MYKOLO ROMERIO UNIVERSITETO
TEISĖS MOKYKLOS
BAUDŽIAMOSIOS TEISĖS IR PROCESO INSTITUTAS

JONAS AUGULIS
Baudžiamosios teisės ir kriminologijos nuolatinių studijų programa

SUKČIAVIMAI ELEKTRONINĖJE ERDVĖJE: KRIMINOLOGINIAI ASPEKTAI

Magistro baigiamasis darbas

Darbo vadovas –
doc. Dr. Alfredas Kiškis

Vilnius, 2020

Turinys

ĮVADAS

Darbo aktualumas. Informacinių technologijų raida daro įtaką ir tradicinių nusikaltimų pasikeitimui, nusikaltimų persikėlimui į elektroninę erdvę. Kaip teigia Renata Marcinauskaitė: „*Elektroninėje erdvėje, savo parametrais nors ir nutolusioje nuo fizinės, neišvengiama įvairių grėsmių teisinėms vertybėms, taip pat ir iš esmės naujų arba dėl informacinių technologijų taikymo pakitusių nusikalstamų veikų*“[1]. Europos Komisijos pateikto DESI (Skaitmeninio ekonomikos ir visuomenės indekso) 2019 m. tyrimo duomenimis: „Lietuvos, kaip ir kitų ES šalių, gyventojai noriai užsiima įvairia veikla internete. Interneto naudotojų skaičius auga ir šiuo metu jau siekia 81 proc.“[2] Neabejotinai, šis skaičius esant globaliai pandemijai COVID-19 turėjo didėti, kadangi daugelis įmonių pandemijos metu įvedė nuotolinį darbą, o kai kurie verslo atstovai net ir po pandemijos sudarys galimybę žmonėms ir toliau dirbti nuotoliniu būdu. COVID-19 pandemija suskubo pasinaudoti ir sukčiai. Europolo duomenimis, COVID-19 pandemijos metu sukčiai pritaikė jau žinomus sukčiavimo metodus bei pasinaudojo aukų baime krizės metu[3]. Padidėjus dezinfekcinių priemonių paklausai, sukčiai elektroninėje erdvėje sukūrė fiktyvius elektroninės prekybos tinklalapius siekiant apgaule įgyti žmonių lėšas. Europolo pranešime[4] pateikiamas apgaulės atvejis, kuomet 6,6 mln. eurų už apsaugines kaukes bei rankų dezinfekcinį skystį buvo pervesti kompanijai į Singapūrą, tačiau prekės taip ir nebuvo pristatytos. Federalinis tyrimų biuras taip pat įspėja apie padidėjusį apgaulės, susijusios su apsimetimu įmonės vadovybe atvejų skaičių COVID-19 metu[5].

Jungtinių Amerikos Valstijų kibernetinio nusikalstamumo centro (toliau ir - *IC3*) 2019 m. nusikalstamumo ataskaitoje[6] 2019 m. buvo gauta virš 460 tūkst. pranešimų dėl sukčiavimo elektroninėje erdvėje, kurių žala viršijo 3,5 milijardo JAV dolerių. Ataskaitoje minimi ir daugiausiai žalos padarę sukčiavimo elektroninėje erdvėje modeliai: apgaulė, apsimetant įmonės vadovybe, meilės nusikaltimai, apgaulingi elektroniniai laiškai ir skambučiai. Vien tik apgaule apsimetant įmonės vadovybe buvo padaryta daugiau nei apie pusė turtinės žalos – 1,7 mlrd. JAV dolerių. Žiniasklaidoje taip pat buvo minimas Lietuvos Respublikos pilietis, kuris panaudodamas

[1] Renata Marcinauskaitė, *Nusikalstamos veikos elektroninėje erdvėje :elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje: monografija* (Vilnius: Registrų centras, 2019), 11.
[2] „Skaitmeninės ekonomikos ir visuomenės indeksas (DESI) 2020 m.“, Lietuvos ataskaita, žiūrėta 2020 m. rugsėjo 8 d., https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66948.
[3] „How criminals profit from the COVID-19 pandemic“, Europol, žiūrėta 2020 m. rugsėjo 8 d., https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic.
[4] *Ibid*
[5] „FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic“, FBI, žiūrėta 2020 m. rugsėjo 19 d., https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic.
[6] „2019 Internet Crime Report“, IC3, žiūrėta 2020 m. rugsėjo 17 d. https://pdf.ic3.gov/2019_IC3Report.pdf.

pastarąjį sukčiavimo modelį apgaule iš JAV kompanijų įgijo daugiau nei 100 mln. JAV dolerių[7]. *IC3* 2018 m. pateiktoje ataskaitoje[8] apie apgaulę, apsimetant įmonės vadovybe, teigiama, jog tarp 2016 m. gruodžio mėn. ir 2018 m. gegužės mėn. matomas 136 proc. globalus žalos padidėjimas. *IC3* ataskaitos duomenimis nuo šio sukčiavimo aukos nukentėjo 50-yje JAV valstijų ir 150-yje šalių. Apgaulės, apsimetant įmonės vadovybe įgytos lėšos buvo pervestos į 115 šalių.

Jungtinės Karalystės nacionalinio sukčiavimų tyrimų biuro (toliau ir - *Action Fraud*) pateiktame pranešime[9] per pirmąjį 2020 m. pusmetį finansinių įstaigų specializuotų padalinių darbuotojai sustabdė apgaule padarytų mokėjimų 19 mln. Jungtinės Karalystės svarų sumai. Populiariausi sukčiavimo modeliai Jungtinėje Karalystėje – apsimetimas banko darbuotoju, meilės nusikaltimai. Kaip matyti *IC3* ir *Action Fraud* pateiktose ataskaitose vienas iš dominuojančių sukčiavimo modelių elektroninėje erdvėje yra meilės nusikaltimai[10]. 2019 m. *IC3* ataskaitos duomenimis šiuo sukčiavimo modeliu buvo padaryta beveik 500 mln. JAV dolerių žala 52–iose JAV valstijose. Taip pat vienas populiariausių sukčiavimo modelių *IC3* ataskaitos duomenimis, nukreiptų į fizinius asmenis yra apgaulė, susijusi su investavimu. 2019 m. *Action Fraud* duomenimis[11] investicijų sukčiavimo aukų skaičius Jungtinėje Karalystėje daugiau nei patrigubėjo, lyginant su 2018 m. Jungtinės Karalystės gyventojai prarado daugiau nei 27 mln. JK svarų. Vidutiniškai vienas asmuo prarado 14,6 tūkst. JK svarų. Lietuvos žiniasklaidoje galima pastebėti atvejų, kai asmuo dėl apgaulės, susijusios su investavimu prarado ne tik viso gyvenimo santaupas, bet greta to pardavė savo nekilnojamąjį turtą ir taip prarado daugiau nei 36 tūkst. eurų[12].

2020 m. liepos 16 d. Lietuvos Respublikos Valstybės kontrolės audito ataskaitos duomenimis: „*apie 62 proc. nusikaltimų elektroninėje erdvėje ikiteisminių tyrimų 2016–2019 m. atliko nespecializuoti pareigūnai.* [...] *40 proc. 2016–2019 m. baigtų nusikaltimų elektroninėje*

---

[7] „Lithuanian Man Arrested For Theft Of Over $100 Million In Fraudulent Email Compromise Scheme Against Multinational Internet Companies“, United States Department of Justice, žiūrėta 2020 m. rugsėjo 17 d., https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme.

[8] „Business E-Mail compromise the 12 billion dollar scam“, IC3, žiūrėta 2020 m. rugsėjo 17 d., https://www.ic3.gov/media/2018/180712.aspx.

[9] „Bank branch staff and police team up to stop £19 million of fraud in first half of 2020“, Action Fraud UK, žiūrėta 2020 m. rugsėjo 17 d., https://www.actionfraud.police.uk/news/bank-branch-staff-and-police-team-up-to-stop-19-million-of-fraud-in-first-half-of-2020.

[10] „Meilės nusikaltimai“ (angl. *romance scam*) – tai toks apgaulės būdas, kai sukuriamos fiktyvios anketos pažinčių svetainėse ir siekiama užmegzti pažintį su priešingos lyties asmeniu bei kai kalba eina apie susitikimą, paprašoma pinigų už lėktuvo bilietus, drabužius, viešbutį ar kitas išlaidas. Jeigu pinigai pervedami – kaltininkas dingsta, ištrina fiktyvų profilį pažinčių svetainėse arba bando iš aukos išvilioti dar daugiau pinigų. Kai kuriais atvejais, aukos ne tik patiria finansinius nuostolius, bet ir būna nužudytos. Pvz. https://www.scmp.com/news/world/article/1420830/nigerian-man-arrested-over-australian-womans-death-online-dating-scam.

