VILNIUS TECH
Vilniaus Gedimino technikos universitetas

26-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“ teminė konferencija
Proceedings of the 26th Conference for Junior Researchers “Science – Future of Lithuania”

EKONOMIKA IR VADYBA / ECONOMICS AND MANAGEMENT

eISSN 2029-7149
2023 m. spalio 17 d., Vilnius, Lietuva
17 October 2023, Vilnius, Lithuania
eISBN 978-609-476-343-4
Straipsnio Nr.: vvf.2023.027

Finansų valdymas / Financial Management
https://vilniustech.lt/jmk-vvf

PINIGŲ PLOVIMO ATPAŽINIMO TYRIMAS NAUDOJANT SKAITMENINĮ INTELEKTĄ

Akvilė EREMINĖ*, Nijolė MAKNICKIENĖ

[1]*Vilniaus Gedimino technikos universitetas, Verslo vadybos fakultetas,*
Saulėtekio al. 11, LT-10223 Vilnius, Lietuva
**El. paštas akvile.eremine@stud.vilniustech.lt*

Gauta 2023-02-20; priimta 2023-06-15

Santrauka. Pinigų plovimo prevencija, siekiant atpažinti ir laiku sustabdyti šią nusikalstamą veiklą, vis dar išlieka viena aktualiausių temų globaliu mastu. Didelis duomenų kiekis, susijęs su pinigų plovimo reikalavimų laikymusi, ir didėjantis nusikalstamų metodų sudėtingumas verčia finansų įmones ieškoti naujų priemonių, kurios padėtų įvykdyti reguliavimo įsipareigojimus. Siekiant šio tikslo technologijos, kurių veikimas paremtas dirbtiniu intelektu, tampa neatsiejamos nuo pinigų plovimo prevencijos. Šiame straipsnyje pagrindžiama pinigų plovimo tikroji kaina pasaulinei ekonomikai. Tyrimo tikslas – įvertinti skaitmeninio intelekto pritaikymo svarbą pinigų plovimo prevencijoje. Šiam tikslui pasiekti buvo lyginamos skirtingos technologijos, taikomos finansiniam sukčiavimui atpažinti. Ypatingas dėmesys šiame straipsnyje skiriamas dirbtinio intelekto pogrupiui skaitmeninio intelekto ir mašininio mokymosi metodams. Remiantis naujausiais moksliniais tyrimais, šių technologijų derinys leidžia numatyti ateities įvykius, sukurti tinkamas taisykles, priimti tikslingus sprendimus, komunikuoti su tiksline auditorija. Dirbtinio intelekto svarbą pinigų plovimo prevencijoje pabrėžia straipsnyje analizuojamas tyrimas, kuriame buvo apklausiami aukščiausio lygio vadovai, atsakingi už pinigų plovimo prevenciją. Respondentai išreiškė vienbalsę nuomonę, jog tolesnis dirbtinio intelekto taikymas pinigų plovimo prevencijos srityje yra prioritetas. Tačiau sykiu tyrimo rezultatai identifikavo respondentų įvardytas grėsmes, dėl kurių praktiškai dirbtinio intelekto metodai veikloje taikomi vangiai.

Reikšminiai žodžiai: pinigų plovimas, dirbtinis intelektas, skaitmeninis intelektas.

Įvadas

Pinigų plovimo prevencija, siekiant atpažinti šį finansinį nusikaltimą, vis dar išlieka viena aktualiausių temų globaliu mastu įmonėms, vykdančioms finansines operacijas, įskaitant bankus, finansų technologijų įmones, kriptovaliutų prekybos įmones ir kitas šio sektoriaus įmones. Šį faktą sustiprina tai, jog, 2021 metų duomenimis, Bazelio pinigų plovimo rizikos indeksas padidėjo nuo 5,22 iki 5,3 dešimtiems balų sistemoje (Basel Institute on Governance, 2021). Taip pat, remiantis naujausiais Jungtinių Tautų duomenimis, apskaičiuota, jog kasmet išplaunama nuo 800 bilijonų iki 2 trilijonų dolerių, o tai sudaro nuo 2 proc. iki 5 proc. viso pasaulio BVP (United Nations, 2022). Siekdami kovoti su pinigų plovimo problema, bankai ir kitos finansų sektoriaus įmonės įpareigotos stebėti, įvertinti ir praneši apie įtariamą pinigų plovimą. Didelis duomenų kiekis, susijęs su pinigų plovimo reikalavimų laikymusi, ir didėjantis nusikalstamų metodų sudėtingumas verčia finansų įstaigas nuolat ieškoti naujų priemonių, kurios padėtų įgyvendinti reguliavimo įsipareigojimus. Siekiant šio tikslo, technologijos, kurių veikimas paremtas dirbtiniu intelektu, tampa neatsiejamos nuo pinigų plovimo prevencijos. Tai pagrindžiama prognozėmis, jog pasaulinė kovos su pinigų plovimu įrankių rinka nuo 2020 m. iki 2025 m. augs 15,6 proc., vadinasi, nuo 2,2 mlrd. USD 2020 m. iki 4,5 mlrd. USD 2025 m. (Anti-money Laundering Market, 2022).

Tyrimo problema – kaip, naudojantis skaitmeniniu intelektu, sukurti įrankiai gali būti pritaikomi pinigų plovimui atpažinti?

Tyrimo objektas – skaitmeninio intelekto metodai.

Tyrimo tikslas – išanalizuoti skaitmeninio intelekto modelių pritaikymo galimybes pinigų plovimui atpažinti.

Tyrimo uždaviniai:

1. Pagrįsti tikrąją pinigų plovimo prevencijos kainą pasaulinėje ekonomikoje.

2. Apibrėžti skaitmeninio intelekto sampratą ir pranašumą prieš kitas technologijas.
3. Palyginus moksliniuose tyrimuose taikomus skaitmeninio intelekto metodus, kurie galėtų būti pritaikyti pinigų plovimui atpažinti, identifikuoti tinkamiausius metodus.

Tyrimo metodai: mokslinės literatūros analizė, lyginamoji analizė, aprašomoji analizė, duomenų aprašymas.

1. Pinigų plovimo samprata

Pinigų plovimo (angl. *Money Laundering*) reiškinys pirmą kartą užfiksuotas JAV 1980 m. pabaigoje, kai buvo pastebėtas didesnis nei įprastai narkotikų ir iš jų gaunamų pajamų srautų augimas. Pinigų plovimas buvo siejamas su procesu, kai nelegaliai gautos pajamos buvo verčiamos legaliomis (Georgieva, 2020). Šio proceso metu slepiama neteisėtų pajamų kilmė, neteisėtos pajamos naudojamos ir maskuojamos, kad atrodytų teisėtos. Ekonomistė Vainienė (2008) paantrina, kad paprastai pinigai plaunami vykdant sudėtingas pinigines operacijas, kuriomis siekiama paslėpti tikrąją pinigų kilmę ir dažniausiai grynuosius pinigus paversti negrynaisiais (Zhang & Trubey, 2018).

