tinklų paskyros (Facebook, Google, Apple-ID)	+	-	-

Šaltinis: sudaryta autorės remiantis finansinių institucijų internetiniuose puslapiuose/ aplikacijose pateikta informacija (2023)

dokumentus asmens tapatybei nustatyti yra naudojamas kombinuotas būdas: įmonėse dirbantys darbuotojai ir automatizuoti sprendimai teikiami trečiųjų šalių. Toks metodas pasirinktas siekiant suvaldyti ir sumažinti riziką patvirtinti suklastotus/ netikrus dokumentus. 2018 metais N26 buvo kritikuojamas dėl netikrų dokumentų patikrinimo, tačiau su šia problema susiduria visos institucijos, kurios suteikia galimybę klientams patvirtinti tapatybę internetu. „Wise“ ir „N26“ naudoja beveik visas tas pačias priemonės, o „Monese“ išsiskiria tuo, kad naudoja veido vaizdo įrašą nustatyti asmens tapatybei internetu bei paskyrai autentifikuoti naudoja patvirtintą telefono numerį. Visos trys tirtos įmonės naudoja 2FA, kai vienkartinis kodas yra gaunamas į telefoną arba kai jungiamasi prie internetinės bankininkystės prašoma autentifikuoti paskyrą per mobiliąją programėlę. Pakartotinai jungiantis prie paskyros per mobiliąją programėlę naudojant patikimą prietaisą, t. y. pritaisą, kuris buvo anksčiau naudotas autentifikuojant paskyrą, pakanką suvesti programėlės PIN kodą ar ją autentifikuoti naudojantis biometriniais duomenimis. Biometrinių duomenų naudojimo saugumas dažniausiai priklauso nuo naudojamo įrenginio patikimumo. Pažymėtina, kad Wise leidžia klientams susieti savo

paskyras su socialiniais tinklais (Facebook, Google, Apple-ID) ir naudoja šį prisijungimo būdą autentifikuojant vartotoją. Tokio būdo pažeidžiamumas yra susijęs internetine bankininkyste ir vartotojų įpročiais naudotis vienu/ keliais prietaisais ir išsaugoti įvairių paskyrų prisijungimo duomenis.

Išanalizavus Danijoje ir Jungtinėje Karalystėje naudojamus, tapatybės nustatymo internete ir paskyrų autentifikavimo, priemones galima pastebėti reikšmingų skirtumų. Įvertinus tai, kad abi analizuotos šalys užima aukštą vietą kibernetinio saugumo reitinguose (pagal Comparitech: Danija - pirma, Jungtinė Karalystė – aštunta), Lietuva ir šalyje veikiančios finansinės institucijos galėtų pasisemti gerosios praktikos pavyzdžių. Įvertinus technologines savybes viena iš tokių inovacijų galėtų būti paremta MitID programėle ar jos saugumo technologijomis paremtas atitikmuo pritaikytas prie Lietuvoje veikiančių įstaigų.

3. ASMENS TAPATYBĖS NUSTATYMO INTERNETE METODŲ KELIAMOS GRĖSMĖS PINIGŲ PLOVIMO PREVENCIJOS RĖŽIMUI

Pinigų plovimas yra sudėtingas procesas siekiant legalizuoti nusikalstamu būdu įgytus pinigus/ turtą, bei nuslėpti jų kilmę. Šis procesas turi tris etapus: pinigų įnešimas į finansų sistemą (angl. Placement), sluoksniavimas (angl. Layering) ir integracija (angl. Integration). Kiekvienas iš minėtų etapų kelią skirtingas rizikas pinigų plovimo prevencijos (angl. anti-money laundering, AML) rėžimui, tačiau pirmieji du yra glaudžiai susiję su tapatybės nustatymu ir paskyrų autentifikavimu. Tinkamas tapatybės nustatymas internete gali sumažinti AML rėžimui kylančias rizikas susijusias su paskirų autentifikavimu, tačiau netinkamas – gali padidinti. Perkėlus tapatybės nustatymą į elektroninę erdvę iš dalies buvo sumažinta žmogiškųjų klaidų riziką. Darbuotojai nustatantys asmens tapatybę klientui atvykus į banką, gali neturėti tinkamų priemonių, įrangos ar patirties padedančio nustatyti dokumento tikrumą. Patikima automatizuota sistema gali padėti sumažinti žmogiškos klaidos skaičių patvirtinant klientų tapatybę. Tačiau kaip parodė atvejų analizė, finansinės institucijos naudoja tiek automatinę sistemą, tiek ir savo darbuotojus siekiant patvirtinti dokumentų autentiškumą. Pažymėtina, kad sukčiai siekiantys nuslėpti savo tikrąją tapatybę ir apeiti tapatybės internete patvirtinimą neatsilieka nuo techninių sprendimų pažangos ir dažnai naudoja įvairias technologijas sukurti netikrus ar modifikuoti tikrus dokumentus. Dėlto tapatybės patvirtinimas internetu kokybė priklauso nuo naudojamų sistemų patikimumo ir turimų žinių.

Siekiant užtikrinti, kad klientas yra tas asmuo, kuriuo jis tvirtina esąs, ir būtent jis jungiasi prie elektroninės bankininkystės paskyros, finansinės institucijos turi turėti atitinkamas procedūras/ sistemas, kurios padėtų nustatyti ir užkirsti kelią neteisėtam paskyros atsidarymui/ naudojimui. Kaip pagrindines grėsmes kylančias iš neteisėtos paskaitos atsidarymo/ naudojimo galima išskirti šias: *(1) paskyra yra sukurta naudojantis pavogta ar netikra tapatybe, (2) į paskyrą yra piktavališkai įsilaužiama, (3) paskyra yra parduota ar kitaip perleista tretiesiems asmenims*

Dabartinis lietuvių kalbos žodynas tapatybę apibrėžia kaip tolygumą, vienodumą ir lygybę pačiam sau. ***Tapatybės vagystę*** galima suprasti įvairiai, tačiau šiame darbe tapatybės vagystę laikysime neteisėtą pasinaudojimą asmens tapatybę įrodančiais duomenimis/ dokumentais (pvz. pasas, vardas ir pavardė) siekiant piktavališkų tikslų. Tapatybės vagystės auka bet kuriuo atveju patirs neigiamas pasekmes, tačiau būtina atkreipti dėmesį, kad toks nusikaltimas susijęs su apmokėjimais/ finansinėmis įstaigomis pasižymi dideliais nuostoliais. Verta pažymėti, kad tapatybės vagystę/ netikrų dokumentų pateikimą galimą išskirti į kelis rūšis:

- *Apsimetinėjimas kitu asmeniu* - sukčius turintis pavogtą asmens dokumentą į save panašaus žmogaus apsimeta esąs dokumento savininku
- *Sintetinė tapatybė* – sujungiant informaciją (pvz. asmens kodą) ir fiktyvią (pvz.: vardas, gimimo metai) informaciją yra sukuriama nauja tapatybė. Kadangi bankai neturi galimybių patikrinti ar klientas gyvas, kuriant sintetinę tapatybę, nusikaltėliai dažnai išnaudoją šį pažeidžiamumą ir naudoja dalį negyvo žmogaus duomenų.

Sužinojus kito asmens asmeninę informaciją ir užvaldžius jo tapatybę galima imtis įvairių neteisėtų veiksmu, tokių kaip banko sąskaitos atsidarymas, kredito kortelės ar paskolų paėmimas. Finansinės institucijos turėtų tai įvertinti ir imtis priemonių siekiant sumažinti tapatybės vagystės riziką. Tai galima padaryti prašant klientų pateikti asmens dokumentus ir savo veido atvaizdą tiesioginio vaizdo/ nuotraukos perdavimo būdu. Tokių dokumentų tikrinimas yra atliekamas finansinių įstaigų darbuotojų arba yra automatizuotas naudojantis trečiųjų šalių programomis. Kai kurios įmonės (pvz. Veriff, iDenfy) teikia dokumentų patikros paslaugas naudojantis sukurta technologija, kuri yra paremta dirbtiniu intelektu. Dirbtinis intelektas analizuoja daugybę technologijų ir įvairių rodiklių, tačiau nei viena programa nėra ideali ir turi tam tikrą paklaidą, kai netikri/ manipuliuoti/ pakeisti dokumentai yra patvirtinami. Verta pažymėti, kad naujos technologijos yra naudojamos ne tik dokumentų tvirtinimo procese, tačiau ir siekiant juos suklastoti ar paveikti taip, kad niekas nepastebėtų. Viena iš tokių technologijų yra „Deepfake“ kuri naudoja dirbtinį intelektą siekiant sukurti nuotrauką/ vaizdo įrašą kuriame turinys yra manipuliuojamas taip, kad asmens išvaizda ar išvaizda atrodytų ar skambėtų kaip kieno nors kito. Vilius Petkauskas (2022) pažymi, kad Deepfake technologija sustiprina esamas tapatybės nustatymo/ paskyrų autentifikavimo grėsmes. Bandant atsidaryti banko sąskaitą su pavogtais tapatybės dokumentais, sukčiai dažnai susiduria su problemomis siekiant apeiti biometrinių duomenų reikalavimą. Tačiau Deepfake technologija suteikia sukčiams galimybę apeiti šį reikalavimą. Norint tinkamai suvaldyti Deepfake (ar kitų ateityje atsirasiančių technologijų) sustiprintas grėsmes, finansinėms institucijoms svarbu sekti aktualias naujienas ir prireikus atnaujinti klientų tapatybės atpažinimo/ paskyrų autentifikavimo procesus ir naudojamas technologijas. Taip pat siekiant užtikrinti kuo mažesnį žmogiškųjų klaidų skaičių, kai dokumentus tikriną darbuotojai, svarbu nuolat vykdyti mokymus ir skatinti sąmoningumą. Visiškai panaikinti tapatybės vagystės ar netikros tapatybės rizikų nėra įmanoma, tačiau tinkami tapatybės nustatymo ir paskyrų autentifikavimo procesai, tokias rizikas minimaliai sumažins ir padės jas suvaldyti.