[11] „Over £27 million reported lost to crypto and forex investment scams“, Action Fraud UK, žiūrėta 2020 m. rugsėjo 19 d. https://www.actionfraud.police.uk/news/over-27-million-reported-lost-to-crypto-and-forex-investment-scams.

[12] „Senolė pardavė butą ir sukčiam pervedė 36 000 EUR“ Teismo Vikingas, patalpinta 2019 m. gruodžio 4 d., YouTube klipas, https://youtu.be/OGpLei1heAU.

erdvėje ikiteisminių tyrimų truko ilgiau nei 9 mėn.“ [13] Iš to galima spręsti, kad Lietuvoje trūksta žinių, patirties ir specializuotų ikiteisminio tyrimo tyrėjų. Elektroninėje erdvėje galima pastebėti SEB banko sukurtą interaktyvų žaidimą, kuris padeda suprasti labiausiai paplitusius sukčiavimo elektroninėje erdvėje modelius[14]. Panašų projektą prieš grėsmes elektroninėje erdvėje šiais metais sukūrė ir Lietuvos Respublikos vyriausybės kanceliarija[15]. Būtent padidėjęs sukčių elektroninėje erdvėje veikimo mastas prieš Lietuvos gyventojus[16] ir nulėmė panašių interaktyvių kampanijų atsiradimą. Kaip pastebėta, kol kas tokių iniciatyvų imasi pačios finansinės įstaigos, siekdamos apsaugoti visuomenę nuo elektroninėje erdvėje veikiančių sukčių. Baigiamojo darbo autorius dirba Lietuvoje veikiančiame banke. Pastebėta, jog kiekvieną dieną įvairaus amžiaus asmenys tampa sukčių elektroninėje erdvėje aukomis. Kai kurios aukos patiria pakartotinę viktimizaciją. Susisiekus su aukomis kai kurios iš jų net neigia jų atžvilgių padarytos apgaulės faktą ir reikalauja toliau vykdyti transakciją.

Baigiamasis darbas aktualus visuomenei, nes bus nustatyti tam tikri sukčiavimo elektroninėje erdvėje modeliai, žinant šiuos modelius galima imtis savisaugos priemonių. Aktualu tyrinėti sukčiavimą elektroninėje erdvėje, jų paplitimą, žalą, kitimo tendencijas, juos darančius asmenis ir aukas bei prevenciją, siekiant pateikti pagrįstų siūlymų jų prevencijos ir kontrolės gerinimui. Sukčiai elektroninėje erdvėje gali nesunkiai adaptuotis naujoje socialinėje aplinkoje ir atsižvelgiant į toje aplinkoje vyraujančius pokyčius, prie jų prisitaikyti ir sugalvoti naujų sukčiavimo modelių.

Baigiamajame darbe tiriamos problemos ištyrimo lygis. Lietuvoje elektroninėje erdvėje vyraujančiais nusikaltimais vienas pirmųjų iš teisės pusės pradėjo domėtis R. Petrauskas[17]. Kompiuteriniai nusikaltimai ir jų prevencija: mokomajame leidinyje nagrinėta kompiuterinių nusikaltimų klasifikacija, teisiniai kompiuterinių nusikaltimų aspektai. Vienas pirmųjų, nagrinėjusių kompiuterizacijos kriminologinius aspektus buvo S. Starkus[18]. Šio mokslininko darbe

[13] „Ar veiksmingai kovojama su elektroniniais nusikaltimais?“, Valstybinio audito ataskaita, žiūrėta 2020 rugsėjo 10 d., https://www.vkontrole.lt/failas.aspx?id=4101.
[14] „Interaktyvus SEB banko žaidimas „Pinklės“, kuris padės, suprasti labiausiai paplitusius sukčių metodus ir patars, kaip elgtis konkrečiose situacijose“, SEB bankas, žiūrėta 2020 m. rugsėjo 12 d., https://sukciupinkles.lt.
[15] „Sustiprink imunitetą“, kuris moko atpažinti ir atremti grėsmes internete“, Sustiprink imunitetą, žiūrėta 2020 m. rugsėjo 13 d., https://sustiprinkimuniteta.lt.
[16] Pvz. apgaulingos sms žinutės iš banko (angl. *smshishing*) - https://www.seb.lt/naujienos/2020-05-15/seb-ispeja-apie-sukciu-platinamas-melagingas-neva-banko-siunciamas-sms-zinutes, apgaulė, susijusi su investavimu (angl. *investment scam*) - https://www.lrt.lt/naujienos/verslas/4/1187305/investavimo-lietuviai-bijo-ne-be-reikalo-sukciams-praskolina-ir-visos-gimines-santaupas, https://www.lrytas.lt/lietuvosdiena/kriminalai/2020/04/09/news/i-kriptovaliutas-investuoti-siule-sukciai-is-vyro-isviliojo-virs-23-tukst-euru-14416054/, https://www.ve.lt/naujienos/lietuva/lietuva/sukciai-zmoniu-kisenes-tustina-vis-moderniau-stai-4-populiariausios-aferos-1780861/.
[17] Rimantas Petrauskas ir Darius Štitilis, *Kompiuteriniai nusikaltimai ir jų prevencija: mokomasis leidinys parengtas pagal Tempus Phare projektą „Valstybės pareigūnų rengimas teisinės sistemos reformai Lietuvoje“* (Vilnius: LTA Leidybos centras, 2000).
[18] Saulius Starkus, "Kriminologiniai Kompiuterizacijos Aspektai." *Jurisprudencija*. 20(2001): 85-92. https://talpykla.elaba.lt/elaba-fedora/objects/elaba:2706487/datastreams/MAIN/content.

nagrinėta kriminogeninė kompiuterizacijos įtaka įvairioms gyvenimo sritims. Kiek vėliau D. Štitilio išleistoje disertacijoje[19] tirta elektroninė erdvė, kaip nauja erdvė vykdyti tradicinius nusikaltimus, elektroninėje erdvėje padaromų nusikalstamų veikų teisiniai aspektai. Taipogi D. Štitilis su kitais mokslininkais – P. Pakutinsku, M. Laurinaičiu, I. Dauparaite 2011 m. nagrinėjo tapatybės vagystės elektroninėje erdvėje teisinius aspektus[20]. Šiame kolektyviniame leidinyje tyrinėta tapatybės vagystė elektroninėje erdvėje, jos kvalifikavimo problemos. 2013 m. R. Marcinauskaitė išleistoje disertacijoje[21] plačiau nagrinėjo 198 ir 198[1] BK straipsnių nusikalstamų veikų sudėties požymius. 2004 m. D. Štitilis kartu su S. Tolušiu mokomajame leidinyje[22] viename iš mokomojo leidinio skyrių nagrinėjo kompiuterinių nusikaltimų sampratą ir jų rūšis, taip pat buvo apžvelgta 2001 m. Konvencija dėl elektroninių nusikaltimų. 2016 m. D. Štitilio mokomajame leidinyje[23] buvo atskleisti interneto teisinio reguliavimo ypatumai, elektroninių ryšių teisinis reguliavimas, intelektinės nuosavybės elektroninėje erdvėje teisinės problemos, devintajame skyriuje nagrinėjami nusikaltimai elektroninėje erdvėje: jų apibrėžimas, ypatumai, teisiniai aspektai. 2019 m. R. Marcinauskaitės monografijoje[24] plačiau nagrinėjamos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui. Labiausiai paplitusio turtinio pobūdžio (BK 178, 180, 181 ir 182) nusikalstamumą analizavo A. Petkus[25], tačiau nebuvo analizuotas sukčiavimas, kaip veika padaryta elektroninėje erdvėje, jo veikimo modeliai.

Užsienyje kibernetinių nusikaltimų problematika mokomajame leidinyje domėjosi J. Graham[26]. Šiame leidinyje analizuojami tiek techninio pobūdžio duomenys, susiję su kibernetiniais nusikaltimais (pvz. *proxy* serverių naudojimas), tiek ir atskleidžiamos nusikalstamos veikos elektroninėje erdvėje tokios kaip – neteisėtas elektroninių mokėjimo priemonių duomenų panaudojimas, nelegaliai įgytų pinigų legalizavimas pasitelkiant trečiuosius asmenis. Įvairių straipsnių rinkinį apie apgaulę, apsimetant įmonės vadovybe yra parašę K. M. Bakarich ir D. Baranek[27] - tirtas apgaulės, apsimetant įmonės vadovybe veikimo modelis, analizuotas „*Ubiquiti*

[19] Darius Štitilis, „Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos“ (daktaro disertacija, Mykolo Romerio Universitetas, 2002), https://www.lvb.lt/permalink/f/1gjkcsi/ELABAETD14382236.