Tokia neteisėta veikla, pasak Unger (Under et. al., 2006), turi ne mažiau kaip aštuoniolika skirtingų pinigų plovimo sąvokų apibrėžčių. Šis faktas įrodo šios nusikalstamos veiklos nagrinėjimo aktualumą įvairiose srityse. 1 lentelėje pateiktos oficialios teisinėje veikloje vartojamos pinigų plovimo sąvokų apibrėžtys.

Apibendrinant pinigų plovimo sąvokų analizę, išskirtini keli aspektai. Pirma, tiek analizuoti autoriai, tiek teisės aktai pabrėžia tai, jog pinigų plovimas yra neteisėtu būdu gauti pinigai. Antra, šis reiškinys dažnu atveju įvardijamas kaip procesas, tai reiškia, kad jis yra sudėtingas, daugiasluoksnis veiksmas. Trečia, šia nusikalstama veikla siekiama nuslėpti neteisėto turto kilmę arba padėti bet kokiam nusikalstamoje veikoje dalyvaujančiam asmeniui išvengti atitinkamai teisinių tokios nusikalstamos veikos pasekmių.

2. Tikroji pinigų plovimo kaina pasaulinei ekonomikai

Tikrosios pinigų plovimo kainos ir masto nustatyti neįmanoma dėl kelių priežasčių, kurias įvardija Pol (2020).

Pinigų plovimą ypač sunku nustatyti dėl šių toliau išvardytų veiksnių:

1) dėl pinigų plovimo proceso daugiasluoksniškumo;
2) dėl nuolat kintančių nusikaltėlių vykdomų schemų, kurias nusikaltėliai naudoja siekdami apeiti esamus reguliavimo mechanizmus ir atitikties procesus;
3) dėl išaugusio duomenų srauto finansų institucijų paslaugoms persikėlus į skaitmeninę erdvę, dėl šios situacijos finansų įstaigos priverstos ieškoti naujų technologijų duomenims apdoroti;
4) dėl finansų institucijų reguliavimo ir nuolatinio lenktyniavimo tarpusavyje, siekiant sukurti reguliavimo ir atitikties metodus, kurių taikymo sritis būtų plati, naujoviška ir veiksminga, kad būtų galima stebėti ir prireikus laiku sustabdyti neteisėtą veiklą.

Šiuolaikinė kova su pinigų plovimu yra iš esmės neveiksminga (Pol, 2020; Economist, 2021). Finansinės atskaitomybės, skaidrumo ir sąžiningumo komisija (FACTI) – su Jungtinėmis Tautomis (toliau – JT) susijusi institucija, kurios tikslas – pasiekti tvarų vystymąsi kovojant su finansiniais nusikaltimais – apskaičiavo, kad

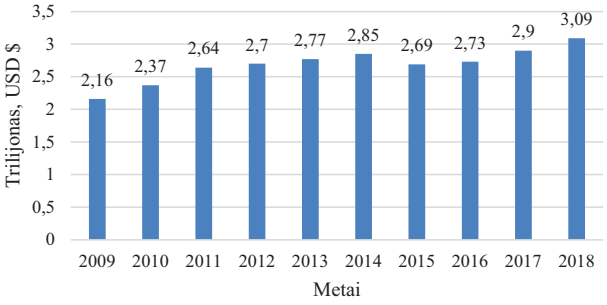
1 lentelė. Pinigų plovimo sampratos teisinės sąvokos

Autorius ir metai	Sąvokos paaiškinimas
Lietuvos Respublikos pinigų plovimo prevencijos įstatymas, 2021	1) turto teisinės padėties pakeitimas arba turto perdavimas žinant, kad šis turtas yra gautas iš nusikalstamos veikos arba dalyvaujant tokioje veikoje, siekiant nuslėpti arba užmaskuoti neteisėtą turto kilmę arba siekiant padėti bet kokiam nusikalstamoje veikoje dalyvaujančiam asmeniui išvengti teisinių šios veikos pasekmių; 2) turto tikrojo pobūdžio, tikrosios kilmės, šaltinio, vietos, disponavimo, judėjimo, nuosavybės ar kitų su nuosavybe susijusių teisių nuslėpimas arba užmaskavimas žinant, kad šis turtas yra gautas iš nusikalstamos veikos arba dalyvaujant tokioje veikoje; 3) turto įgijimas, valdymas ar naudojimas, įgijimo (perdavimo) metu žinant, kad šis turtas gautas iš nusikalstamos veikos arba dalyvaujant tokioje veikoje.
Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) 216 straipsnis[6]	…tas, kas siekdamas nuslėpti ar įteisinti savo paties ar kito asmens pinigus ar turtą, žinodamas, kad jie įgyti nusikalstamu būdu, atliko su tuo turtu ar pinigais ar jų dalimi susijusias finansines operacijas, sudarė sandorius ar naudojo juos ūkinėje, komercinėje veikloje ar melagingai nurodė, kad tai gauta iš teisėtos veiklos, bus baudžiamas bauda arba laisvės atėmimu iki septynerių metų.

Šaltinis: sudaryta autorės, remiantis Lietuvos Respublikos pinigų plovimo prevencijos įstatymu bei Lietuvos Respublikos baudžiamuoju kodeksu.

dėl nusikaltėlių vykdomo pinigų plovimo kasmet prarandama 3,6 % pasaulio BVP (Financial Accountability Transparency & Integrity, 2020).

1 pav. šis faktas tik patvirtinamas. Tiriamuoju periodu nuo 2009 m. iki 2018 m. pajamos iš nusikalstamos veiklos nuosekliai auga, o tai reiškia, kad problema yra įsisenėjusi ir blogėjanti.



1 paveikslas. Jungtinių Tautų įvertintos pajamos globaliu mastu iš nusikalstamos veiklos sudarė 3,6 % BVP (Pol, 2020)

Analizuojant 2 lentelę svarbu akcentuoti, jog net 50 proc. konfiskuotų neteisėtų lėšų yra iš pinigų plovimo tiek Europos, tiek pasauliniu mastu. Taip pat net 50 proc. atitikčiai reguliuoti skiriamų lėšų yra paskiriama pinigų plovimo temai, nors kovos su pinigų plovimo sėkmės rodiklis Europos mastu yra vos 0,55 proc., o pasauliniu mastu – tik 0,05 proc.