Neteisėta sąskaitos perėmimas (angl. account takeover) įvyksta, kai sukčiai gauna priėjimą prie tikrų prisijungimo duomenų ir juos sėkmingai užvaldo siekiant iš užvaldytos sąskaitos atlikti neteisėtas operacijas. Toks piktavališkas įsilaužimas į finansinės institucijos kliento sąskaita sudaro sąlygas atsirasti pirminiam nusikaltimui (angl. Predicative offence), kuris yra būtina sąlyga pinigų plovimui

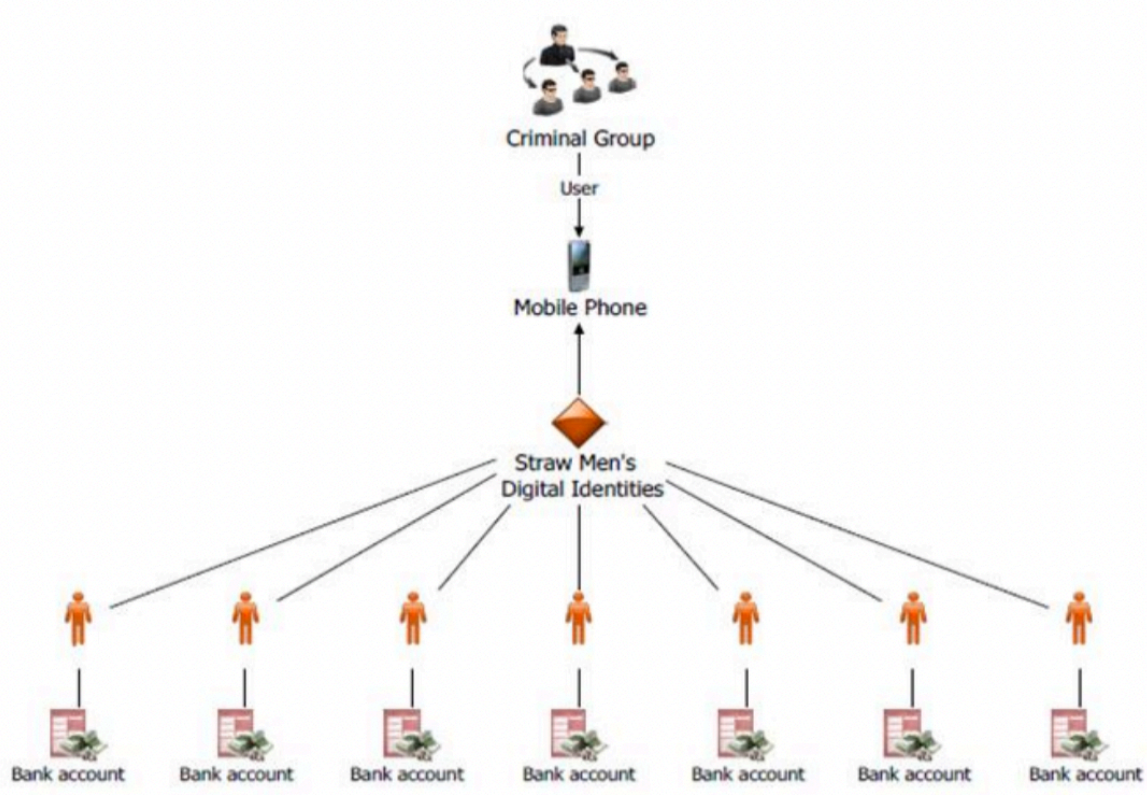
(pinigai turi kilti iš neteisėtos veiklos). Pažymėtina, kad neteisėtai užvaldyta sąskaita gali būti naudojami ne tik pasisavinti visas sąskaitoje esamas lėšas, bet ir būti naudojama kaip tarpinė sąskaita pinigų sluoksniavimui. Įmonė SEON, siūlanti technologinius sprendimus sukčiavimo prevencijai ir aptikimui, išskyrė kelis pagrindinius būdus, kaip sukčiai gali užvaldyti finansinių įstaigų klientų sąskaitas:

- Kredencialų užpildymas (angl. credential stuffing) – kibernetinės ataka, kurios metu yra naudojami prisijungimo duomenys, gauti nutekėjus duomenims, iš vieno tinklapio prisijungti prie kito visiškai nesusijusio.
- Sąskaitos perėmimas pasitelkus duomenų vagystę „phishing“ – „phishing“ atakos yra gaunamos žinutės/ elektroninis laiškas su nuorodą į originalaus puslapio kloną, kuriame prašoma pateikti prisijungimo duomenis.
- Socialinės inžinerija (angl. social engineering) – duomenų/ informacijos išgavimas naudojant psichologines manipuliacijos priemones siekiant išvilioti jautrią/ konfidencialią informaciją
- Žmogaus viduryje ataka (angl. Man in the middle attack, MitM) – atakos metu yra perimami duomenys siunčiami tarp vartotojo ir tinklapio.
- SIM kortelės perėmimas (angl. SIM swapping)
- Kelių svetainių scenarijų ataka (angl. Cross-Site-Scripting, XSS) ir sąskaitos parėmimas

Finansinėms institucijoms siekiant apsisaugoti nuo minėtų ataką visų pirmiausia svarbu šviesti klientą ir jį supažindinti su kibernetinio atakų tipais bei pasidalinti patarimais kaip tinkamai apsaugoti savo paskyrą. Seb bankas (2020) siekdamas atkreipti dėmesį į pavojus ir parodyti kaip juos atpažinti sukūrė saugumo internete testą. Papildomas dėmesys ir saugumo priemonės turėtų būti skiriamos pažeidžiamiems klientams kurie, dėl įvairių asmeninių aplinkybių (pvz.: amžius, silpna sveikata), kelią didesnę riziką tapti kibernetinių atakų aukomis. Vienas iš technologinių sprendimų kaip apsaugoti klientų sąskaitas yra dviejų ar kelių faktorių autentifikavimas. Dviejų ar kelių veiksnių autentifikavimas yra vartotojo atpažinimo procesas, kai tapatybei nustatyti yra naudojami keli būdai. Neteisėtos prieigos temą nagrinėjo nemažai užsienio autorių (pvz.: Tao, Hui, Xiong ir Tsai, 2018; Ogbanufe ir Baham, 2023) ir kai kurie jų pasiūlė savo modelius kaip aptikti neteisėtą prieigą. Coppolino, D'Antonio, Formicola, ir Massei (2015) pasiūlė savo sukčiavimo aptikimo sistema kurioje naudojama Dempster–Shafer teorija. Tuo tarpu Tsai, C.-H., & Su, P.-C. (2021) pasiūlė alternatyvų, panašia į kelių faktorių autentifikavimą, sprendimą pagrįsta maišos pagrindu sukurtą kelių serverių autentifikavimo schema su išmaniąja kortele (angl. a hash-based multi-server authentication scheme in conjunction with a smart card). Nėra aišku ar bent vienas iš paminėtų būdų šiuo metu yra naudojamas finansinėse institucijose, dėl to sunku vertinti jų patikimumą.

Paskyros pardavimas ar kitoks perleidimas tretiesiems asmenims yra traktuojama kaip nelegali veikla daugumoje jurisdikcijų. Finansinėms įstaigoms labai svarbu atitinkamai įvertinti tokią

veiklą, nes ji tiesiogiai kelią grėsmę pinigų plovimo prevencijos rėžimui. Jei sąskaita buvo parduota, galima manyti, kad pirkėjas pasirūpino ir dokumentais, kurių ateityje gali prašyti klientas. Dėl to analizuojant kliento pateiktus duomenis svarbu atkreipti dėmesį ar pateiktuose dokumentuose yra ženklų (pvz. asmenukė yra padaryta ne pačio kliento) parodančių trečiųjų šalių dalyvavimą. Nepaisant to, siekiant nustatyti ar prie paskyros jungiasi tas asmuo, kurio tapatybė buvo patvirtinta anksčiau, paskyros autentifikavimo gali nepakakti ir to finansinės institucijos turi vertinti ir kitus duomenis. Svarbu palyginti naudojamų prietaisų, prisijungti prie paskyros, duomenis/ IP adresą ir įvertinti ar esama informacija atitinka kliento profilį. Parduotų paskyrų atveju dažnai yra statytinis (angl. „straw man“ arba „front person“). Pagal pateiktą schema (2 pav.) matyti, kaip statytinis gali būti naudojant nusikalstamos grupuotės siekiant „plauti“ pinigus gautus iš nelegalios/ nusikalstamos veiklos.