[20] Darius Štitilis ir kt., *Tapatybės Vagystė Elektroninėje Erdvėje: Socialiniai, Elektroninio Verslo Ir Teisinio Reguliavimo Aspektai: Kolektyvinė Mokslo Monografija*. (Vilnius: Mykolo Romerio Universitetas, 2011).

[21] Renata Marcinauskaitė, „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai“ (daktaro disertacija, Mykolo Romerio Universitetas, 2013), https://www.lvb.lt/permalink/f/1gjkcsi/ELABAETD14384562.

[22] Mindaugas Civilka ir kt., *Informacinių technologijų teisė* (Vilnius: NVO Teisės institutas, 2004).

[23] Darius Štitilis ir kt., *Interneto ir technologijų teisė: vadovėlis* (Vilnius: Registrų centras, 2016).

[24] Marcinauskaitė, *supra note,* 1.

[25] Genovaitė Babachinaitė ir kt., *Kriminologija: vadovėlis* (Vilnius: Mykolo Romerio universitetas, 2010), 448.

[26] Rick Howard ir kt., *Cyber fraud: tactics, techniques, and procedures* (New York: CRC Press, 2009).

[27] Kathleen M. Bakarich ir Devon Baranek, „Something Phish-y Is Going On Here: A Teaching Case on Business Email Compromise.“ *Current Issues in Auditing* 14, no. 1 (Spring 2020): A1–9. doi:10.2308/ciia-52706., http://web.b.ebscohost.com/ehost/detail/detail?vid=5&sid=968498f9-5d33-4fad-8968-1cb61faabc20%40pdc-v-sessmgr02&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=bth&AN=143803649.

Networks“ apgaulės atvejis. J. C. Archie, S. Turner, ir T. Wybitul[28] straipsnyje atskleistas apgaulės, apsimetant įmonės vadovybe sukčiavimo veikimo modelis bei pateikiami prevencijos būdai. J. Pringle[29] tyrinėjo apgaulės, apsimetant įmonės vadovybe prevencijos metodus. Tolesni autoriai atskleidė apgaulės, apsimetant įmonės vadovybe veikimo modelį, apgaulės metu padaromą žalą juridiniams asmenims, jų reputacijai - W. Rash[30], J. Rabkin, B. M. Shireen, J. Little, S. L. Shadmand, R. G. Shields, G. P. Silberman, N. J. Stephens, ir kt.[31], S. Polansky[32], B. Zagaris[33], M. R. Davisson ir P. M. Parisi[34]. M. Deliema, D. Shadel ir K. Pak[35] apžvelgė investicijos apgaulės aukų viktimiškumo savybes. V. Bischoff[36] straipsnyje pateikė pavyzdį, kad panaudojant apgaulės, susijusios su investavimu modelį yra pasinaudojama žymių žmonių vardais. J. Hurley[37], R. Pfeil[38] straipsniuose apžvelgtas sukčiavimo, susijusio su netikromis sąskaitomis-faktūromis veikimo modelis, pateikiama statistika apie šio modelio registruotų pranešimų didėjimą. G. Keizer[39] apžvelgė netikros techninės pagalbos skambučių aukų viktimiškumo savybes, J. Gilbert[40] atskleidė

[28] Jennifer C. Archie, Serrin Turner ir Tim Wybitul, „The Pervasive Threat of Business Email Compromise Fraud - and How to Prevent It.“ *Intellectual Property & Technology Law Journal* 32, no. 7 (July 2020): 13–15. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=144723570&site=ehost-live.

[29] Jack Pringle, „Avoiding Business Email Compromise Schemes.“ *Credit Union Times* 30, no. 23 (July 17, 2019): 1–3. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=142355870&site=ehost-live.

[30] Wayne Rash, „FBI Crime Report Lists Business Email Compromise as Top Scam.“ *EWeek*, April 24, 2019, N.PAG. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=136100388&site=ehost-live.

[31] Jeff Rabkin ir kt., „Phishing for Corporate Dollars: The Emerging Global Threat Posed by Spear Phishing and Business Email Compromise.“ *Venulex Legal Summaries*, July 2015, 1–6. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=110358898&site=ehost-live.

[32] Shelley Polansky, „Businesses Warned to Be Wary of Email Compromise Practices.“ *Wyoming Business Report* 20, no. 7 (October 2019): 3–15. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139337266&site=ehost-live.

[33] Bruce Zagaris, „Cybercrime and Fraud,“ *International Enforcement Law Reporter* 35, no. 9 (September 2019): 351-354 https://heinonline-org.skaitykla.mruni.eu/HOL/Page?public=true&handle=hein.journals/ielr35&div=122&start_page=351&collection=journals&set_as_cursor=0&men_tab=srchresults.

[34] Michael Davisson ir Patricia Michelena Parisi, „Imposter Fraud: Courts May Decide This Year on Key Coverage Questions Tied to Email Scams That Dupe Employees into Transferring Company Funds to Fraudsters.“ *Best's Review* 119, no. 3 (March 2018): 22. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=f5h&AN=128201035&site=ehost-live.

[35] Marguerite Deliema, Shadel Doug ir Karla Pak, „Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors.“ *Journal of Consumer Research* 46, no. 5 (February 2020): 904–14. doi:10.1093/jcr/ucz020. http://web.b.ebscohost.com/ehost/detail/detail?vid=21&sid=968498f9-5d33-4fad-8968-1cb61faabc20%40pdc-v-sessmgr02&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=141139652&db=bth.

[36] Victoria Bischoff, „Warning over Investment Scams 'Endorsed by Stars.“ *Daily Mail*, August 14, 2020. http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=145088940&site=ehost-live.

[37] James Hurley, „Rise in Fake Invoice Scams on Small Firms.“ *Times, The (United Kingdom)*, August 25, 2015, 43. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=nfh&AN=7EH103151202&site=ehost-live.

[38] Ryan Pfeil, „Officials Warn of Scam Involving Fake Invoices for School Supplies.“ *Mail Tribune (Medford, OR)*, September 10, 2014. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=nfh&AN=2W63252884655&site=ehost-live.

[39] Gregg Keizer, „Younger Consumers More Likely to Fall for Tech Support Con Jobs.“ *CIO (13284045)*, October 18, 2016, 1. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=bth&AN=118913307&site=ehost-live.

[40] James Gilbert, „Yuma Police Warn about Scam Involving Fake Technical Support Calls.“ *Sun, The (Yuma, AZ)*, September 9, 2013.

netikros techninės pagalbos apgaulės veikimo modelį. A. Coluccia, A. Pozza, F. Ferretti, F. Carabellese, A. Masti ir G. Gualtieri[41] ištyrė meilės nusikaltimų aukų viktimiškumo savybes bei nusikaltėlių charakteristikos bruožus, šia tema taip pat kelis straipsnius parašė M. T. Whitty[42,43,44]. C. Cross, M. Dragiewicz, K. Richards[45] atlikę apklausą taip pat atskleidė meilės nusikaltimų *modus operandi*.

Baigiamojo darbo mokslinis naujumas. Baigiamajame darbe tiriamas sukčiavimų elektroninėje erdvėje *modus operandi*. Anksčiau minėti Lietuvių mokslininkai plačiau nenagrinėjo sukčiavimų metodų elektroninėje erdvėje Lietuvoje. Taip pat atskleidžiama 2014-2019 m. sukčiavimų elektroninėje erdvėje raiška. Analizuojamos aukų viktimiškumo savybės bei nusikaltėlių charakteristika, greta to apžvelgiami veiksniai bei prevencijos metodai ir pateikiami pasiūlymai, kaip gerinti šių nusikalstamų veikų prevenciją ir kontrolę.

Tiriama problema. Tiriama problema gali būti apibrėžiama šiais klausimais: Kokie sukčiavimų modeliai dažniausiai naudojami elektroninėje erdvėje? Kokia yra nusikaltėlio, padariusio sukčiavimus elektroninėje erdvėje asmenybė? Kaip atsiskleidžia sukčiavimų elektroninėje erdvėje laikotarpiu 2014-2019 m. raiška? Kas lemia tai, kad asmenys nukenčia nuo sukčių elektroninėje erdvėje ir praranda lėšas? Kokių prevencijos priemonių galima imtis, kad visuomenė būtų apsaugota nuo elektroninėje erdvėje veikiančių sukčių?