2 lentelė. Pinigų plovimo prevencijos politikos patiriami kaštai (Pol, 2020)

	Europa (Eur)	Pasaulinis (USD)
Kasmet sugeneruojamos lėšos iš nusikalstamos veiklos	110 B	3 T
Kasmet konfiskuojamos neteisėtos lėšos / turtas	1,2 B	3 B
Konfiskuotų neteisėtų lėšų arba turto dalis iš pinigų plovimo	50 proc.	50 proc.
Kovos su pinigų plovimu sėkmės rodiklis	0,55 proc.	0,05 proc.
Atitikties išlaidos	144 B	304 B
Atitikties išlaidų, tenkančių pinigų plovimui	50 proc.	50 proc.

Apibendrinant pateiktą statistiką apie pinigų plovimo prevenciją, galima teigti, kad šiandien vykdama politika, nukreipta prieš pinigų plovimą, reikalavimai ir kiti būtini žingsniai neduoda teigiamų rezultatų. Šis faktas tik sustiprina požiūrį, jog būtent naujos technologijos, tokios kaip dirbtinio intelekto metodų taikymas pinigų plovimo prevencijai, gali ne tik sumažinti kaštus, patiriamus dėl gaunamų baudų už finansų institucijų pažeidimus, bet ir palengvinti specialistų kasdienę veiklą, proaktyviai užkertant kelią šiam finansiniam nusikaltimui.

3. Skaitmeninio intelekto taikymas pinigų plovimo prevencijai

3.1. Sukčiavimo atpažinimo technologijų taikymas pinigų plovimui atpažinti

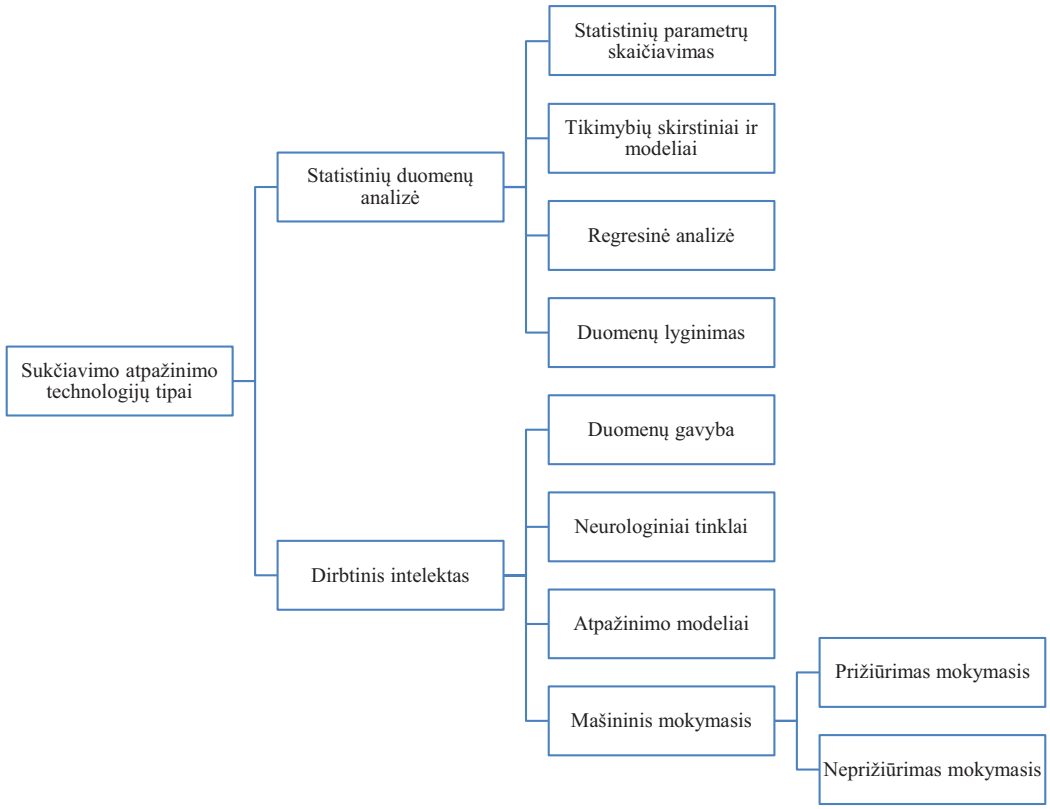
Šiame darbe nagrinėjama, kaip skaitmeninio intelekto (angl. *Computational Intelligence*, CI) technologijos gali prisidėti prie pinigų plovimo prevencijos. Pasak Donepud (2017), tradicinės dirbtinio intelekto (toliau – AI) technologijos susiduria su tokiomis problemomis, kaip didelis, vis sudėtingėjantis taisyklių rinkinys, taisyklių nesuvienodinimas tarp valstybių, todėl AI ne visada atliepia poreikį optimaliai mokytis ir laiku aptikti nuokrypius nuo standartų. Pasikartojančios AI klaidos atvėrė kelią skaitmeninio intelekto įrankiams atrasti (Sadiku, Foreman, Musa, 2018).

Pasak Kanade (2021), labai svarbu suprasti, kad sukčiavimo aptikimas – tai procesas ar visuma veiksmų, kurių imamasi siekiant aptikti ir užblokuoti sukčių bandymą apgaule įgyti pinigų ar turto. Dažnu atveju tai daugiasluoksnis veiksmas, todėl įmonėms, teikiančioms finansines paslaugas, jį atpažinti tampa vis sunkiau ir klasikinių technologijų nebepakanka. Organizacijos diegia šiuolaikines sukčiavimo aptikimo ir prevencijos technologijas bei rizikos valdymo strategijas, siekdamos kovoti su augančiais nesąžiningais sandoriais įvairiose platformose (Kobadilov, Omarov, Yermekbayeva, 2020).

Mokslinėje literatūroje išskiriami 2 pav. pateikti technologijų metodai, taikomi sukčiavimui nustatyti (Kanade, 2021).

Sukčiavimo aptikimo statistinė duomenų analizė atlieka įvairias statistines operacijas: sukčiavimo duomenų rinkimas, sukčiavimo nustatymas ir sukčiavimo patvirtinimas atliekant išsamius tyrimus. Kalbant apie technologijas, kurių veikimas pagrįstas dirbtiniu intelektu, jos gali būti pritaikomos ne tik sukčiavimui atpažinti, bet ir sukčiavimo prevencijai, nes mokydamasis iš istorinių duomenų gali greičiau pastebėti atsikartojimą, kas praeityje buvo pripažinta pinigų plovimu. Šios sukčiavimo atpažinimo technologijos padeda įmonėms sustiprinti vidinį saugumą ir supaprastinti verslo procesus. Padidėjus efektyvumui, dirbtinis intelektas tapo pagrindine technologija, padedančia užkirsti kelią sukčiavimui (Duhart & Hernández-Gress, 2016).