4 pav. Skaitmeninės tapatybės piktnaudžiavimas pasitelkiant statytinį

Šaltinis: FATF 2020

Atkreiptinas dėmesys į tai, kad finansinės įstaigos kliento paskyra gali būti *perduota trečiajam asmeniui* su *kliento sutikimu* arba *sąskaita gali būti netiesiogiai naudojama trečiųjų asmenų jos neužvaldant.* Tokiais atvejais tikrasis sąskaitos savininkas dažniausia tampa pinigų mulu. Pinigų mulas tai asmuo, kuris sukčiams/ nusikaltėliams leidžia naudotis savo sąskaita neteisėtoms operacijoms atlikti. Remiantis Interpolo (2022) pateikta medžiaga pinigų mulai dažniausiai yra užverbuojami pasitelkiant fiktyvius/ melagingus darbo skelbimus ar romantinį/ investicinį/ apsimetinėjimo sukčiavimo būdus. Swed bankas (2021) pasidalino istorija, kai banko klientė ieškodama darbo pakliuvo į sukčių pinkles ir

leido savo sąskaitą naudoti kaip tarpinę sąskaitą siekiant pervesti lėšas gautas iš nelegalios veiklos. Šis atvejis parodo, kad net ir nustačius kliento tapatybę ir autentifikavus vartotoja, finansinės įstaigos sąskaita gali būti panaudota pinigų plovimui.

Apibendrinant galima teigti, internetinės tapatybės atsiradimas pagerino finansinių įstaigų klientų patirtį ir suteikė didesnį prieinamumą prie banko paslaugų, tačiau tuo pačiu, finansinėms įstaigoms atsirado papildomų grėsmių. Nepaisant to, kad asmens tapatybės internete ir paskyros autentifikavimas būdai yra reglamentuoti įstatymuose, naudojami būdai yra pažeidžiami ir tai kelia grėsmes pinigų plovimo prevencijai. Išanalizuotas PPTFPĮ įstatymo dalis reglamentuojanti asmens tapatybės nustatymą kartu su finansinėse įstaigų naudojamų būdų apžvalga yra geras pagrindas atlikti kokybinį tyrimą, kurio metu bus siekiama įvertinti, Lietuvoje veikiančių finansinių įstaigų, naudojamus metodus asmens tapatybės nustatymui bei atskleisti jų keliamas grėsmės pinigų plovimo prevencijos rėžimui.

3. LIETUVOJE VEIKIANČIŲ FINANSINIŲ INSTITUCIJŲ NAUDOJAMŲ, TAPATYBĖS NUSTATYMO INTERNETE METODŲ GRĖSMĖS PINIGŲ PLOVIMO RĖŽIMUI TYRIMAS

3.1. Tyrimo metodologija

Siekiant, įvertinti Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų naudojamus tapatybės internete nustatymo metodus bei jų keliamas grėsmes pinigų plovimo prevencijos rėžimui, pasirinktas kokybinis tyrimas (kiekybinis yra naudojamas analizuoti skaičių forma pateiktus rezultatus). Teorinėje darbo dalyje nagrinėta literatūra padėjo išanalizuoti tapatybės nustatymo internete metodų patikimumą ir jų keliamas grėsmes pinigų plovimo prevencijos rėžimui. Šio darbo tiriamojoje dalyje bus atsižvelgta į realius scenarijus išryškinančius tapatybės nustatymo internete trūkumus. Išanalizuota informacija bus pasitelkta vertinant Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų tapatybės nustatymo internete ypatumus ir susijusias grėsmes pinigų plovimo prevencijos rėžimui. Vertinimo metu bus siekiama ištirti, pasirinktų Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų, naudojamų tapatybės nustatymo internete būdų patikimumą bei išanalizuoti jų keliamas grėsmes pinigų plovimo prevencijos rėžimui

Tyrimo metodai. Tyrimui atlikti bus naudojami tokie metodai:

- Informacijos, pateiktos oficialiose puslapiuose, analizė. Atsirinkus, Lietuvoje veikiančius bankus ir elektroninių pinigų įstaigas, bus siekiama įvertinti, jų naudojamus tapatybės nustatymo internete būdus, nagrinėjant informaciją pateiktą oficialiose svetainėse. Taip pat šis metodas bus naudojamas analizuojant realius scenarijus atskleidusius tapatybės nustatymo internete grėsmes pinigų plovimo prevencijos rėžimui
- Lyginamoji analizė. Teorinėje dalyje atlikta asmens tapatybės internete ir paskyros autentifikavimo būdų patikimumo bei jų keliamų grėsmių pinigų plovimo prevencijos rėžimui analizė bus lyginama su Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų naudojamais metodais ir jų keliamomis grėsmėmis. Taip pat pasirinktos finansinės institucijos bus lyginamos tarpusavyje. Visa tai leis padaryti išvadas apie Lietuvoje naudojamų tapatybės nustatymo internete būdų keliamas rizikas pinigų plovimo prevencijos rėžimui

Tyrimo problema. Kaip suvaldyti Lietuvoje veikiančių finansinių institucijų, naudojamų tapatybės nustatymo internete ir paskyrų autentifikavimo, metodų keliamas grėsmes pinigų plovimo prevencijos rėžimui

Tyrimo objektas. Lietuvoje veikiančių finansinių institucijų metodai naudojami asmens tapatybės internete patvirtinimui ir paskyros autentifikavimui

Tyrimo tikslas. Įvertinti, Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų, naudojamus metodus asmens tapatybės internete nustatymui ir paskyros autentifikavimo nustatymui bei atskleisti jų keliamas grėsmės pinigų plovimo prevencijos rėžimui.

Tyrimo uždaviniai:

1. Identifikuoti Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų, naudojamus tapatybės nustatymo internete metodus
2. Įvertinti Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų, naudojamus paskyros autentifikavimo metodus
3. Atskleisti Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų, naudojamų tapatybės nustatymo internete ir paskyrų autentifikavimo grėsmes pinigų plovimo prevencijos rėžimui

Tyrimo reprezentatyvumas. Tyrimo imties sudarymui pasirinkta tikslinė atranka. Bankai ir elektroninių pinigų institucijos, kurių metodai nustatyti asmens tapatybės internete ir paskyros autentifikavimui bus tiriami, pasirinkti pagal šiuos kriterijus

- Keturi Lietuvoje veikiantys bankai, turintis daugiausia turto (remianti Lietuvos banko duomenimis).
- Keturios elektroninių pinigų institucijos turinčios Lietuvoje elektroninių pinigų įstaigos licencijas (remiantis 2023 m. duomenimis). Įstaigos buvo pasirinktos remiantis informacijos prieinamumu ir teikiamomis paslaugomi (asmeninių sąskaitos)

Tyrimo planas. Tyrimas susideda iš trijų dalių:

1. Lietuvoje veikiančių bankų asmens tapatybės internete nustatymo ir paskyros autentifikavimo analizė
2. Lietuvoje veikiančių elektroninių pinigų įstaigų asmens tapatybės internete nustatymo ir paskyros autentifikavimo analizė
3. Netinkamo tapatybės internetu nustatymo ir paskyrų autentifikavimo keliamos grėsmės pinigų plovimo rėžimai

3.2. Lietuvoje veikiančių bankų asmens tapatybės internete nustatymo ir paskyros autentifikavimo analizė

Siekiant išanalizuoti Lietuvoje veikiančių bankų asmens tapatybės internete ir paskyros autentifikavimo būdus, buvo pasirinkti šie bankai: Swedbank AB (toliau Swedbank, AB SEB bankas (toliau SEB), Revolut Bank UAB (toliau Revolut) ir AB Šiaulių bankas (toliau Šiaulių bankas)

4 lentelė. Pasirinktų Lietuvoje veikiančių bankų, asmens tapatybės internete nustatymo būdai

Būdai	**SEB**	**Swedbank**	**Revolut**	**Šiaulių bankas**
Asmens dokumento kopija	+	+	+	-
Asmenukė	+	+	+	-
Vaizdo konsultacija	+	+	-	-
Smart ID	-	+	-	-

Šaltinis: sudaryta autorės remiantis finansinių institucijų internetiniuose puslapiuose/ aplikacijose pateikta informacija (2023)

Lentelėje (4 lentelė) pateikti pasirinktų bankų naudojami asmens tapatybės nustatymo būdai, parodo kad du bankai taikos panašias saugumo priemones, o kitu du skirtingas. Šiaulių bankas nepriima asmens tapatybę patvirtančių dokumentų ir neleidžia savo klientams atsidaryti banko sąskaitos internetu. Tokiu atveju rizika nustatant tapatybę internetu išnyksta, tačiau toks rizikos valdymas yra ne visada geriausias sprendimas. Revolut leidžia savo klientams pateikti prašomus dokumentus per mobiliąją programėlę. Tuo tarpu SEB ir Swed bankas patvirtina kliento tapatybę jam neatvykstant į banko skyrių dviem būdais – per mobiliąją programėlę pateikiami prašomi dokumentai arba užsiregistruojama į vaizdo konsultacija. Registruojantis į konsultacija SEB banke pakanka užpildyti formą ir pateikti prašomus dokumentus, tačiau Swedbankas taiko papildomą priemonę – norint užsiregistruoti į konsultaciją reikia patvirtinti tapatybę prisijungiant su Smart-iD, Mobile-ID arba ID kortele. Registracijos į konsultacija metu abu minėti bankai prašo pateikti tuos pačius dokumentus kaip ir patvirtinant tapatybę per mobiliąją programėlę.