Baigiamojo darbo reikšmė. Teorinė sukčiavimo metodų elektroninėje erdvėje analizė bei registruoto nusikalstamumo statistikos analizė gali būti naudinga teisės taikytojams – teisėsaugoms institucijų pareigūnams, kurie tiria sukčiavimą elektroninėje erdvėje siekiant įvertinti sukčiavimo elektroninėje erdvėje mastą, ikiteisminio tyrimo metu tiksliau nustatyti modernius sukčiavimo elektroninėje erdvėje modelius. Baigiamasis darbas taip pat gali būti naudingas finansinių įstaigų darbuotojams, siekiant atpažinti sukčiavimo metodus bei apsaugoti asmenis nuo turtinės žalos atsiradimo. Darbas taip pat gali būti naudingas fiziniams ir juridiniams

---

http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=nfh&AN=2W61298856560&site=ehost-live.

[41] Anna Coluccia ir kt., „Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review." *Clinical Practice and Epidemiology in Mental Health : CP & EMH* 16 (March 26, 2020): 24–35. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7254823/.

[42] Monica T. Whitty, „Do You Love Me? Psychological Characteristics of Romance Scam Victims." *CyberPsychology, Behavior & Social Networking* 21, no. 2 (February 2018): 105–9. doi:10.1089/cyber.2016.0729. https://www.liebertpub.com/doi/10.1089/cyber.2016.0729.

[43] Monica T. Whitty ir Tom Buchanan, „The online dating romance scam: The psychological impact on victims - both financial and non-financial" *Criminology & Criminal Justice* 16, no. 2 (2016): 176-194. https://heinonline-org.skaitykla.mruni.eu/HOL/Page?public=true&handle=hein.journals/crmcj16&div=13&start_page=176&collection=journals&set_as_cursor=0&men_tab=srchresults.

[44] Monica T. Whitty, „The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam", *The British Journal of Criminology*, Volume 53, Issue 4, July 2013, Pages 665–684, https://doi-org.skaitykla.mruni.eu/10.1093/bjc/azt009.

[45] Cassandra Cross, Molly Dragiewicz ir Kelly Richards, „Understanding Romance Fraud: Insights From Domestic Violence Research", *The British Journal of Criminology*, Volume 58, Issue 6, November 2018, Pages 1303–1322, https://doi-org.skaitykla.mruni.eu/10.1093/bjc/azy005.

asmenims, siekiant suprasti, kokie yra sukčiavimo modeliai bei žinant juos iš anksto imtis prevencijos priemonių bei apsaugoti savo turtinius interesus.

Baigiamojo darbo originalumas. Darbas atliktas savarankiškai remiantis moksline literatūra, registruoto nusikalstamumo statistika bei kitais šaltiniais. Tyrimo metu yra apžvelgti Lietuvos bei užsienio mokslininkų straipsniai, sukčiavimo elektroninėje erdvėje metodai, nusikaltėlių kriminologiniai aspektai, aukų viktimiškumas, registruoto nusikalstamumo statistika, veiksniai, prevencija.

Tyrimo tikslas. Ištirti sukčiavimo elektroninėje erdvėje kriminologinius aspektus ir pateikti siūlymų jų prevencijai.

Tyrimo uždaviniai.

1. Atskleisti teorinius sukčiavimo elektroninėje erdvėje aspektus;
2. Išanalizuoti sukčiavimo elektroninėje erdvėje nusikalstamų veikų raišką 2014–2019 m.;
3. Pateikti asmenų, įtariamų įvykdžius sukčiavimą elektroninėje erdvėje charakteristiką;
4. Pateikti aukų, patyrusių sukčiavimą elektroninėje erdvėje, charakteristiką ir pasekmės jai;
5. Atskleisti veiksnius, nuo kurių priklauso, kodėl žmonės daro sukčiavimą elektroninėje erdvėje;
6. Apžvelgti prevencijos nuo sukčiavimo elektroninėje erdvėje metodus ir pateikti siūlymų prevencijos gerinimui.

Tyrimo metodika. Tiriant pasirinktą problemą ir siekiant išsikelto darbo tikslo, naudoti šie tyrimo metodai: duomenų analizės (tiriant įvairių šalių statistinius duomenis, susijusius su sukčiavimu elektroninėje erdvėje), analogijos (remiantis užsienio mokslininkų tam tikrų sukčiavimo metodų ypatumais, padaromos konkrečios išvados), lyginamasis (lyginant įvairių regionų (Europos - *Europol* ir Jungtinės Karalystės – *Action Fraud*) teisėsaugos institucijų patirtį sukčiavimo elektroninėje erdvėje srityje), mokslinės literatūros ir dokumentų analizės (apibūdinant sukčiavimo elektroninėje erdvėje charakteristiką), loginis metodas (iškeliant tiriamojo darbo tikslus, aiškinant sukčiavimo elektroninėje erdvėje veiksnius, pateikiant išvadas ir pasiūlymus), apibendrinimo metodas (registruoto nusikalstamumo rezultatams įvertinti).

Tyrimo struktūra. Baigiamąjį darbą sudaro įvadas, 6 skyriai, išvados ir pasiūlymai, literatūros sąrašas, anotacija lietuvių ir anglų kalbomis, santrauka lietuvių ir anglų kalbomis. Pirmajame skyriuje yra analizuojami sukčiavimo elektroninėje erdvėje atsiradimas, *modus operandi,* teisiniai aspektai bei žala. Antrajame skyriuje yra pateikiama sukčiavimo elektroninėje erdvėje raiška 2014-2019 m. Trečiajame skyriuje yra pateikiama asmenų, įvykdžiusių sukčiavimą elektroninėje erdvėje charakteristika. Ketvirtajame skyriuje pateikiama aukų, patyrusių

sukčiavimą charakteristika ir pasekmės aukai. Penktajame skyriuje atskleidžiami veiksniai, nuo kurių priklauso, kodėl yra padaromas sukčiavimas elektroninėje erdvėje. Šeštajame skyriuje atskleidžiami prevencijos nuo sukčiavimo elektroninėje erdvėje metodai.

Ginamieji teiginiai.

1. Daugiausia elektroninėje erdvėje sukčiauja vyrai.
2. Sukčiai elektroninėje erdvėje yra jaunesnio amžiaus, nei jų aukos.

1. SUKČIAVIMŲ ELEKTRONINĖJE ERDVĖJE TEORINIAI ASPEKTAI

Technologijų vystymasis mus priartino prie įvairių nusikalstamumo formų atsiradimo[46]. Žmonijai vis dažniau pereinant prie kompiuterizacijos anksčiau tik fizinėje erdvėje padaromos veikos persikėlė į elektroninę erdvę. Anot D. Štitilio: „Elektroninė erdvė suteikia naujų galimybių įvykdyti nusikaltimus, sudaro sąlygas naujiems nusikaltimų būdams atsirasti, be to, sudaro galimybes įvykdyti naujas veikas, iki tol nežinomas teisinėje praktikoje“[47]. Nusikaltimai elektroninėje erdvėje, įskaitant ir sukčiavimą gali būti įvykdomi iš bet kurios pasaulio vietos. Taip pat elektroninėje erdvėje, kaip socialinėje aplinkoje niekada negalima būti tikram, ar bendraujama su tuo asmeniu, su kuriuo ir manoma, kad bendraujama. Elektroninėje erdvėje galima būti bet kuo. Pavyzdžiui, 2019 m. tarp sausio ir kovo mėn. socialinis tinklas *Facebook* panaikino daugiau nei 2 mlrd. netikrų paskyrų[48]. Natūralu, kad asmenys tokio pobūdžio anketas kuria ne vien nekaltais tikslais, bet ir vykdyti nusikalstamo pobūdžio veikas, pavyzdžiui, sukčiavimą.