Apibendrinant audito kompanijos *Deloitte* (2022) išvadas, kuriose teigiama, kad sudėtingėjant finansiniams produktams, sparčiai diegiant naujas technologijas, klasikinės sistemos nebeatliepia finansų institucijoms keliamų reikalavimų, todėl būtent dirbtinis intelektas geba



2 paveikslas. Sukčiavimo atpažinimo technologijų tipai (Kanade, 2021)

pagerinti įvairias galimybes siekiant atpažinti modelius, numatyti ateities įvykius, sukurti tinkamas taisykles, priimti tikslingus sprendimus, komunikuoti su tiksline auditorija.

3.2. Skaitmeninio intelekto metodų palyginimas

Prieš pradedant analizuoti skaitmeninio intelekto metodus, būtina apsibrėžti šią sąvoką. Skaitmeninis intelektas (toliau – CI) yra dirbtinio intelekto pogrupis, adaptacinių mechanizmų gebėjimas išmokti konkrečią užduotį iš besikeičiančių duomenų ar eksperimentinio stebėjimo (Siddique, 2013).

Mokslinėje klasikinėje literatūroje išskiriami šie pagrindiniai skaitmeninio intelekto modeliai: dirbtiniai neuroniniai tinklai (angl. *Artificial Neural Network*), evoliucinis skaičiavimas (angl. *Evolutionary Computation* ar *Genetic Algorithm*), neraiškiosios logikos sistemos (angl. *Fuzzy Logic*). Tačiau Donepud (2017) savo darbe papildomai akcentuoja ir šiuos modelius: Bajeso tinklas (angl. *Bayesian / Belief Networks*), mokymosi teorija (angl. *Learning Theory*), tikimybinė logika (angl. *Probabilistic Reasoning*).

Neuroniniai tinklai yra sudaryti iš neuronų, kurie vienas su kitu sujungti ir jungtimis perduoda signalus (Johnston, 2018). Veikimo esmė – tinklas priima įvesties signalą ir kelis kartus apdoroja, o tai suteikia gilesnio ir naudingesnio mokymosi galimybes (Vosyliūtė & Maknickienė, 2022). Šių metodų taikymas reiškia, kad algoritmas gali pagerinti užduoties atlikimą vis kartodamas naudojamus duomenis (Rajawat & Jain, 2020). Šio metodo taikymas praktikoje skirstytinas į penkias grupes: duomenų analizė ir klasifikacija, asociatyvioji

3 lentelė. Skaitmeninio intelekto sampratos analizė (Raj, 2019)

Autorius ir metai	Sąvokos paaiškinimas
Bezdek (1994)	Sistema skaičiavimo požiūriu vadinama intelektualia, jei ji tvarko žemo lygio duomenis, pvz., skaitmeninius duomenis, turi komponentus ir nenaudoja žinių dirbtinio intelekto prasme. Taip pat algoritmas rodo adaptyvius skaičiavimus.
Konar et al. (2006)	Skaitmeninis intelektas gali būti apibrėžtas kaip protingų įrankių ir skaičiavimo priemonių modelis, kuris gali tiesiogiai priimti neapdorotus duomenis ir tiesiogiai juos apdoroti paskirstytu būdu bei toleruoti netikslumą, neapibrėžtumą, dalinę tiesą.
Raj (2019)	Sąvoka „skaitmeninis intelektas“ paprastai reiškia kompiuterio gebėjimą išmokti konkrečią užduotį iš duomenų ar eksperimentinio stebėjimo. Skaitmeninis intelektas paprastai laikomas minkštojo skaičiavimo sinonimu.

atmintis, grupių modelių generavimas ir valdymas. Paprastai šiuo metodu siekiama išanalizuoti ir klasifikuoti medicininius duomenis, pereiti prie veido ir sukčiavimo nustatymo (Berniukevičius & Kurilovas, 2017).

Neraiškioji logika (angl. *Fuzzy Logic*) yra daugiareikšmės logikos forma, kurioje kintamųjų tiesos reikšmė gali būti bet koks realusis skaičius nuo 0 iki 1. Ji naudojama dalinės tiesos sąvokai nustatyti, kai tiesos reikšmė gali svyruoti nuo visiškai teisingos iki visiškai klaidingos (Majhi, 2019). Analizuojant mokslinę literatūrą akcentuojama, jog neraiškioji logika yra vienas labiausiai pritaikomų skaitmeninio intelekto metodų (Majhi, 2019). Ši paradigma susideda iš matavimų ir procesų modeliavimo, sukurtų sudėtingiems realaus gyvenimo procesams (Heidarinia et al., 2014). Priešingai nei AI, kuriam reikalingos tikslios žinios, skaitmeninis intelektas gali susidurti su nepilnumu ir duomenų nežinojimu proceso modelyje.

Ši technika paprastai taikoma įvairioms sritims, kurioms reikalinga kontrolė kaip vaizdo apdorojimas ir sprendimų priėmimas, kai naudojatės vaizdo kamera. Neraiškioji logika čia padeda stabilizuoti vaizdą, netvirtai laikant kamerą (Siddique, 2013).

Evoliucinis algoritmas – tai algoritmas, imituojantis natūralios atrankos procesą. Jis padeda spręsti optimizavimo ir paieškos problemas. Genetiniai algoritmai priklauso didesnei evoliucinių algoritmų klasei. Genetiniai algoritmai imituoja natūralius biologinius procesus, tokius kaip paveldėjimas, mutacija, atranka ir kryžminimas (Rada, 2008). Genetinių algoritmų sąvoka – tai paieškos metodas, dažnai taikomas informatikoje sudėtingiems, neakivaizdiems algoritminio optimizavimo ir paieškos problemų sprendimams rasti. Genetiniai algoritmai yra globalios paieškos euristika (Brabazon et al., 2008). Pasak Rados (2008), pagrindinis šio principo taikymas apima tokias sritis kaip kelių tikslų optimizavimas, kuriems tradicinės matematinės technikos nebepakanka pritaikyti įvairioms problemoms, tokioms kaip DNR analizė.

Bajeso tinklas yra tikimybinis grafinis modelis, vaizduojantis kintamųjų rinkinį ir jų sąlygines priklausomybes per nukreiptą aciklinį grafiką. Bajeso tinklai idealiai tinka įvykiui įvertinti ir numatyti tikimybę, kad bet kuri iš kelių galimų žinomų priežasčių buvo veiksnys (Fong-Rey Liu & Chen, 2011).