Dėl taikoma 2FA paskyrų autentifikavimas susideda iš dviejų etapų. Remianti žemiau pateikta lentele (5 lentelė) vienintelis Revolut neprašo bankų dažnai suteikiamo naudotojo/ atpažinimo ID, vietoje to pakanka telefono numerio su kuriuo bus susieta paskyra. Visi kiti bankai prašo unikalaus naudotojo ID. Šiaulių bankas taip pat prašo suvesti, vartotojo sukurtą slaptažodį, Swedabnkas - PIN kodą

5 lentelė. Pirmas žingsnis - pasirinktų Lietuvoje veikiančių bankų, paskyros autentifikavimo būdai

Būdai	**SEB**	**Swedbank**	**Revolut**	**Šiaulių bankas**
Naudotojo ID	+	+	-	+
Asmens kodas	+	-	-	
PIN kodas	+ (jungiantis su generatoriumi)	+ (jungiantis su generatoriumi)	-	
Slaptažodis	-	-	-	+
Telefono numeris	-	+ (jungiantis su Mobile-ID	+	

Šaltinis: sudaryta autorės remiantis finansinių institucijų internetiniuose puslapiuose/ aplikacijose pateikta informacija (2023)

(jungiantis su generatoriumi) arba telefono numerį (jungiantis su mobile-ID) , SEB – asmens kodą arba PIN kodą (jungiantis su generatoriumi). Tokiuose paskyrų autentifikavimo būduose galima būtų įžvelgti pažeidžiamumų, tačiau yra naudojama papildom apsauga (2FA). Dėl to paskyrų autentifikavimo būdų pažeidžiamumą naudingiau yra vertinti antrame etape.

Antrame paskyrų autentifikavimo etape (6 lentelė) vėl išsiskiria *Revolut* nes šis bankas yra vienintelis, kuris nenaudoja Lietuvoje patvirtintų kvalifikuotų elektroninių parašų ar kodų generatoriaus, vietoj to – jungiantis per programėlę į telefoną gaunamas vienkartinis kodas, o jungiantis per internetinę bankininkystę prisijungimą patvirtinti reikia programėlėje (ji tuo metu jau apsaugot kodu). Toks būdas iš pirmo žvilgsnio atrodo nesaugus, nes sukčiams užvaldžius telefoną prisijungimas paskyra gali būti sukompromituota. Tačiau jei trečioji šalis turi prieigą prie telefono bet nežino apsauginio kodo,

6 lentelė. Antras žingsnis - pasirinktų Lietuvoje veikiančių bankų, paskyros autentifikavimo būdai

	SEB	**Swedbank**	**Revolut**	**Šiaulių bankas**
Smart ID	+	+	-	+
Mobile-ID	+	+	-	+
PIN Generatorius	+	+	-	+
PIN kortelė	-		-	+
Biometriniai duomenys	-	+	-	-
Asmens tapatybės kortelė/ USB	-	+	-	-
Programėlės kodas	-	-	+ (jungiantis per internetinę bankininkystę	-
Kodas telefone	-	-	+ (jungiantis per programėlę)	-

Šaltinis: sudaryta autorės remiantis finansinių institucijų internetiniuose puslapiuose/ aplikacijose pateikta informacija (2023)

prisijungti prie programėlės nebus taip lengvą – norint pakeisti minėtą kodą Revolut prašo patvirtinti tapatybę pateikiant asmenukę realiuoju laiku. Kiti analizuojami bankai (išskyrus SEB) siūlo dar kelis prisijungimo būdus. Įvedus Smart-ID dauguma bankų palaipsniui atsisakė PIN kodų kortelių, nepaisant to Šiaulių bankas vis dar teikia šią paskyros autentifikavimo priemonę. Tačiau nuo 2019 m. rugsėjo14 d. įsigaliojus Europos parlamento ir Tarybos deleguotajam reglamentui 2018/389, Šiaulių bankas įvedė papildomą saugomo priemonę – klientui siekiant autentifikuoti paskyrą su kodų kortelę SMS žinute bus siunčiamas vienkartinis kodas. Bankas taip pat suteikę galimybę gauti kodą susirašinėjimo programėle „Viber“. Šioje programėle visi pokalbiai/ žinutės yra pilnai užšifruoti dėl to tai leidžia šią apsaugos priemonę laikyti saugia. Apanalizuojant Swedbanko siūlomus paskyrų autentifikavimo būdus, pastebima, kad šis bankas vienintelis leidžia savo klientams patvirtini paskyrą asmens tapatybės kortele arba biometriniais duomenimis. LR tapatybės kortelė yra vienintelė atpažinties priemonė Lietuvoje, kuri yra pripažinta ES, ir tai leidžia teigti, kad toks paskyros autentifikavimas yra saugus. Norint prisijungimą

prie paskyros patvirtinti biometriniais duomenimis, antrame žingsnyje yra gaunama kontrolinis kodas Swedbanko programėlėje, kuris yra patvirtinamas piršto antspaudu arba veido atpažinimo technologija.

3.3. Lietuvoje veikiančių elektroninių pinigų įstaigų asmens tapatybės internete nustatymo ir paskyros autentifikavimo analizė

Siekiant išanalizuoti Lietuvoje veikiančių elektroninių pinigų įstaigų asmens tapatybės internete ir paskyros autentifikavimo būdus, buvo pasirinktos šios įstaigos: Paysera LT UAB (toliau Paysera), TransferGo Lithuania UAB (toliau TransferGo), Satchelpay UAB (toliau Satchelpay),Wittix

Minėtų įstaigų asmens tapatybės internete nustatymas yra beveik vienodas (žr. 7 lentelė) – visos savo klientų prašo pateigti tiesioginio perdavimo būdu padaryta asmens tapatybės dokumento kopiją asmenukę (asmenukės neprašo tik Wittix. Tuo Tarpu Satchel vietoj asmenukės vykdo kliento tapatybės

7 lentelė. Pasirinktų Lietuvoje elektroninių pinigų asmens tapatybės internete ir paskyrų autentifikavimo būdai

	Paysera	**TransferGo**	**Satchel**	**Wittix**
Asmens tapatybės internete nustatymo būdai				
Asmens dokumento kopija	+	+	+	+
Asmenukė	+	+		+
Vaizdo skambutis			+	
Adreso patvirtinimas			+	
Paskyros autentifikavimo būdai				
Telefono numeris	+	+		+
Elektroninis paštas			+	+
Slaptažodis	+	+	+	+
Vienkartinis kodas gaunamas į telefoną	+	+	+	+
Patvirtinimas per mobiliąją programėle			+ (jungiantis per internetinę bankininkystę)	

Šaltinis: sudaryta autorės remiantis finansinių institucijų internetiniuose puslapiuose/ aplikacijose pateikta informacija (2023)

patvirtinimą vaizdo skambučio metu bei adreso patvirtinančiu dokumentu. Vaizdo skambutis yra pranašesnis už asmenukę, nes pastarąja yra lengviau suklastoti. Vertinant paskyrų autentifikavimo būdus esminių skirtumų nenustatyta, nes dažniausiai prašoma elektroninio pašto adreso arba telefono numerio kartu su slaptažodžiu. 2FA yra užtikrinamas gaunant vienkartinį kodą į registruotą telefono numerį arba patvirtinant prisijungimą per mobiliąją programėlę. Verta pažymėti, kad Lietuvoje veikiančių (t.y. turinčių licenciją išduota Lietuvos banko) elektroninių pinigų įstaigų asmens tapatybės internete

nustatymas ir paskyros autentifikavimo metodai yra labai panašūs į naudojamus kitų institucijų užsiimančių ta pačia veikla

3.4. Netinkamo tapatybės internetu nustatymo ir paskyrų autentifikavimo keliamos grėsmės pinigų plovimo rėžimai

Analizuojant mokslinę ir profesinę literatūrą buvo nustatyti šios pinigų prevencijos rėžimui kylančios grėsmės kylančios iš neteisėtos paskyros atsidarymo/ naudojimo:

- Paskyra gali būti sukurta naudojanti pavogta ar netikra tapatybe;
- Piktavališkas įsilaužimas į paskyrą;
- Paskyra yra parduodama ar kitaip perleidžiama tretiesiems asmenims

Šios nustatytos rizikos bus lyginamos su 4.2 ir 4.3 skyriuose nagrinėtomis institucijomis.