Europos Taryba su valstybėmis narėmis matydamos dėl kompiuterizacijos vykstančias permainas bei matydamos, kad kompiuteriniai tinklai bei juose esanti informacija gali būti naudojama nusikaltimams vykdyti 2001 m. pasirašė Konvenciją dėl elektroninių nusikaltimų[49]. Šios Konvencijos 8 straipsnyje yra įtvirtinta „Kompiuterinio sukčiavimo“ nusikalstama veika: „[...] sąmoningus ir neteisėtus veiksmus, sąlygojusius kito asmens nuosavybės praradimą: a) įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis; b) paveikiant kompiuterinės sistemos darbą, nesąžiningai arba nedorai ketinant gauti neteisėtos ekonominės naudos sau arba kitam asmeniui.“ Tai Europos Sąjungos mastu buvo pirmasis dokumentas, siekiant kovoti su nusikaltimais elektroninėje erdvėje. Kaip matyti, kompiuterinis sukčiavimas šios Konvencijos kontekste suprantamas kaip 1. informacinės sistemos duomenų pakeitimas arba jų panaikinimas, siekiant nesąžiningai gauti ekonominės naudos sau arba kitam asmeniui 2. informacinės sistemos darbo paveikimas siekiant nesąžiningai gauti ekonominės naudos sau ar kitam asmeniui. Konvencijos 8 straipsnio a) dalyje yra įtvirtintas paprastas sukčiavimas, pasinaudojant kompiuteriniais tinklais.

LR BK[50] sukčiavimas yra įtvirtintas skyriuje XXVIII skyriuje „Nusikaltimai ir baudžiamieji nusižengimai nuosavybei, turtinėms teisėms ir turtiniams interesams“ 182 straipsnyje. Šio straipsnio pirmojoje dalyje yra numatyta atsakomybė už paprastą sukčiavimą,

---

[46] George E. Higgins, *Cybercrime: an introduction to an emerging phenomenon* (Boston: McGraw-Hill Higer Education, 2010), 1.
[47] Darius Štitilis, *Elektroniniai nusikaltimai: metodinė priemonė* (Vilnius: Mykolo Romerio universitetas, 2011), 5.
[48] Craig Silverman, „Facebook Removed Over 2 Billion Fake Accounts, But The Problem Is Getting Worse“, *Buzzfeed news*, 2019 m. gegužės 24 d., https://www.buzzfeednews.com/article/craigsilverman/facebook-fake-accounts-afd
[49] 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų (Žin., 2004, Nr. 36-1188).
[50] Lietuvos Respublikos baudžiamasis kodeksas (Žin., 2000, Nr. 89-2741).

antrojoje – kvalifikuotą, trečiojoje – baudžiamąjį nusižengimą. Esminis sukčiavimo, kaip nusikalstamos veikos skirtumas nuo kitų LR BK XXVIII numatytų veikų yra apgaulės naudojimas prieš turto savininką. Apgaulė sukčiavimo atveju naudojama kaip turto užvaldymo būdas (Lietuvos Aukščiausiojo Teismo 2012 m. rugsėjo 7 d. Teismų praktikos sukčiavimo baudžiamosiose bylose (BK 182 straipsnis) apžvalga Nr. AB-36-1). Lietuvos Aukščiausiojo Teismo atrankos kolegijos 2019 m. gruodžio 19 d. nutartyje išaiškinta, kad: „apgaulė sukčiaujant ***panaudojama turint tikslą suklaidinti*** turto savininką, valdytoją, asmenį, kurio žinioje yra turtas (įskaitant banką), [...] o ***pastarasis, suklaidintas apgaulės, savanoriškai pats perleidžia turtą*** ar turtinę teisę kaltininkui manydamas, kad šis turi teisę jį gauti, arba panaikina jo turtinę prievolę, arba priima sprendimą dėl nukentėjusiojo turto, turtinės teisės perleidimo kaltininkui ar kaltininko turtinės prievolės panaikinimo“[51]. Atskirai sukčiavimas, kaip veika, padaryta elektroninėje erdvėje, LR BK nėra kriminalizuotas.

Baigiamajame darbe toliau bus palyginami Švedijos ir Jungtinės Karalystės baudžiamuosius teisinius aspektus sukčiavimo elektroninėje erdvėje srityje su Lietuvos baudžiamaisiais teisiniais aspektais. Švedijos Karalystės baudžiamajame kodekse[52] sukčiavimas, kaip veika yra nustatyta IX skyriuje pavadinimu „Sukčiavimas ir kitas nesąžiningumas“, 1-3a dalyse. 1 dalyje įtvirtinta paprasta sukčiavimo norma, kurioje nustatyta, jog tas, kas apgaule įgijo svetimą turtą, dėl kurio auka prarado turtą baudžiamas laisvės atėmimu iki 2 metų. Tas, kas pateikia neteisingą informaciją ar suklaidina informacinę sistemą, dėl ko gauna turtinės naudos, o auka praranda turtą taip pat atsako už sukčiavimą. 2 dalyje numatyta privilegijuota sukčiavimo norma, kur nustatyta, jog jeigu nusikaltimas, padarytas 1 dalyje padaro mažą turtinę žalą, asmuo baudžiamas bauda arba laisvės atėmimu iki 6 mėn. Asmuo, kuris paskelbdamas informaciją apie teikiamas apgyvendinimo, maitinimo, pervežimo ar kitas panašias paslaugas ir priėmęs pinigus šių paslaugų nesuteikia, taip pat atsako pagal šį straipsnį, nebent žala nėra maža, tuomet asmuo atsako pagal 1 šio skyriaus dalį. 3 dalyje įtvirtinta kvalifikuota sukčiavimo sudėtis bei šioje dalyje įtvirtinta, kad tas, kas padarė šio skyriaus 1 dalyje numatytus veiksmus ir įgijo didelės vertės turtą baudžiamas laisvės atėmimu nuo 6 mėn. iki 6 metų. Kai yra spendžiama dėl didelės vertės turto, atsižvelgiama į tai ar nukentėjo visuomenė, ar kaltininkas naudojo specialius įrankius tikslui pasiekti. Šio skyriaus 3a dalyje yra įtvirtinta kvalifikuota sukčiavimo, nukreipto į netikrų sąskaitų faktūrų siuntimą ir didelės žalos padarymą, sudėtis. Būtent ši sukčiavimo norma gali būti vykdoma išimtinai elektroninėje erdvėje, kas Švedijoje įtvirtintą sukčiavimą iš esmės ir skiria nuo LR BK įtvirtinto sukčiavimo.

[51] Lietuvos Aukščiausiojo Teismo atrankos kolegijos 2019 m. gruodžio 19 d. nutartis Nr. 2K-303-693/2019.
[52] The Swedish Criminal Code (brottsbalken, SFS 1962:700), žiūrėta 2020 m. spalio 1 d., https://www.government.se/4a8349/contentassets/7a2dcae0787e465e9a2431554b5eab03/the-swedish-criminal-code.pdf.

Lyginant paprastą sukčiavimą, Švedijos Karalystėje yra nustatytas laisvės atėmimas iki 2 metų, kai Lietuvoje – iki 3 metų. Lyginant kvalifikuotą sukčiavimą, Švedijos Karalystėje – laisvės atėmimas nuo 6 mėn. iki 6 metų, kai Lietuvoje – laisvės atėmimas iki 8 metų. Lyginant priveligijuotą sukčiavimą, Švedijos Karalystėje – bauda arba laisvės atėmimas iki 6 mėn., kai Lietuvoje tai yra vertinama kaip baudžiamasis nusižengimas nustatant alternatyvias bausmes – baudą, viešuosius darbus, laisvės apribojimą arba areštą. Palyginus nustatytas bausmes, galima teigti, jog Švedijos Karalystėje sukčiavimo veika numatytos maženės bausmės nei Lietuvoje.

Švedijos Karalystėje sukčiavimas, nustatytas Švedijos BK 9 sk. 1-3 dalyse registruoto nusikalstamumo statistikoje nuo 2019 m.[53] yra išskiriamas į grupes – „Romantinis“ sukčiavimas, sukčiavimas, susijęs su investicijomis, sukčiavimas, apsimetant įmonės vadovu, kiti sukčiavimai, pasinaudojant socialine inžinerija, sukčiavimai nukreipti į tapatybę sudarančių duomenų vagystę, sukčiavimai, nukreipti į apgaulingas sąskaitas – faktūras, sukčiavimai, susiję su banko mokėjimo kortelėmis, sukčiavimai, susiję su prekių nepateikimu galutiniam vartotojui. Kiekviena grupė taip pat padalinta į pogrupius – prieš asmenį su negalia/senyvą asmenį, prieš fizinių/psichinių negalių neturintį asmenį. Taip pat sukčiavimų registruotoje statistikoje išskiriami ir kiti sukčiavimai. Manytina, jog Švedijos Karalystės institucijų žingsnis išskirti sukčiavimą į grupes naudojant tarptautinėje erdvėje esančius sukčiavimo modelių pavadinimus aiškiau atvaizduoja kiekvieno sukčiavimo modelio raišką, kiek asmenų praneša teisėsaugos institucijoms apie patirtą turtinę žalą.