Mokymosi teorija aprašo, kaip mokiniai mokydamiesi gauna, apdoroja ir išlaiko žinias. Kognityvinė, emocinė ir aplinkos įtaka, taip pat ankstesnė patirtis turi įtakos supratimui ir pasaulėžiūros įgijimui ir žinių bei įgūdžių išlaikymui (Dunjko & Briegel, 2018).

Tikimybinė logika apima tikimybės ir logikos naudojimą neapibrėžtose situacijose. Tikimybinė logika išplečia tradicines logikos tiesos lenteles tikimybinėmis išraiškomis. Tikimybinės logikos sunkumas yra jų polinkis padauginti tikimybinių ir loginių komponentų skaičiavimo sudėtingumą (Triepels et al., 2018).

4 lentelėje lyginami skaitmeninio intelekto metodai.

Analizuojant mokslinę literatūrą pinigų plovimo atpažinimo prevencijos praktikoje išbandytas ir davęs teigiamų rezultatų yra neraiškiosios logikos ir neuroninių tinklų metodų derinių pritaikymas, nes šių metodų derinys turi pranašumų numatyti, klasifikuoti, grupuoti ir

4 lentelė. Skaitmeninio intelekto technologijų palyginimas (Raj, 2019)

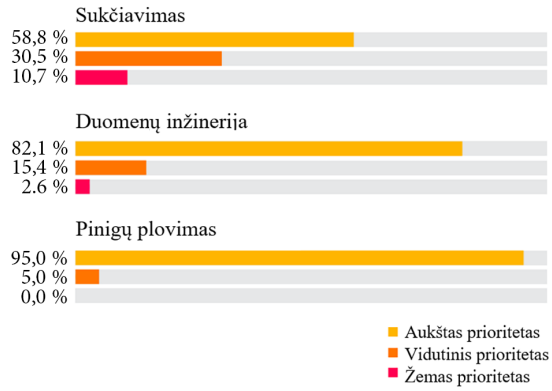
	Technologija	Aprašymas	Taikymas	Privalumai	Trūkumai
Skaitmeninis intelektas	Neraiškioji logika	Naudojamos aibės nariams įvertinti iš daugybės rinkinių	Patentų atpažinimas, kelių tikslų optimizavimas, žinių bazės sistemos	Užtikrina lengvą samprotavimą, įgyvendinimą ir gebėjimą valdyti neapibrėžtumus ir netiesiškumą	Patikimumo stoka
	Neuroniniai tinklai	Kuria paprastą matematinę sistemą, panašią į smegenis, išmoksta ją ir įgyja įžvalgų problemoms spręsti	Netiesinio proceso modeliavimas, struktūros numatymas, anomalijų aptikimas, sprendinių sudarymas	Atsparus gedimams, mokosi iš pavyzdžių, smulkūs pokyčiai neturi didelės įtakos	Reikalingas procesorius su lygiagrečiojo apdorojimo galimybe
	Evoliucinis algoritmas	Remiasi natūraliu atrankos procesu	Intelektuali paieška, kelių tikslų optimizavimas	Lankstus, savaime prisitaikantis, optimalus sprendimas	Ankstyva konvergencija, lemianti vietinį optimalumą
	Mokymosi teorija	Paremta ankstesnių rezultatų išmokimu, kad būtų galima numatyti būsimus rezultatus	Diagnozė, aptikimas, nelaimių valdymas	Problemos sprendimas. Taikoma bet kuriai nuspėjamai mokymosi sferai	Trūksta detalumo
	Tikimybinė logika	Nustato galimą problemos rezultatą, pagrįstą ankstesnėmis įžvalgomis	Pramoninės diagnostikos prognozė	Tvarko neapibrėžtumą ir rizikos skaičiavimus	Brangus ir neefektyvus laiko požiūriu

optimizuoti, sutvarkyti duomenis (Jamshidi et al., 2019; Rajawat & Jain, 2020). Vertinant abstrakčiai, skaitmeninio intelekto modeliai parodo gebėjimą mokytis ir prisitaikyti prie naujų situacijų, atrasti neatitikimus, todėl šie metodai gali būti bandomi pritaikyti pinigų plovimui atpažinti ir prevencijai.

3.3. Dirbtinio intelekto įrankių pritaikymo pinigų plovimo prevencijai svarba

Jungtinėse Amerikos Valstijose atliktame tyrime (The State of Fraud and Financial Crime in the U.S., 2022) dalyvavo 200 finansų institucijų darbuotojai, kurių turtas sudarė ne mažiau kaip 5 mlrd. dolerių. Apklausti darbuotojai užėmė vadovaujamas pareigas sukčiavimo ir rizikos operacijų, pinigų plovimo, sukčiavimo strategijos, sukčiavimo analizės, technologijų ir duomenų srityse. 177 iš apklausos respondentų buvo atsakingi už sukčiavimo atpažinimo ir prevencijos valdymą, iš kurių 20 – už pinigų plovimo prevencijos valdymą. Kiti respondentai buvo atsakingi už duomenų mokslą ir technologijas.

Tyrimo dalyvių buvo prašoma įvardyti prioritetus pagal skirtingas sritis, kuriose vadovaujamas pareigas užimantys darbuotojai teikia naujų sprendimų kurti arba aptikimui tobulinti ir prevencijos sistemoms, skirtoms kovai su sukčiavimu ir finansiniais nusikaltimais pagal specializacijos sritis (3 pav.).



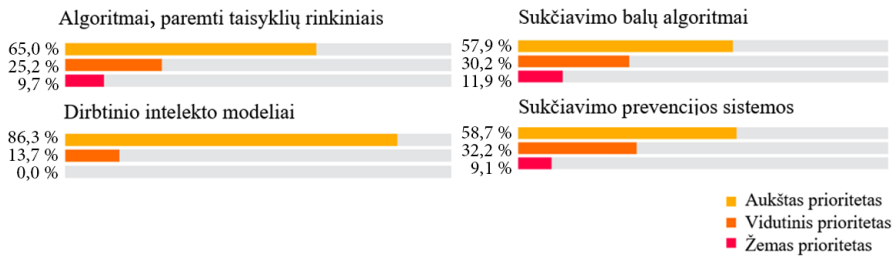
3 paveikslas. Naujovių ir tobulėjimo svarba pagal respondentų veiklos sritis (The State of Fraud and Financial Crime in the U.S., 2022)

Tyrimo duomenys atskleidžia, kad vadovaujamas pareigas einantys darbuotojai pinigų plovimo prevencijos srityje beveik vienbalsiai – 95 proc. – mano, jog naujoviškų kovos sprendimų naudojimas pinigų plovimo prevencijai yra prioritetinis. Taip pat šios nuomonės laikosi vadovai, dirbantys finansinio sukčiavimo srityje: net 82 proc. mano, jog naujausios technologijos ir inovacijos yra viena iš galimybių, padedančių kovoti su finansiniais nusikaltimais. Duomenų mokslo vadovų tik daugiau nei 59 proc. laikosi nuomonės, jog tai prioritetinė sritis.