Asmens tapatybės nustatymas internete tiesiogiai siejasi su *tapatybės vagyste*. Aptikus vogtą/ netikrą tapatybes iš karto užkertamas kelias, paskyrų naudojimui neteisėtiems tikslams. Šiuo atveju vienintelis Šiaulių bankas neturi valdyti pinigų plovimo rizikos susijusios su tapatybės nustatymu internete, nes jis tiesiog nenustatinėja tapatybės internetu. Nepaisant to, rizikos susijusios su netikra pavogta/ tapatybę išlieka, nes net ir tapatybės nustatymas banko skyriuose negali visiškai panaikinti žmogiškosios klaidos faktoriaus. Tuo tarpu Revolut naudojamos tapatybės nustatymo internete priemonės yra panašesnės į nagrinėtų elektroninių pinigų institucijų priemones, tai galima paaiškint tuo, kad tik 2021 m. Revolut gavo pilnaverčio banko licenciją (buvo pakeista iš specializuoto banko į banko). Nepaisant to Revolut kartu su Paysera, TransferGo, Satchel ir Wittix susiduria su panašiomis rizikomis. Kadangi nei viena iš minėtų įstaigų nenaudoje elektroninio kvalifikuoto ar saugaus parašo, jos susiduria su padidinta netikros/ pavogtos tapatybės rizika. Ypač padidėja sintetinės tapatybės ir Deepfake technologijos panaudojimo tikimybė, nes pateikti asmens duomenys nėra tikrinami su išoriniais šaltinis ir yra pasikliaujama tik automatizuota dokumentų tikrinimo sistema/ ar tai darančiai darbuotojais. Pažymėtina, kad Satchel naudojaisi keliomis papildomomis (vaizdo skambučiu ir adreso patvirtinimu) nustatyti kliento tapatybę internete ir toks veiksmas šiek tiek sumažina pavogtos/ netikros tapatybės riziką.

Lyginant SEB ir Swedbanką su kitomis nagrinėtomis įstaigomis, pastebimas akivaizdus skirtumas – šios dvi institucijos ne tik prašo pateiktis dokumentus internetu bet ir užsiregistruoti video konsultacijai. Deepfake technologijos naudojimo rizika išlieka tačiau, video konsultaciją padeda ją sumažinti. Atkreiptinas dėmesys, kad Swedbankas šiuo atveju yra pranašesnis, nes jis taip pat patvirtina asmens tapatybę su Smart-ID, o tai maksimaliai sumažina netikros/ pavogtos tapatybės riziką. Dėl gyventojų skaičiaus skirtumų, tapatybės vagystė yra labiau paplitusi Jungtinėse Amerikos

Valstijose, tačiau nereikėtų turėti klaidingo įspūdžio ir manyti, kad Lietuvoje šios rizikos nėra arba ji labai maža. Remiantis Lietuvos vartotojų (2014) instituto apklausos duomenimis, net 19 proc. Lietuvos gyventojų buvo susidūrę su asmens tapatybės vagyste.

Įvertinus tai, kad tapatybės nustatymas nuotoliniu būdu yra tiesiogiai susijęs su rizikomis kylančiomis iš netikros/ pavogtos tapatybės, būtina paminėti, kad paskyros autentifikavimas yra siejamas su rizikomis kylančiomis iš piktavališkos sąskaitos užvaldymo. Visos nagrinėtos elektroninių pinigų įstaigos ir Revolut leidžia savo vartotojams pirmą kartą prisijungti suvedant telefono numerį arba elektroninį paštą, įvedant slaptažodį ir patvirtinant 2FA su vienkartiniu kodu, gautu į registruotą telefono numerį, arba patvirtinant prisijungimą per mobiliąją programėlę. Tokie paskyrų autentifikavimo metodai atitinka standartus, bet yra labiau pažeidžiami kibernetinių atakų ir neteisėto sąskaitos užvaldymo. SEB, Swedbanko ir Šiaulių banko naudojami paskyrų autentifikavimo metodais (Smart-ID, Mobile-ID yra saugesni nei elektroninių pinigų įstaigų ir Revolut dėl įdiegtų technologinių sprendimų, kurie buvo analizuojami 2.1 skyriuje. Investavimas į saugos sistemų ir technologinius sprendimus negali apsaugoti institucijų nuo silpniausios dalies – tai yra pačio kliento. Dėl to nusikaltėliai dažnai naudoja socialinę inžineriją ir „phishing“ siekiant apgaulės būdu išvilioti visus prisijungimo duomenys. 2020 metai mokamų Google reklamų pagalba Revolut klientams buvo pateikimas netikras Revolut klientų aptarnavimo numeris, kurie paskambinę žmonės kalbėdavo su sukčiais apsimetančiais Revolut darbuotojais. Jie pasitelkia socialinės inžinerijos būdus sugebėdavo įtikinti klientus atlikti pavedimą į kitą “saugią” sąskaitą arba tiesiog išviliodavo prisijungimo duomenis. Verta paminėti, kad 2020 m. Revolut neturėjo klientų aptarnavimui skirto numerio, bet nepaisant to, klientai vis tiek sugebėjo papulti į pinkles. Šis pavyzdys tik įrodo, kad norint sumažinti neteisėtos prieigos prie paskyros, finansinės įstaigoms būtiną užsiimti edukacine veikla ir pranešti klientams apie galimas grėsmės bei kaip užtikrinti saugų elektroninės bankininkystės naudojimais. SEB banko klientai irgi yra tapę sukčių aukomis – remiantis 15min.lt straipsniu (2020), banko klientas gavo SMS žinutę su nuorodą į netikrą banko internetinės bankininkystės puslapį ir ten suvedė visus patvirtinimui reikalingus duomenis (slaptažodį, Smart-ID kodą ir pan.). Šie abu pavyzdžiai tik įrodo, kad esamos technologinės priemonės nepadeda vartotojų pasaugoti nuo socialinės inžinerijos ir kitų kibernetinių atakų. Verta pažymėti, kad paskyros saugumas taip pat dažnai priklauso ir nuo naudojamo prietaiso bei jo programinės įrangos, kurią reikia atnaujinti. Pavyzdžiu nėra paslaptis, kad Samsung telefonų gamintojas labiau orientuojasi į piršto atspaudo atpažinimo technologija, o tuo tarpų iPhone išmaniuosiuose telefonuose daugiau dėmesio skiriama veido atpažinimo sistemai. Tai įvertinus, finansinės įstaigos galėtų taikyti skirtingus reikalavimus paskyros autentifikavimui, siekiant užtikrinti kuo didesnį biometrinių duomenų tikslumą ir saugumą.

Paskyros pardavimą ar kitokį perleidimą tretiesiems asmenims neteisėta veikla, kurią finansinėms institucijoms aptikti nėra lengva. Norint suvaldyti su. Tuo susijusias rizikas, patartina imti bent vieno iš šių veiksmų:

- Pateiktų dokumentų nustatant asmens tapatybę internetu (adresą, tautybę, amžių) palyginti su paskyros autentifikavimo metu gauta informacija (IP adresas ir kiti įrenginio, naudoto prisijungti prie paskyros, duomenys). Svarbu nustatyti ar yra daugiau paskyrų besijungiančių iš to pačio prietaiso. Reiktų nepamiršti patikrinti ar klientas jungiasi iš tos pačios vietos kaip pirmąjį/ kelis pastaruosius kartus. Jei šie duomenys nesutampa, reiktų išanalizuoti ar klientas turi kokias nors sąsaja su vieta iš kurios yra jungiamai. Verta pažymėti, kad jei klientas naudoja VPN jungiantis prie paskyros, tokia analizė bus nevertinga, nes tikroji prisijungimo vieta nebus žinoma.
- Analizuoti kliento veiklą elektroninėje bankininkystėje ir nustatyti ar jo veikloje pastebimi požymiai rodantys galimą neteisėta sąskaitos naudojimai ir/ ar ženklus pastebimus pinigų plovimo atvejuose

Tokios informacijos nagrinėjimas gali padėti padaryti išvadas, tačiau norint suvaldyti riziką , kai sąskaita yra netiesiogiai naudojama trečiųjų asmenų, svarbu edukuoti klientus ir priimti jiems apie galima rizikas/ pasekmes už jų veiksmus

IŠVADOS

1. Išanalizavus Lietuvos teisės aktus ir mokslinę literatūra buvo nustatyti pagrindiniai metodai naudojami asmens tapatybės nustatymui internete (kvalifikuotas elektroninis parašas, tiesioginio vaizdo perdavimas užfiksuojant kliento veido atvaizdą ir kliento parodytą asmens tapatybės dokumento originalą) ir paskyrų autentifikavimo užtikrinimui (Smart-ID, Mobile ID, Pin kodų kortelė/generatorius, biometriniai duomenys ir LR asmens tapatybės kortelė).