Jungtinėje Karalystė sukčiavimas yra įtvirtintas Sukčiavimo akte[54]. Sukčiavimo akto 1 str. yra nustatyti trys būdai: atstovavimo sukčiavimas (kai asmuo nesąžiningai save pristato su tikslu gauti sau ar kitam asmeniui turtinės naudos arba pakenkti kitam asmeniui ar sukelti pavojų padaryti turtinę žalą), sukčiavimas neatskleidžiant informacijos (kai asmuo nutyli informaciją, kurią pagal teisinį pagrindą privalėjo pranešti su tikslu gauti sau ar kitam asmeniui turtinės naudos arba pakenkti kitam asmeniui ar sukelti pavojų padaryti turtinę žalą) ir sukčiavimas, naudojantis turimomis pareigomis (kai asmuo, pasinaudoja savo turimomis pareigomis su tikslu gauti sau ar kitam asmeniui turtinės naudos arba pakenkti kitam asmeniui ar sukelti pavojų padaryti turtinę žalą). Asmuo, padaręs šias alternatyvias nusikalstamas veikas baudžiamas laisvės atėmimu iki 12 mėn. arba bauda, arba ir bauda ir laisvės atėmimu iki 12 mėn. (esant sumariniam procesui), arba esant įprastam procesui – bauda arba laisvės atėmimu iki 10 metų, arba ir bauda ir laisvės atėmimu iki 10 metų. Lyginant Jungtinėje Karalystėje bausmę su LR BK 182 numatyta bausme, galima teigti, jog Jungtinėje Karalystėje sukčiavimo veika numatyta didesnė bausmė nei Lietuvoje.

[53] „Swedish National Council for Crime Prevention (Brå), Total number of reported offences 2019“, BRA, žiūrėta 2020 m. spalio 1 d., https://www.bra.se/download/18.7d27ebd916ea64de5304e143/1585655101251/Total_number_of_reported_offences_2019.xls.

[54] „Fraud act 2006“, žiūrėta 2020 m. spalio 2 d., https://www.legislation.gov.uk/ukpga/2006/35/contents.

LR BK 182 str. 2 d. kvalifikuotas sukčiavimu nustatyta bausmė iki 8 metų, kai Jungtinėje Karalystėje įprastu sukčiavimu iki 10 metų ir greta to papildomai gali būti skiriama bauda. Atskirai sukčiavimas, kaip veika padaryta išimtinai elektroninėje erdvėje Jungtinėje Karalystėje taip pat nėra kriminalizuota.

Toliau baigiamajame darbe bus atskleidžiami sukčiavimų, elektroninėje erdvėje modeliai juos išskiriant į sukčiavimus, nukreiptus į fizinius asmenis bei sukčiavimus nukreiptus į juridinius asmenis. Sukčiavimai, nukreipti į fizinius asmenis elektroninėje erdvėje šiame baigiamajame darbe apima: sukčiavimas, susijęs su investavimu, apgaulingi elektroniniai laiškai, SMS žinutės ir skambučiai, „romantinis“ sukčiavimas. Sukčiavimai, nukreipti į juridinius asmenis elektroninėje erdvėje šiame baigiamajame darbe apima: sukčiavimas, apsimetant įmonės vadovu, sukčiavimas, susijęs su verslo partnerio banko sąskaitos pasikeitimu. Dėl baigiamojo darbo apimties bei sukčiavimo elektroninėje erdvėje modelių įvairovės ir naujų modelių atsiradimų, baigiamajame darbe bus nagrinėti tik aukščiau minėti, praktikoje dažniausiai pasitaikantys sukčiavimo elektroninėje erdvėje modeliai.

Sukčiavimas, susijęs su investavimu – tai toks sukčiavimo modelis, kurio metu auka apgaule yra įtikinama, kad investavus savo lėšas į kriptovaliutas ar kitokius sudėtingai atsekamus finansinius instrumentus, atgaus neįtikinamai didelę grąžą per trumpą laikotarpį. Kaip teigia N.Roubini, „kriptovaliuta yra visų sukčiavimų motina“ taip pat jis pacitavo *Satis Group* tyrimą, kuriame teigiama, jog 81 proc. kriptovaliutų buvo sukurtos, siekiant apgaule įgyti žmonių lėšas, 11 proc. kriptovaliutų nebėra arba jos prie žlugimo ribos ir tik 8 proc. valiutų išliko bei jomis vyksta prekyba[55]. Kaip teigia S. D. Brown, *Bitcoin* kriptovaliuta tapo nusikaltėlių elektroninėje erdvėje valiuta. Ji yra decentralizuota, pusiau-anoniminė, taip pat ši valiuta buvo įvertinta kaip turinti mažą pinigų plovimo riziką[56]. Panašią nuomonę turi ir K. Driscoll. Ji teigia, jog kriptovaliutos nėra reguliuojamos jokių oficialių institucijų ar valdžios. Nepaisant to, kad vietiniai kriptovaliutos naudotojai mano, jog kriptovaliutomis naudojasi ir daugybė jokių nusikalstamų tikslų neturinčių vartotojų, tačiau kriptovaliutų pervedimo greitis bei pervedimų sąlyginis slaptumas taip pat pritraukė ir nusikaltėlius[57]. Taigi kriptovaliutomis nusikaltėliai naudojasi pagrinde dėl šių priežasčių: kriptovaliutos pervedimo neįmanoma atšaukti, kriptovaliutos yra

[55] Melanie Waddell, „Cryptocurrencies Are the ‘Mother of All Scams“: Testifying before the Senate Banking Committee, a Popular Academic Also Lays into Blockchain and Argues the ‘Real Revolution’ Is in Fintech.“ *Investment Advisor*, (November 2018): 1. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=132741339&site=ehost-live.

[56] Steven David Brown, „Cryptocurrency and Criminality: The Bitcoin Opportunity,“ *Police Journal* 89, no. 4 (December 2016): 327. https://heinonline-org.skaitykla.mruni.eu/HOL/Page?collection=journals&handle=hein.journals/policejl89&id=323&men_tab=srchresults.

[57] Kara Driscoll, „Crime and Cryptocurrency: How Local Criminals Use Bitcoin Illegally.“ *Dayton Daily News (OH)*, December 22, 2017. http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=2W61703430549&site=ehost-live.

sunkiai atsekamos, pervedimas įvykdomas per trumpą laiko tarpą. Prieš asmenis, sumaniusius investuoti į kriptovaliutas apgaulė gali būti panaudota šiais atvejais: 1) kai investuojama į nerentabilią, nesaugią kriptovaliutą, kurios ateitis, kaip finansinio instrumento, neaiški. 2) kai manoma, jog investuojama į saugią kriptovaliutą, bet investicijų portfelį valdo ne pats investuotojas, o trečiasis asmuo. Toliau baigiamajame darbe bus atskleisti šie du sukčiavimo, susijusio su investavimu būdai.

Kai investuojama į nerentabilią, nesaugią kriptovaliutą. Remiantis *Coinlore*[58] kriptovaliutų biržos pateiktais duomenimis, 2020 m. rugsėjo 28 d. pasaulyje iš viso buvo 5013 kriptovaliutos, kurių bendra kapitalizacijos vertė apie 357,5 mlrd. JAV dolerių. Kiekviena nauja kriptovaliuta, norėdama pritraukti vartotojų investicijas išleidžia *ICO*[59] (liet. *pirminis tokenų siūlymas*). Asmenys, investavę į naują kriptovaliutą gauna tos kriptovaliutos vienetų ir jiems suteikiama galimybė laukti bei ateityje parduoti kriptovaliutą už didesnę kainą. Tačiau ne visos kriptovaliutos būna sėkmingos. Kai kurios būna sukurtos tam, kad apgaule įgyti žmonių investicijas. Apgaulė šiuo atveju yra nukreipta į tyčinį investuotojo suklaidinimą, tikslą negrįžtamai investuotojo lėšas paversti savo nuosavybe. Pavyzdžiui, *Envion* surinko daugiau nei 100 mln. JAV dolerių iš investuotojų, siekiant sukurti švaresnę energiją kompiuterinei įrangai, kuri valdo *Bitcoin* kriptovaliutą. *Envion* kriptovaliuta žlugo ir investuotojai liko nežinioje, ar pavyks atgauti nors dalį pinigų[60].