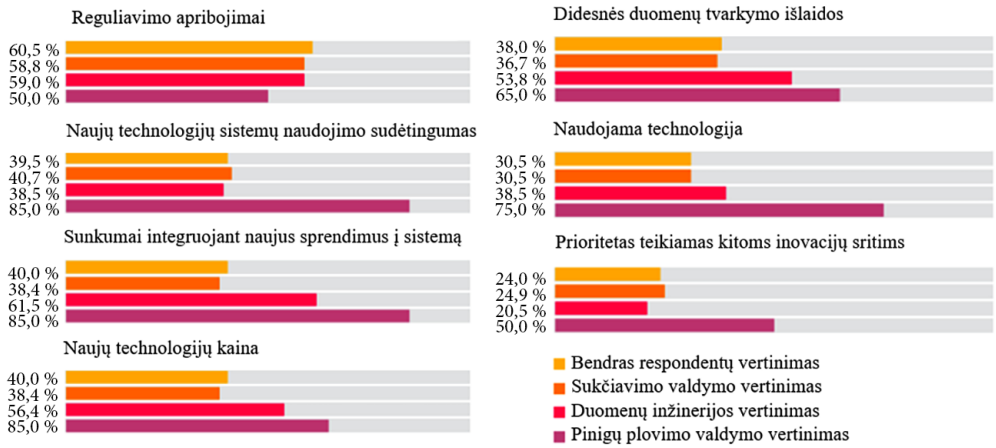
Įmonės, jau taikančios modernias technologijas, buvo linkusios ir toliau teikti pirmenybę šiuolaikinių pinigų plovimo (toliau – AML) ir kovos su sukčiavimo technologijų integracijai. Įmonės, kurios dar nėra integravusios naujų kovos su sukčiavimu ir AML sprendimų, galimas suvokimo sudėtingumas yra didelė modernizavimo kliūtis. Apklausti vadovai, kurie nepriėmė šiuolaikinių AML ir kovos su sukčiavimu strategijų, tai padarė ne todėl, kad nebuvo technologinių sprendimų, kuriuos būtų galima integruoti su esamomis technologijomis ar strategijomis, bet todėl, kad buvo įsitikinę, kad tai padaryti bus per sunku. Atlikus apklausą nustatyta, kad 66 proc. vadovų išreiškė susirūpinimą, jog reguliavimo standartai yra per sudėtingi ir jų sprendimas gali neatitikti visų jų atitikties poreikių. Taigi 58 proc. manė, kad šiuolaikinės sukčiavimo schemos buvo pernelyg sudėtingos ir joks sprendimas negalėjo būti veiksmingas, o 49 proc. nerimauja, kad didėjantis sukčiavimo lygis priblokš bet kurią sistemą.

Technologijų, kurioms vadovai skiria dėmesį ir taiko veikloje (4 pav.), tyrimo duomenys atskleidė, jog 86 proc. įmonių, naudojančių dirbtinio intelekto įrankius, mano, jog tai prioritetinė sritis, duodanti teigiamų rezultatų kovojant su sukčiavimu. Taip pat 78 proc. apklaustųjų mano, jog debesijoje veikiančios sukčiavimo platformos lengvina jų kasdienę veiklą.

Svarbu suprasti ir veiksnius, stabdančius skaitmeninio intelekto taikymą pinigų plovimui atpažinti ir prevencijai. Tyrimo respondentai sutinka, kad šie veiksniai (5 pav.) slopina naujoves arba naujų funkcijų įtraukimą į esamus sprendimus. Iš pinigų plovimo prevencijos srityje vadovaujamas pareigas užimančių asmenų net 85 proc. mano, jog naujų technologijų sistemų



4 paveikslas. Naujų technologijų pritaikymo svarba (The State of Fraud and Financial Crime in the U.S., 2022)



5 paveikslas. Veiksniai, slopinantys naujų technologijų diegimą (The State of Fraud and Financial Crime in the U.S., 2022)

naudojimas yra sudėtingas, turi sunkumų integruojant naujus sprendimus į esamas sistemas. Net 75 proc. respondentų teigia, jog naudojama technologija įvardijama kaip veiksnys, stabdantis naujų technologijų taikymą veikloje.

Apibendrinant tyrimą galima teigti, jog aukščiausio lygmens vadovai aiškiai supranta, kad naudojant dirbtinį intelektą sukurti sprendimai yra būdas suvaldyti pinigų plovimo nusikalstamą veiklą. Įmonės, teikiančios finansines paslaugas, ieško būdų, kaip kovoti su vis sudėtingesnėmis finansinių nusikaltimų formomis, taikydamos naujų technologijų sprendimus, tokius kaip dirbtinis intelektas. Tyrimo rezultatai paviešino veiksnius, kurie stabdo naujų technologijų diegimą pinigų plovimo prevencijoje, t. y. nusistatymas, jog dirbtinio intelekto metodai atrodo sudėtingi ir sunkiai pritaikomi.

3.4. Pinigų plovimo duomenų aprašymas

Šiame darbe naudojama pinigų plovimo atpažinimo duomenų bazė, prieinama kaggle.com. Dirbtiniu būdu sukurtos analizuojamos duomenų bazės modeliavimas pagrįstas trimis pinigų plovimo etapais:

1) pinigų įdėjimas;
2) pinigų sluoksniavimas;
3) pinigų integravimas.

Duomenų bazėje šie etapai kategorizuoti tipais, kai 1 taisyklė yra susijusi su pinigų išgryninimu (angl. *Cash-in*), o 2 ir 3 taisyklės – su pervedimu (angl. *Transfer*).

Iš pateiktų duomenų pinigų išsigryninimas sudarė 38 proc., pervedimas – 62 proc. visų duomenų. Sugeneruotų duomenų laikotarpis yra 6 mėn. Per visą laikotarpį buvo užfiksuota 59 proc. pinigų plovimo atvejų, iš kurių išsigryninant pinigus užfiksuota 57 proc. nelegalios veiklos, o pervedant pinigus – 62 proc. tipinių plovimo veiksmų. Dar detaliau analizuojant duomenis tiek antrame, tiek trečiame pinigų plovimo etapuose, nelegalių pervedimų skaičius buvo panašus. Taip pat pastebėta, jog pinigų plovimo veiksmai užfiksuoti pervedant ar išsigryninant mažesnes sumas.