2. Atliekant naudojamų tapatybės nustatymo internete metodų ir paskyrų autentifikavimo būdų veiksmingumo analizę buvo tiriami ne tik Lietuvoje bet ir užsienyje (Danijoje ir Jungtinėje Karalystėje) naudojami būdai. Ši analizė leido išskirti šias, aukščiausius standartus atitinkančias, priemones: MitID (Danija), Smart-ID, Mobile-ID ir LR asmens tapatybės kortelė. Analizuojant biometrinius duomenis buvo nustatytą, kad jų saugumo patikimumas priklauso nuo naudojamų įrenginių, nes biometriniai duomeny yra saugomi juose.

3. Tiriant pinigų plovimo prevencijos rėžimo grėsmes kylančias iš neteisėtos sąskaitos atsidarymo/ naudojimo, buvo išskirtos trys: (1) paskyros sukūrimas naudojantis pavogta ar netikra tapatybe, (2) piktavališkas įsilaužimas į paskyrą, (3) paskyra pardavimas ar kitoks perleidimas tretiesiems asmenims. Tapatybės vagystės ar netikrų dokumentų pateikimas budo išskirtas į dvi rūšis: apsimetinėjimas kitu asmeniu ir sintetinė tapatybė. Kaip viena iš pagrindiniu susijusi š grėsmių buvo iškirsta sparčiai besivystanti „Deepfake“ technologija Buvo pastebėta, kad neteisėtas sąskaitos perėmimas/ įsilaužimas dažniausiai susijęs su kibernetinėmis atakomis ir pagrindiniu finansinių įstaigų pažeidžiamumu – klientu. Paskyros pardavimas ar kitoks perleidimas buvo susietas su keliais faktoriais: statytinio naudojimu (sąskaitos atidaromos ir perduodamos su tikrojo savininko sutikimu), pinigų mulu (naudojamas kaip papildomas sluoksnis paslėpti tikrąją pinigų kilmę) asmens su ir pradžioje patikliu asmeniu (dažniausiai sukčių auka, kuri neįtaria kad jos veiksmai sąskaitoje yra susiję su nelegalia veikla).

4. Pagrindiniai Lietuvos bankai naudoja užtikrintas saugumo priemones (pvz. sertifikuotas elektroninis parašas“ tačiau tirtos elektroninių pinigų įstaigos ir neseniai banku tapęs Revolut naudoja mažiau saugias priemones (tačiau atitinkančias reikalavimus) tokias kaip vartotojo vardas/ telefono numeri, slaptažodis ir vienkartinis patvirtinimo kodas gaunamas į registruotą telefono numerį. Vertinant Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų naudojamus tapatybės patvirtinimo internete ir paskyrų autentifikavimo būdus, buvo išskirtos tos pačios rizikos pinigų plovimo rėžimui: (1) paskyros sukūrimas naudojantis pavogta ar netikra tapatybe, (2) piktavališkas įsilaužimas į paskyrą, (3) paskyra pardavimas ar kitoks perleidimas

tretiesiems asmenims. Realūs pavyzdžiai ir nuketėjusiųjų istorijos parodė, kad nors Lietuva ir yra nedaug gyventojų turinti šalis, išskirtos grėsmės yra realios

5. Įvertinus technologinius sprendimus slypinčiu už kiekvieno nagrinėto tapatybės internete nustatymo ir paskyros autentifikavimo metodų patikimiausiu buvo pripažintas Danijoje naudojamas sprendimas – MitID. Technologija slypinti šios sistemos viduje atitinka aukščiausius eIDAS standartus ir dėl to MityID yra pripažįstama ES kaip aukšto lygio elektroninės atpažinties priemonė.

PASIŪLYMAI

- Nuolat atidžiai stebėti besikeičiančias technologijas ir įvertinti su jomis susijusias saugumo grėsmes. Keičiantis technologijoms patartina atnaujinti bankuose naudojamas tapatybės patvirtinimo internetu ir paskyrų autentifikavo
- Finansinės institucijos norėdamos pasisaugoti nuo klientų paskyrų užgrobimo turėtų ne tik taikyti technologinius sprendimus ,bet ir investuoti į žmonių edukaciją kibernetinio saugumo ir skatinti skaitmeninį raštingumą
- Skatinti asmenis palaikyti skaitmeninę higieną, taip užkertant kelią naudojamų prietaisų sukompromitavimui
- Šio darbo tyrimas atskleidė tapatybės patvirtinimo internetu ir paskyrų autentifikavimo keliamas grėsmes pinigų plovimo rėžimui, tačiau patartina nesustoti ir toliau nagrinėti šia tema. Kituose tiriamojo pobūdžio darbuose siūloma nagrinėti vieną iš dviejų temų:

  (1) automatinių sistemų tvirtinančių dokumentus naudojamus tapatybei nustatyti analizė. Siūloma pasirinkti kelias pagrindines sistemas ir išanalizuoti naudojamą mechanizmą, bei pasiūlyti jo tobulinimo būdų

  (2) „Deepfake“ technologijos analizė siekiant ištirti šią sistemą ir pasiūlyti techninį sprendimą padėsiantį nustatyti šios technologijos panaudojimo atvejus.

LITERATŪROS SARAŠAS

1. All About Cookies (n. d.). Which Cell Phone Is Most Secure in 2023? iPhone vs. Android. Prieiga per internetą: https://allaboutcookies.org/android-security-vs-ios#:~:text=Android%20phones%20are%20generally%20considered,target%20it%20presents%20to%20hackers.
2. Apple Inc (n.d.). About Face ID advanced technology. Prieiga per internetą: https://support.apple.com/en-us/HT208108#:~:text=Security%20safeguards&text=Face%20ID%20uses%20the%20TrueDepth,only%20to%20the%20Secure%20Enclave
3. Apple Inc (n.d.). About Touch ID advanced security technology. Prieiga per internetą: https://support.apple.com/en-us/HT204587#:~:text=Your%20fingerprint%20data%20is%20encrypted,matches%20the%20enrolled%20fingerprint%20data
4. Ashu Agrahar, (2022). Samsung to make fingerprint login 2.5bn times more secure in 2025. Prieiga per internetą: https://r2.community.samsung.com/t5/Tech-Talk/Samsung-to-make-fingerprint-login-2-5bn-times-more-secure-in/td-p/12684590
5. Barclays Bank UK PL, (n.d.). How to apply online for a current account. Prieiga per internetą: https://www.barclays.co.uk/help/accounts/opening/how-to-open-an-account-online/
6. Basel Committee on Banking Supervision (2012). Core Principles for Effective Banking Supervision. Prieiga per internetą: https://www.bis.org/publ/bcbs230.pdf
7. Bogdan Petrovan, (2019). Friendly reminder: Biometrics are not the best way to secure your phone. Prieiga per internetą: https://www.androidauthority.com/fingerprints-insecure-phone-1043477/
8. Cam Bunton, (2023). In-display fingerprint readers: How they work plus optical vs ultrasonic. Prieiga per internetą: https://www.pocket-lint.com/in-display-fingerprint-readers-how-do-they-work/
9. Coppolino, L., D'Antonio, S., Formicola, V., Massei, C., & Romano, L. (2015). Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. *Journal of Ambient Intelligence and Humanized Computing*, *6*(6), 753–762. Prieiga per internetą: https://link-springer-com.hallam.idm.oclc.org/article/10.1007/s12652-015-0276-9
10. Dabartinės lietuvių kalbos žodynas. Taptybė. Prieiga per internetą: http://www.lkz.lt/?zodis=tapatyb%C4%97&id=26012680000
11. Dauparaitė, Inga, Laurinaitis, Marius, & Pakutinskas Paulius. (2011). *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai: kolektyvinė*

mokslo monografija. Mykolo Romerio universitetas. Prieiga per internetą: https://repository.mruni.eu/handle/007/16821