Kai manoma, jog investuojama į saugią kriptovaliutą, bet investicijų portfelį valdo ne pats investuotojas, o trečiasis asmuo. Šis apgaulės metodas toliau bus aiškinamas per interviu, su sukčiavimo, susijusio su investavimu, auka[61]. Asmeniui, sulaukus skambučio į savo telefoną, jam yra pasiūloma investuoti į kriptovaliutą su didžiule finansine grąža. Pradžioje investuotojo paprašoma pervesti pradinį registracijos mokestį į sukčių valdomą banko sąskaitą. Aukai yra sukuriama anketa, netikrame sukčių tinklalapyje tiesiogiai skirtam daryti nusikalstamą veiką, numatytą BK 182 straipsnyje. Kai auka perveda pinigus į sukčių nurodytą sąskaitą, ši suma yra atvaizduojama sukčių sukurtame tinklalapyje. Aukai apgaulingai yra pateikiama investicijų grąža, neva, jos investicija padidėja keliasdešimt procentų per trumpą laiko tarpą. Sukčius vėl bendrauja su auka telefonu ir bando ją apgaule įtikinti, jog laikas investuoti daugiau lėšų, tai tik trumpalaikis pasiūlymas. Tačiau besikeičianti, didėjanti suma sukčių sukurtame investicijų tinklalapyje yra skirta tik suklaidinti auką. Jeigu auka pabando išsiimti pinigus, jai pranešama, kad investicija žlugo ar sukčių sukurtas tinklalapis panaikinamas.

---

[58] „Coinlore.com, list of all cryptocurrency“, Coinlore, žiūrėta 2020 m. rugsėjo 28 d., https://www.coinlore.com/all_coins.
[59] „Kas tai, ICO?“, Kriptoinfo, žiūrėta 2020 m. rugsėjo 28 d., https://www.kriptoinfo.lt/page/kas-tai-ico.
[60] Nathaniel Popper, „When Good Crypto Investment Goes Bad.“ *Toronto Star (Canada)*, June 2, 2018. http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=6FPTS2018060246091442&site=ehost-live.
[61] „Senolė pardavė butą ir sukčiam pervedė 36 000 EUR“, *Supra note* 12.

Greta sukčiaus skambučio telefonu auka investicijų pasiūlymą gali pamatyti elektroninėje erdvėje, tam gali būti pasitelkiami žymūs, visuomenėje pasitikėjimą turintys asmenys[62]. Pavyzdžiui, sukčiai neteisėtai paveikę informacinę sistemą *Twitter* per joje esančius oficialius žymių asmenų profilius patalpino apgaulingą pranešimą, kad B. Obama, E. Musk, J. Biden ir J. Bezos savo sekėjams siūlo investuoti į *Bitcoin* kriptovaliutą ir ribotam asmenų kiekiui pervedus pinigų sumą šie pinigai padvigubės. Tačiau paveikus informacinę sistemą *Twitter* pinigus buvo prašoma pervesti ne į minėtų asmenų privačias kriptovaliutų pinigines, o į sukčių sukurtas pinigines. Sukčiai per kelias valandas, kol buvo pastebėtas neteisėtas poveikis informacinei sistemai apsimesdami žymiais žmonėmis įgijo daugiau nei 100 tūkst. JAV dolerių.

Taigi sukčiavimo modelis, susijęs su investavimu šiuo moderniu laikotarpiu vykdomas pasitelkiant sudėtingai atsekamą kriptovaliutų tinklą bei inovatyvius apgaulės metodus. Sukčiai gali su auka susisiekti tiesiogiai ir taip išreikšti pasiūlymą investuoti arba auka gali aptikti neįtikėtinai pelningą pasiūlymą investuoti elektroninėje erdvėje.

Sukčiavimas, pasitelkiant apgaulingus laiškus, SMS žinutes ir skambučius. Šis apgaulės modelis yra glaudžiai susijęs su asmens tapatybe elektroninėje erdvėje. Kaip teigia D. Štitilis: „Elektroninėje erdvėje tapatybę gali atstoti vardas ir slaptažodis: vardas – kokio nors objekto sutartinis tą objektą vienareikšmiškai identifikuojantis pavadinimas, kuris sistemoje turi būti unikalus; slaptažodis – ženklų seka, žinoma tik paslaugų teikėjui ir jos vartotojui, pagal kurią paslaugos teikėjas patikrina į jį besikreipiančiojo tapatybę“[63]. Sukčiai elektroninėje erdvėje neabejotinai siekia turtinės naudos, todėl norint ją įgyti apgaunant banką kaltininkai turi įgyti asmens tapatybę identifikuojančius duomenis. Asmeniui norint naudotis elektronine bankininkyste jis turi pasirašyti paslaugų teikimo sutartį, pagal kurią išduodami identifikavimo kodai. Pavyzdžiui, remiantis SEB banko bendrosiomis paslaugų teikimo taisyklėmis, kliento identifikavimo priemonės apibūdinamos kaip: „Kliento ar jo atstovo parašas, elektroninis parašas, klientui suteiktas asmens atpažinimo kodas (PIN kodas) arba kita priemonė (slaptažodžiai, kodai, raktai ar kt.), kuri banko ir kliento sutartu būdu naudojama klientui arba jo atstovui atpažinti“[64]. Panašaus pobūdžio taisykles turi ir kiti finansinių paslaugų teikėjai, pavyzdžiui *Paypal* platforma

[62] Margaret Brennan ir Kris Van Cleave, „High-Profile Twitter Accounts Hacked in Cryptocurrency Scam.“ *CBS Evening News with Katie Couric*. Accessed September 28, 2020. http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=32U2663153790CB3&site=ehost-live. Ir William Turton, „Twitter Cryptocurrency Scam Echoes Previous Schemes on YouTube.“ *Bloomberg.Com*, July 23, 2020, N.PAG. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=144732153&site=ehost-live, Lietuvoje, pvz. https://www.60plius.lt/2019/11/26/a-sabonis-nekviecia-investuoti/, https://www.delfi.lt/partnerio-turinys/sustiprink-imuniteta/suklastoti-portalai-lietuvos-izymybiu-veidai-ir-greitas-uzdarbis-sveiki-pateke-i-naujausias-sukciu-pinkles.d?id=85018947.

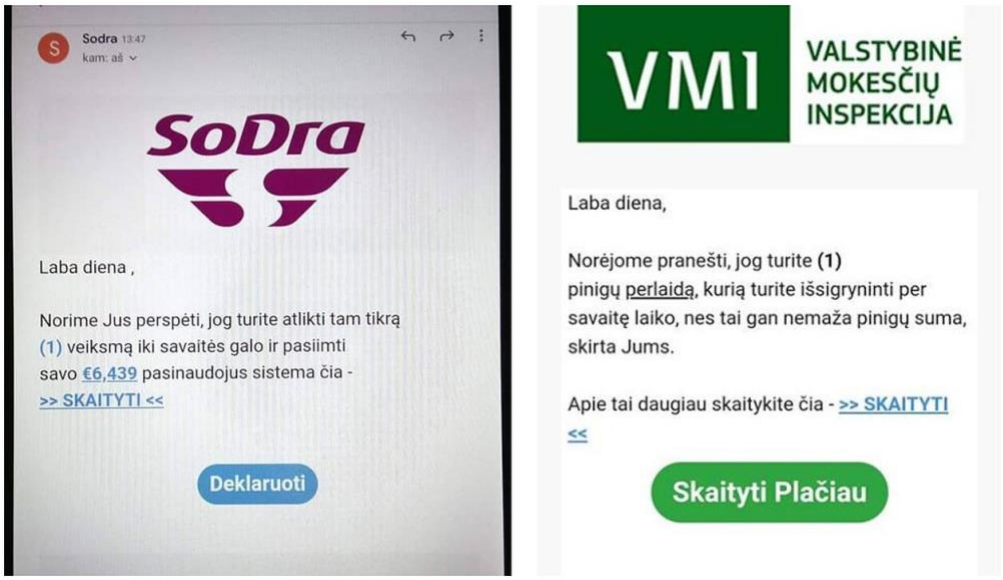
[63] Štitilis ir kt., *supra note*, 20: 34.