Taigi šioje duomenų bazėje pateikti duomenys leidžia daryti prielaidą, jog daugiau atliktų pinigų plovimo veiksmų pastebėta pervedimo etape arba pinigų sluoksniavimo ir pinigų integravimo etapuose. Taip pat ši nusikalstama veikla atliekama pervedant mažesnes pinigų sumas.

Išvados

Vis didėjantys kaštai patiriami kovojant su pinigų plovimu ir tik 0,5 proc. sėkmingų pinigų plovimo atskleidimo atvejų konstatuoja faktą, jog vykdoma politika prieš pinigų plovimą, reikalavimai finansų įmonėms ir kiti būtini žingsniai neduoda teigiamų rezultatų. Šis faktas tik sustiprina požiūrį, jog būtent naujos technologijos, tokios kaip dirbtinio intelekto metodų taikymas pinigų plovimui

5 lentelė. Pinigų plovimo duomenų bazės struktūra (kaggle.com)

Duomenys reikšmė	Pinigų operacijos tipai	Šaltinio identifikacijos numeris	Vietos identifikacijos numeris	Pinigų suma	Data, laikas	Pinigų plovimas	Pinigų plovimo etapas
Kategorija	Išsigryninimas, pervedimas	–	–	–	–	1, 0	None; Type1; Type2; Type3

atpažinti ir prevencijai, gali ne tik sumažinti kaštus, kurie patiriami dėl gaunamų baudų už įmonių pažeidimus, bet ir palengvinti kasdienę specialistų veiklą proaktyviai užkertant kelią šiam finansiniam nusikaltimui.

Šiame darbe pasirinkta analizuoti dirbtinio intelekto pošakio skaitmeninio intelekto metodų taikymą pinigų plovimui atpažinti ir prevencijai, nes skaitmeninio intelekto įrankiai yra lankstesnis ir skaičiavimas remiasi „minkštaisiais skaičiavimo metodais“, kurie leidžia prisitaikyti prie daugelio situacijų. Taip pat taikomi metodai yra artimi žmogaus samprotavimo būdui, t. y. naudoja netikslią ir neišsamią informaciją bei sugeba prisitaikant atlikti kontrolės veiksmus, ko priešingai dirbtinio intelekto metodai nesugeba.

Išanalizavus mokslinę literatūrą apie skaitmeninio intelekto metodus, galima teigti, kad jie yra tinkami taikyti pinigų plovimo atpažinimo ir prevencijos metodus, nes technologijos rodo gebėjimą mokytis ir prisitaikyti prie naujų situacijų, atrasti neatitikimus bei susieti informaciją. Sykiu svarbu pabrėžti, kad skaitmeninio intelekto metodų vis daugėja, o tai rodo, kad jų veikimas yra pripažintas kaip naudingas ir praktiškai pritaikomas. Taip pat naujausiuose moksliniuose tyrimuose pabrėžiama, jog neuroninių tinklų ir neraiškiosios logikos modelių derinys leidžia tiksliau grupuoti, klasifikuoti informaciją ir sklandžiau optimizuoti užduotis.

Straipsnyje analizuoti tyrimo rezultatai paviešino veiksnius, kurie visgi stabdo naujų technologijų diegimą pinigų plovimo prevencijos srityje, t. y. nusistatymas, jog dirbtinio intelekto metodai atrodo sudėtingi ir sunkiai pritaikomi. Šiuos nuogąstavimus paneigti gali tik tolesnis šios temos tyrimas ir praktinis jos taikymas pinigų plovimo veikloje. Šio darbo tęstinė dalis – praktiškai lyginant skaitmeninio intelekto metodus, įvertinti efektyviausią metodą ar metodų derinį.

Literatūra

Anti-money Laudering Market. (2022). https://www.marketsandmarkets.com/Market-Reports/anti-money-laundering-solutions-market-95490454.html?gclid=CjwKCAjwm8WZBhBUEiwA178UnEPu4IQINJ45Df5rS12jGtpVAsafr7CCMOsyZ-ZYOWInX60-Bbj9mBoCUwkQAvD_BwE

Basel Institute on Governance. (2021). Basel AML Index 2021 (10th ed.). https://baselgovernance.org/publications/basel-aml-index-2021

Berniukevičius, A., & Kurilovas, E. (2017). Dirbtiniai neuroniniai tinklai personalizuotam mokymuisi. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiqya_sm7D6AhVnkIsKHaI2AXoQFnoECC4QAQ&url=https%3A%2F%2Fwww.zurnalai.vu.lt%2FLMR%2Farticle%2Fdownload%2F17755%2F16919%2F&usg=AOvVaw3mk3w2ve7B0CEmK6f2urge

Bezdek, J. S. (1994). What is Computational Intelligence? https://www.researchgate.net/publication/220045330_What_is_Computational_Intelligence

Brabazon, A., O'Neill, M., & Dempsey, I. (2008, November). An Introduction to Evolutionary Computation in Finance. In *IEEE Computational Intelligence Magazine*, *3*(4), 42–55. https://doi.org/10.1109/MCI.2008.929841

Deloitte. (2022). The new physics of financial services: How artificial intelligence is transforming the financial ecosystem. https://www2.deloitte.com/bd/en/pages/financial-services/articles/artificial-intelligence-transforming-financial-ecosystem-deloitte-fsi.html

Donepud, P. K. (2017). Machine learning and artificial intelligence in banking. *Engineering International*, *5*(2), 83–86. https://doi.org/10.18034/ei.v5i2.490

Duhart, B., & Hernández-Gress, N. (2016). Review of the Principal Indicators and Data Science Techniques used for the Detection of Financial Fraud and Money Laundering. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, pp. 1397–1398 https://doi.org/10.1109/CSCI.2016.0267

Dunjko, V., & Briegel, H. (2018). Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics*, *81*(7), 074001. https://doi.org/10.1088/1361-6633/aab406

Economist. (2021, April 12). The war against money-laundering is being lost: The global system for financial crime is hugely expensive and largely ineffective. https://www.economist.com/finance-and-economics/2021/04/12/the-war-against-money-laundering-is-being-lost

Financial Accountability Transparency & Integrity. (2020, September). *FACTI PANEL Interim Report, 2020*. https://uploads-ssl.webflow.com/5e0bd9edab846816e263d633/5f6b68c7bff4ad6cf6cb53a7_FACTI_Interim_Report_final.pdf