12. Europos Parlamentas ir Europos Sąjungos taryba, (2014). Reglamentas (ES) Nr. 910/2014 2014 m. liepos 23 d. dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32014R0910
13. Europos Parlamentas ir Europos Sąjungos taryba, (2017). Komisijos deleguotasis reglamentas (ES) 2018/389 2017 m. lapkričio 27 d. kuriuo Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 papildoma griežto kliento autentiškumo patvirtinimo ir bendrų ir saugių atvirųjų ryšių standartų techniniais reguliavimo standartais. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32018R0389
14. Europos Parlamentas ir Europos Sąjungos taryba, (2020). Elektroninės atpažinties schemos, apie kurias pranešta pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje (1) 9 straipsnio 1 dalį. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020XC0821(01)&qid=1599046662977&from=EN
15. Financial Action Task Force (2023). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations. Prieiga per internetą: https://www.fatf-gafi.org/content/dam/fatf-gafi/Recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf
16. Handelsblatt GmbH, (2018) Bafin initiates an examination for counterfeit IDs. Prieiga per internetą: https://www.wiwo.de/unternehmen/banken/sicherheitsmaengel-bei-n26-bafin-leitet-wegen-gefaelschter-ausweise-pruefung-ein/23175098.html
17. Hitt, & Frei, F. X. (2002). Do Better Customers Utilize Electronic Distribution Channels? The Case of PC Banking. Management Science, 48(6), 732–748. https://www-emerald-com.hallam.idm.oclc.org/insight/content/doi/10.1108/02652329810228190/full/html
18. Hitt, L. M., & Frei, F. X. (2002). Do Better Customers Utilize Electronic Distribution Channels? The Case of PC Banking. *Management Science*, *48*(6), 732–748. Prieiga per internetą: https://www.jstor.org/stable/822626
19. Hooyu Ltd, (n.d.). As more fake ID documents are sold online is it time to complement ID document validation with new Reg-Tech? Prieiga per internetą: https://www.hooyu.com/h/as-more-fake-id-documents-are-sold-online-is-it-time-to-complement-id-document-validation-with-new-reg-tech/

20. https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
21. Įsakymas dėl techninių reikalavimų kliento tapatybės nustatymo procesui, kai tapatybė nustatoma nuotoliniu būdu, naudojantis elektroninėmis priemonėmis, leidžiančiomis tiesioginio vaizdo perdavimą, patvirtinimo. 2016 m. lapkričio 30 d. Nr. V-314. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr
22. Lietuvos bankų asociacija (2022). Tyrimas: elektronine bankininkyste naudojasi 90 proc. Šalies gyventojų. Prieiga per internetą:https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/tyrimas-elektronine-bankininkyste-naudojasi-90-proc-salies-gyventoju
23. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. 1996 m. birželio 11 d. Nr. I-1374. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/JYEMsuFtbP
24. Lietuvos Respublikos elektroninių pinigų įstaigų įstatymas 2011 m. gruodžio 22 d. Nr. XI-1868. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.40DFB5151B33/asr
25. Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas. 1997 m. birželio 19 d. Nr. VIII-275. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.C44837068B55/asr
26. Lietuvos Respublikos ryšių reguliavimo tarnyba (n.d). Patarimai, kaip saugiai naudotis. Prieiga per internetą: https://www.esaugumas.lt/articles/patarimai-kaip-saugiai-naudotis
27. Lietuvos R*espub*likos vidaus reikalų ministerija (2023, kovo 23 d.). Svarbi informacija! Prieiga per internetą: https://www.nsc.vrm.lt/default.htm
28. Lietuvos Respublikos vidaus reikalų ministerija (n.d). Lietuvos Respublikos asmens tapatybės kortelė. Prieiga per internetą: https://eid.lt/lt/apie-tapatybes-kortele/lietuvos-respublikos-asmens-tapatybes-kortele
29. Lloyds Bank,(n.d.). Current Account. Prieiga per internetą: https://www.lloydsbank.com/current-accounts.html
30. MitID, (n.d.). Read more about how MitID enhances security Prieiga per internetą: https://www.mitid.dk/media/hcjevl0z/om-mitid_baggrund_v1-03.pdf
31. Ogbanufe, O.M., Baham, C. Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret. Inf Syst Front 25, 897–916 (2023). https://doi-org.hallam.idm.oclc.org/10.1007/s10796-022-10278-1
32. Paysera LT, UAB (2022, Vasaris). Kuo skiriasi Paysera mobilioji programėlė ir internetinė bankininkystė? Prieiga per internetą: https://www.paysera.lt/v2/lt-LT/blog/programele-ar-internetine-bankininkyste

33. Parker, T., Parker, M. (2008). Electronic banking in Finland and the effect on money velocity. Journal of money, investment, and banking. Prieiga per internetą: https://www.researchgate.net/publication/276908071_Electronic_banking_in_Finland_and_the_effect_on_money_velocity/citation/download
34. Paul Bischoff, Comparitech (2022). Which countries have the worst (and best) cybersecurity? Prieiga per internetą: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/#Our_methodology_how_did_we_find_the_countries_with_the_worst_cybersecurity
35. Republic of Estonia Information System Authority, (n.d). The Privacy Policy of id.ee. Prieiga per internetą: https://www.id.ee/en/plugins/
36. Revolut Bank, UAB (2023, balandžio 17 d.). Privatiems klientams taikomos sąlygos. Prieiga per internetą: https://www.revolut.com/lt-LT/legal/terms/
37. Samsung (n.d.) Use Facial recognition security on a Galxy phone or tablet. Prieiga per internetą: https://www.samsung.com/us/support/answer/ANS00062630/#:~:text=Make%20sure%20you%20are%20in,(such%20as%20a%20twin)
38. Samsung for Business, (2021). Which biometric authentication method is most secure? Prieiga per internetą: https://insights.samsung.com/2021/05/25/which-biometric-authentication-method-is-most-secure-3/
39. Santander UK plc, (n.d.). Customer identification requirements for UK residents. Prieiga per internetą: https://www.santander.co.uk/assets/s3fs-public/documents/customer_identification_requirements_do-ec-368.pdf
40. SEB bankas, AB (2020). https://www.seb.lt/naujienos/2020-09-14/seb-kviecia-pasitikrinti-ar-neikliutumet-finansiniams-sukciams
41. SEON Technologies Ltd (2023). Guide to Account Takeover (ATO) Fraud Detection & Prevention. Prieiga per internetą: https://seon.io/resources/guides/account-takeover-fraud-prevention-and-detection/
42. SK ID Solutions, AS (2022). Terms and Conditions for Use of Certificates of Mobile-ID. Prieiga per internetą: https://www.skidsolutions.eu/upload/files/SK-TCU-MID-EN-CURRENT.pdf
43. SK ID Solutions, AS (n.d). Dažniausiai užduodami klausimai: Kaip yra apsaugoti mano raktai? Prieiga per internetą https://www.smart-id.com/lt/pagalba/duk/sauga/kaip-yra-apsaugoti-mano-raktai
44. SK ID Solutions, AS (n.d). Skaitmeniniai parašai, naudojant „Smart-ID“. Prieiga per internetą: https://www.smart-id.com/lt/elektroniniu-paslaugu-teikejams/smart-id-kaip-qscd/
45. Sodžiūtė, L., Sūdžius, V. (2006). Elektroninis verslas: pardavimas ir finansinės priemonės. Vilnius: Kronta

46. Swedbank, AB (2016). Rekordinis mobiliosios bankininkystės šuolis. Prieiga per internetą: https://blog.swedbank.lt/asmeniniai-finansai/rekordinis-mobiliosios-bankininkystes-suolis
47. Swedbank, AB (n.d). Prisijungimo priemonės. Prieiga per internetą: https://www.swedbank.lt/private/d2d/ebanking/authentication?language=LIT
48. The Hongkong and Shanghai Banking Corporation Limited (HSBC) ,(n.d.). Open an HSBC Bank Account Online with your mobile. Prieiga per internetą: https://www.hsbc.com.hk/ways-to-bank/mobile-apps/banking/account-opening/#:~:text=Open%20your%20account%20in%203,to%20opening%20your%20HSBC%20account
49. Tsai, C.-H., & Su, P.-C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. Information Systems and e-Business Management, 19(1), 77–105. Prieiga per internetą: https://link-springer-com.hallam.idm.oclc.org/article/10.1007/s10257-020-00481-5
50. UAB „Credit Service" (2023). Tapatybės patvirtinimas. Prieiga per internetą: https://www.vivus.lt/kaip-pasiskolinti/tapatybes-patvirtinimas
51. UAB „Profitus. UAB sutelktinio finansavimo platformos „Profitus“ vidaus kontrolės procedūrų, kuriomis siekiama užkirsti kelią pinigų plovimui ir (ar) teroristų finansavimui, tvarka. Prieiga per internetą: https://www.profitus.lt/files/dokumentai/AML_tvarka.Profitus.pdf
52. V. D. v institucija (Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Pinigų plovimo prevencijos valdybos), BYLA A8.-5463-827/2017. Vilniaus miesto apylinkės teismas. Prieiga per internetą: https://eteismai.lt/byla/66285374280953/A8_-5463-827/2017
53. Vilius Petkauskas (2022). Deepfakes are scary good at bypassing remote identification. Prieiga per internetą: https://cybernews.com/security/deepfakes-are-scary-good-at-bypassing-remote-identification/
54. Wise Payments Limited (2023). Guide to getting verified. Prieiga per internetą: https://wise.com/help/articles/2949782/guide-to-getting-verified?origin=related-article-3lclMmfpEuLXpf6uEkbhaL

Daubaraitė I. (2023). Asmens tapatybės nustatymas internete: grėsmės pinigų plovimo rėžimui (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe analizuojamos asmens tapatybės nustatymo internete ir paskyrų autentifikavimo priemonės, bei jų keliamos rizikos pinigų plovimo prevencijos rėžimui. Atlikta lyginamoji analizė parodė, kad Lietuvoje finansinių institucijų naudojamos priemonės kelia tas pačias rizikas pinigų plovimo rėžimui, kai ir užsienyje. Pirmoje darbo dalyje nagrinėjama elektroninės bankininkystės rūšys, kliento tapatybės nustatymo internete ir vartotojo paskyros autentifikavimo būdai. Antroje dalyje analizuojamas finansinių įstaigų naudojamų, tapatybės nustatymo internete ir paskyros autentifikavimo būdai. Pateikiam atvejo analizė analizuojant Danijos karalystės, Jungtinės Karalystės bankų ir ne Lietuvoje registruotų elektroninių pinigų įstaigų naudojamų būdų patikimumą. Trečioje dalyje nagrinėjamos, asmens tapatybės internete ir paskyrų autentifikavimo būdų, keliamos grėsmės pinigų plovimo prevencijos rėžimui. Ketvirtoje dalyje atliekamas tyrimas išsiaiškinti Lietuvoje veikiančių finansinių įstaigų naudojamų, tapatybės nustatymo internete ir paskyrų autentifikavimo būdų, grėsmės pinigų plovimo rėžimui. Tyrime išvadose yra pasiūlomas saugiausias iš nagrinėtų būdų kuris galėtų būti pritaikytas Lietuvoje

Daubaraitė I. (2023). Identity Verification Online: Threats to the Anti Money Laundering Regime (master thesis) Vilnius: Mykolas Romeris University

ANNOTATION

The master thesis analysed online identification and account authentication methods, as well as the risks they pose to the money laundering prevention regime. Conducted comparative analysis showed that methods used by financial institutions in Lithuania and abroad pose the same risks to the anti money laundering regime. The first part of the work examines types of electronic banking, online verification and account authentication methods. The second part analyzes online identification and account authentication methods used by financial institutions. Case study analysing the reliability of tools used by banks in the Kingdom of Denmark, the United Kingdom and electronic money institutions registered outside Lithuania. The third part examines the tools of identity verification online and account authentication, and their threats to the money laundering prevention regime. In the fourth part, research is carried out to find out the methods of online identification and account authentication used by financial institutions operating in Lithuania, and their threats to the money laundering regime. In the conclusions of the research, the safest of the examined methods is proposed, which could be applied in Lithuania.

Daubaraitė I. (2023). Asmens tapatybės nustatymas internete: grėsmės pinigų plovimo rėžimui (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Magistrinio baigiamasis darbo tikslas – remiantis literatūra bei teisiniais dokumentais, išanalizuoti Lietuvoje veikiančių bankų ir elektroninių pinigų įstaigų naudojamus metodus, asmens tapatybės nustatymui internetu ir paskyrų autentifikavimui, ir nustatyti jų keliamas grėsmes pinigų plovimo prevencijos rėžimui.

Bankininkystei persikėlus į elektroninę erdvę bankai pradėjo teikti savo paslaugas per internetinę ir mobiliąją bankininkystes. Tai pagerino vartotojų pasitenkinimą, nes paslaugos tapo labiau prieinamos ir greičiau pasiekiamos. Tačiau bankams toks perėjimas prie elektroninės bankininkystės sukėlė ir nemažai iššūkiu, nes teko pasirūpinti klientų tapatybės patvirtinimu internetu bei paskyrų autentifikavimu. Šie saugumo iššūkiai kelia grėsmę ne tik, bankų reputacijai ir pinigų plovimo prevencijos režimui. Magistriniame darbe, remiantis mokslinių šaltinių analize, kitų šalių patirtimi ir kokybiniu tyrimu atliktu Lietuvove veikiančių bankų ir elektroninių pinigų tinklapiuose pateikta informacija bus aptartas mažai analizuota probleminė vieta – tapatybės nustatymo internete ir paskyrų autentifikavimo metodu keliamos grėsmės pinigų plovimo rėžimui.

Darbe taikytas mokslinės literatūros, dokumento turinio, teisės aktų, oficialiuose finansinių įstaigų/ institucijų puslapiuose pateiktos informacijos bei lyginamojo duomenų analizė. Magistriniame darbe siekiant išsiaiškinti elektroninės bankininkystės rūšis ir jų įtaką tapatybės patvirtinimui internete, buvo taikyta mokslinės literatūros analizė. Statistinių duomenų analizės metodas buvo taikomas siekiant pasirinkt dvi šalis (Danijos Karalystę ir Jungtinę Karalystę). Pasirinkus atvejo analizės metodą buvo siekiant išskirti atrinktų šalių naudojamus tapatybės nustatymo internete ir paskyrų autentifikavimo metodus, kuriuos vėliau palyginti su Lietuvoje naudojamais. Kokybinis tyrimas buvo pasirinktas siekiant išanalizuoti oficialiuose finansinių įstaigų puslapiuose pateiktą informaciją. Tyrimo metu buvo siekta įvertinti, pasirinktų įstaigų naudojamus metodus asmens tapatybės internete nustatymui ir paskyros autentifikavimui bei atskleisti jų keliamas grėsmės pinigų plovimo prevencijos rėžimui.

Magistro darbą sudaro keturios dalys. Pirmojoje darbo dalyje nagrinėjami elektroninės valdžios. Pirmoje darbo dalyje nagrinėjama elektroninės bankininkystės rūšys, kliento tapatybės nustatymo internete ir vartotojo paskyros autentifikavimo būdai. Antroje dalyje analizuojamas finansinių įstaigų naudojamų, tapatybės nustatymo internete ir paskyros autentifikavimo būdai. Pateikiam atvejo analizė analizuojant Danijos karalystės, Jungtinės Karalystės bankų ir ne Lietuvoje registruotų elektroninių

pinigų įstaigų naudojamų būdų patikimumą. Trečioje dalyje nagrinėjamos, asmens tapatybės internete ir paskyrų autentifikavimo būdų, keliamos grėsmės pinigų plovimo prevencijos rėžimui. Ketvirtoje dalyje atliekamas tyrimas išsiaiškinti Lietuvoje veikiančių finansinių įstaigų naudojamų, tapatybės nustatymo internete ir paskyrų autentifikavimo būdų, grėsmės pinigų plovimo rėžimui. Tyrime išvadose yra pasiūlomas saugiausias iš nagrinėtų būdų kuris galėtų būti pritaikytas Lietuvoje

Daubaraitė I. (2023). Identity Verification Online: Threats to the Anti Money Laundering Regime (master thesis) Vilnius: Mykolas Romeris University

SUMMARY

The aim of this master thesis is to analyze the methods used by banks and electronic money institutions operating in Lithuania for online identification and account authentication. Based on academic literature and legal documents, threats to money laundering prevention regime will be identified.

As traditional banking moved to the electronic space, banks began to provide their services through online and mobile banking. Users satisfaction was increased by making services more accessible and faster. However, such a transition to electronic banking also created a number of challenges for banks, as they had to take care of online identification and account authentication. These security challenges threaten not only the reputation of banks and the money laundering prevention regime. In this master's thesis, the problematic topic of threats posed by the method of online identification and account authentication to the money laundering regime will be discussed. Discussion will be based by several research method such as analysis of scientific sources, the experience of other countries and the qualitative research carried out on the information provided on the websites of banks and electronic money operating in Lithuania.

The work used the analysis of scientific literature, document content, legal acts, information provided on the official pages of financial institutions/institutions, and comparative data analysis. Master thesis used the analysis of scientific literature to find out the types of electronic banking and their influence on online identification. The statistical data analysis method was applied to select two countries (Kingdom of Denmark and United Kingdom). The aim of choosing the case analysis method was to distinguish the online identification and account authentication methods used by the selected countries. Later this data was compared with methods used in Lithuania. A qualitative study was chosen to analyze the information provided on the official websites of financial institutions. Aim of the research was to evaluate the selected institutions, their methods used for online identification and account authentication, and to reveal the threats they pose to the money laundering prevention regime.

The master's thesis consists of four parts. The first part of the work examines the types of electronic banking, online identification and account authentication methods. The second part analyzes the online identification and account authentication methods used by financial institutions. We present a case study

analyzing the reliability of methods used by banks in the Kingdom of Denmark, the United Kingdom, and electronic money institutions not registered in Lithuania. The third part examines the methods of online identification and account authentication and identities and identifies threats to the money laundering prevention regime. In the fourth part, research is carried out to find out the methods of online identification and account authentication used by financial institutions operating in Lithuania and the threats to the money laundering regime. In the conclusions of the research, the safest of the examined methods is proposed, which could be applied in Lithuania.