Fong-Rey Liu, K., & Chen, Jia-Shen. (2011). Prediction and assessment of student learning outcomes in calculus a decision support of integrating data mining and Bayesian belief networks. In *2011 3rd International Conference on Computer Research and Development*, Shanghai, China, pp. 299–303. https://doi.org/10.1109/ICCRD.2011.5764024

Georgieva, N. (2020). Concept, definition and characteristics of the money laundering phenomenon. *Journal of Process Management. New Technologies*, *8*(2), 23–37. https://doi.org/10.5937/jouproman8-26220

Heidarinia, N., Harounabadi, A., & Sadeghzadeh, M. (2014, July). An intelligent anti-money laundering method for detecting risky users in the banking systems. *International Journal of Computer Applications*, *97*(22), 35–39. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.6190&rep=rep1&type=pdf

Jamshidi, M. B., Gorjiankhanzad, M., Lalbakhsh, A., & Roshani, S. (2019). A novel multiobjective approach for detecting money laundering with a neuro-fuzzy technique. In *2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC)*, Banff, AB, Canada, 2019, pp. 454–458. https://doi.org/10.1109/ICNSC.2019.8743234

Johnston, M. (2018, September 28). Seizing the moment for artificial intelligence. https://blog.evergreengavekal.com/seizing-the-moment-for-artificial-intelligence/

kaggle. (n.d.). *Level up with the largest AI & ML community*. https://www.kaggle.com/

Kanade, V. (2021). What Is Fraud Detection? Definition, Ty-

pes, Applications, and Best Practices. Fraud detection prevents fraudsters from obtaining money or property through false means. https://www.toolbox.com/it-security/vulnerability-management/articles/what-is-fraud-detection

Kobadilov, B., Omarov, G. B., & Yermekbayeva, D. D. (2020). Financial technologies trends and how they will shape financial markets [Article]. *The Economy: Strategy and Practice*, *15*(2), 151–157. https://esp.ieconom.kz/jour/article/view/208/204

Konar, A. (2006). *Computational intelligence: principles, techniques and applications*. Springer Science & Business Media,

Lietuvos Respublikos Seimas. (2021). Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas. (2021, gruodžio 31, Nr. XIV-831). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/addbfac066ed11ecb2fe9975f8a9e52e

Lietuvos Respublikos baudžiamasis kodeksas. (2021, rugsėjo 1d. Nr. 89-2741). https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr

Majhi, S. K. (2019). Fuzzy clustering algorithm based on modified whale optimization algorithm for automobile insurance fraud detection. *Evolutionary Intelligence*, *14*(1), 35–46. https://doi.org/10.1007/s12065-019-00260-3

Money laundering data. (n.d.). https://www.kaggle.com/datasets/maryam1212/money-laundering-data?select=ML.csv

Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. *Policy Design and Practice*, *3*(1), 73–94. https://doi.org/10.1080/25741292.2020.1725366

Rada, R. (2008). Expert systems and evolutionary computing for financial investing: A review. *Expert Systems with Applications*, *34*(4), 2232–2240. https://doi.org/10.1016/j.eswa.2007.05.012

Rajawat, A. S., & Jain, S. (2020). Fusion Deep Learning Based on Back Propagation Neural Network for Personalization. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9170693

Raj, J. S. (2019). A comprehensive survey on the computational intelligence techniques and its applications. *IRO Journals: Journal of IoT in Social, Mobile, Analytics, and Cloud*, *1*(3), Article-2. https://irojournals.com/iroismac/V1/I3/02.pdf

Sadiku, M. N. O., Foreman, J., & Musa, S. M. (2018). Computational intelligence. *European Scientific Journal*, July 2018 Edition, *14*(21), 56–60. https://doi.org/10.19044/esj.2018.v14n21p56

Siddique, A. (2013, April 22). *Computational intelligence: synergies of fuzzy logic, neural networks and evolutionary computing*. John Wiley & Sons. https://doi.org/10.1002/9781118534823

Triepels, R., Daniels, H., & Feelders, A. (2018). Data-driven fraud detection in international shipping. *Expert Systems with Applications*, *99*(1), 193–202. https://doi.org/10.1016/j.eswa.2018.01.007

The State of Fraud and Financial Crime in the U.S. (2022). https://www.featurespace.com/the-state-of-fincrime-in-the-us-2022-report/

Unger, B., Siegel, M., Ferwerda J., Kruijf, W., Busuioic, M., & Wokke K. (2006). The amount and the effects of money laundering: Report for the Ministry of Finance February 16, 2006. Utrecht School of Economics and Australian National University. https://www.maurizioturco.it/bddb/2006_02_16_the_amounts_and_.pdf

United Nations. (2022). *Money Laundering*. https://www.unodc.org/unodc/en/money-laundering/overview.html

Vainienė, R. (2008). Ekonomikos terminų žodynas: apie 1400 terminų. Tyto Alba.

Vosyliūtė, I., & Maknickienė, N. (2022). Investigation of financial fraud detection by using Computational intelligence. In *12th International Scientific Conference "Business and Management" 2022, May 12–13*, Vilnius, Lithuania, pp. 390–397. https://doi.org/10.3846/bm.2022.787

Zhang, Y., & Trubey, P. (2018). Machine learning and sampling scheme: An empirical study of money laundering detection. Computational Economics, *54*,1043–1063. https://link.springer.com/article/10.1007/s10614-018-9864-z

INVESTIGATION OF MONEY LAUDERING DETECTION BY USING COMPUTATIONAL INTELLIGENCE

Akvilė EREMINĖ, Nijolė MAKNICKIENĖ

Abstract. The large amount of data related to compliance with money laundering requirements and the increasing sophistication of criminal methods are forcing financial companies to look for new tools to help them meet their regulatory obligations. To achieve this goal, technologies whose operation is based on artificial intelligence become inseparable from the prevention of money laundering. This article makes the case for the true cost of money laundering to the global economy. To achieve this, different technologies used in identifying financial fraud were compared. Special attention in this article is given to a subset of artificial intelligence – digital intelligence methods. According to the latest scientific research, these methods are based on soft computing, which allow to adapt to many situations, predict future events, create appropriate rules, and make targeted decisions. Also, the importance of artificial intelligence in the prevention of money laundering is emphasized by the US study analyzed in the article, in which top-level managers responsible for the field of money laundering prevention were interviewed. The respondents expressed a unanimous opinion that the further application of artificial intelligence in the field of money laundering prevention is a priority.

Keywords: money laudering, computional intelligence, artificial intelligence.