[64] „AB SEB banko bendrosios paslaugų teikimo taisyklės“, SEB bankas, žiūrėta 2020 m. rugsėjo 28 d., https://www.seb.lt/sites/default/files/web/pdf/Bendrosios_taisykles_2017_06_12.pdf.

asmens autentifikacijai naudoja elektroninį paštą kaip prisijungimo vardą bei slaptažodį[65]. Greta įprasto prisijungimo vardo bei slaptažodžio, finansinės įstaigos kaip papildomą autentifikavimo priemonę naudoja mobilųjį parašą, SMART-ID arba generatorių. Įgijus šiuos tapatybę patvirtinančius duomenis, kaltininkai gali inicijuoti neteisėtą lėšų pervedimą iš aukos sąskaitos. Toliau baigiamajame darbe bus aptarti trys tapatybę patvirtinančių duomenų įgijimo apgaule būdai – fišingas (angl. *phishing*), smišingas (angl. *smishing*) ir višingas (angl. *vishing*).

Asmens tapatybę patvirtinančių duomenų įgijimas, pasinaudojant fišingu. Kaip teigia V. M. Vilic, fišingas suprantamas kaip elektroninio laiško siuntimas vartotojui, jį atvaizduojant taip, kad vartotojui atrodytų, jog laišką siuntė teisėtas siuntėjas, siekiant įgyti asmeninę, konfidencialią informaciją[66]. Tokio tipo elektroniniai laiškai gali atrodyti siunčiami finansų įstaigos ar valstybinės institucijos. Dažniausiai fišingo laiškus galima atpažinti iš prastos gramatikos, taip pat juose gali būti raginama sukčių prašymą įvykdyti nedelsiant. Toliau bus aptarti fišingo laiškai siųsti Lietuvos gyventojams.

1 pav. Fišingo laiškų pavyzdžiai[67]



Kaip matyti, fišingo elektroniniame laiške iš „SODROS“ atrodo, jog laiškas iš tikrųjų buvo siųstas „SODROS“, kadangi laukelyje „iš“ matomas „Sodra“ pavadinimas. Tačiau tokius apgaulingus laiškus išduoda gramatinės klaidos. Pavyzdžiui, „SODROS“ laiške po kreipinio „Laba diena“ yra padėtas tarpas ir tik po to kablelis, taip pat nelogiškai skamba pats sakinys, atrodo lyg būtų išverstas vertėjo pagalba. Apgaulingas laiškas iš „VMI“ savo turiniu labai panašus į laišką

[65] „Key Payment and Service Information“, Paypal, žiūrėta 2020 m. spalio 1 d., https://www.paypal.com/uk/webapps/mpp/ua/servicedescription-full#6.
[66] Vida M. VILIĆ, „Phishing and Pharming as Forms of Identity Theft and Identity Abuse.“ *Balkan Social Science Review* 13, no. 13 (June 2019): 46. http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=140388562&site=ehost-live.
[67] „Netikri laiškai iš „Sodros“ ir VMI galėjo būti užsienio sukčių darbas“, LRT, žiūrėta 2020 m. spalio 1 d., https://www.lrt.lt/naujienos/verslas/4/1051818/netikri-laiskai-is-sodros-ir-vmi-galejo-buti-uzsienio-sukciu-darbas.

iš „SODROS“, todėl galima manyti, jog šiuos laiškus siuntė tie patys sukčiai, siekdami įgyti asmens tapatybę identifikuojančius duomenis.

2 pav. Fišingo laiško pavyzdys[68]

Fišingo laiškas, kuris atrodė galimai siųstas iš „VMI“, buvo patalpintas *Facebook* „VMI“ paskyroje. Šiame laiške matyti taisyklinga gramatika, tačiau informaciją, kad laiškas siųstas sukčių, siekiant įgyti tapatybę patvirtinančius duomenis parodo „iš“ laukelyje matomas elektroninio pašto adresas *@vrni.lt*. „R” ir „n” raidės šalia viena kitos atrodo labai panašios į „m“ raidę, todėl adresas tesiskiria keliais simboliais ir įprastam vartotojui gali būti net nepastebėtinas.

Atidarius tokį fišingo laišką, atitinkamai nukreipiama į sukčių sukurtą „SODROS“ ar „VMI“ tinklalapį, kuris gali atrodyti sekančiai: *www-sodra-lt.bitly.ly* ar *vrni.lt*, kas įprastam vartotojui gali pasirodyti, jog siekiant atnaujinti prašomus duomenis buvo nukreipta į tikrą tinklalapį. Tačiau atidarius tokį tinklalapį bus paprašyta prisijungti prie „SODRA“ ar „VMI“ paskyros. Prisijungimas prie šių paslaugų gali būti vykdomas per SMART-ID programėlę, kur sukčiai gali susižinoti asmens tapatybę patvirtinančius duomenis ir vėliau su tais duomenimis mėginti prisijungti prie elektroninės bankininkystės ir taip apgaule įgyti svetimas lėšas.

Asmens tapatybę patvirtinančių duomenų įgijimas, pasinaudojant smišingu. Kaip teigia D. Pinington smišingas suprantamas kaip fišingo atmaina, tačiau skirtingai nei fišingas, jis vykdomas SMS žinutėmis[69]. Auka į savo mobilųjį įrenginį gauna apgaulingą SMS žinutę, neva iš paslaugų teikėjo su nuoroda, kurią atidarius prašoma atnaujinti savo duomenis. Toliau panagrinėsiu smišingo atakas, nukreiptas į Lietuvos gyventojų tapatybę patvirtinančių duomenų įgijimą.

[68] Šaltinis: Facebook, „VMI“ paskyra.
[69] Dan Pinnington, „Financial Fraudsters Want You: Avoiding Scams Targeting Lawyer Trust Accounts.“ *Law Practice: The Business of Practicing Law* 46, no. 5 (September 2020): 1–15. http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=145417888&site=ehost-live.

3 pav. Smišingo žinutės pavyzdys[70]

Kaip matyti šioje apgaulingoje smišingo žinutėje, ji atrodo siųsta pačio SEB banko, tačiau SEB bankas savo siunčiamose žinutėse neprašo spausti ant joje esančių nuorodų. Taip pat žinutė yra labai nekonkreti ir įprastas vartotojas, vedamas smalsumo gali mėginti paspausti nuorodą, siekiant sužinoti, kokio pobūdžio naujas pranešimas yra gautas. Paspaudus tokio tipo nuorodą yra nukreipiama į netikrą elektroninę SEB banko svetainę ir prašoma prisijungti naudojantis kliento tapatybę patvirtinančiais duomenimis bei atnaujinti savo asmeninę informaciją. Įgijus šiuos duomenis sukčiai gali prisijungti prie asmens bankininkystės bei neteisėtai įgyti lėšas.

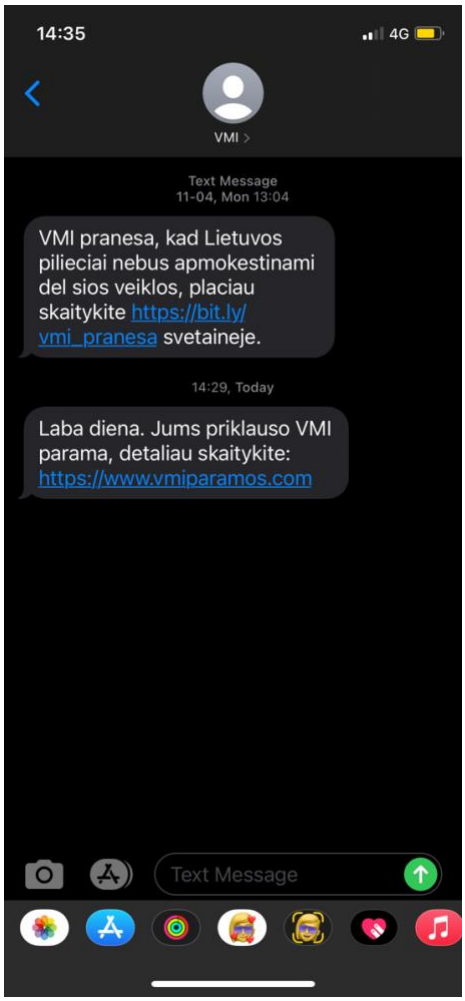
Pavyzdžiui, kaip teigia *Europol*, smišingo žinutes, nukreiptas į finansinių įstaigų vartotojus Lietuvoje bei Estijoje siuntė sukčiai iš Rumunijos. Smišingo žinutėse buvo atvaizduojamos nuorodos į netikrus finansinių įstaigų tinklalapius, kur sukčiai įgijo SMART-ID bei kliento tapatybę patvirtinančius duomenis. Šiais duomenimis pasinaudodami kibernetiniai nusikaltėliai apgaule įgijo daugiau nei 200 tūkst. eurų iš 600 aukų, iš kurių 500 - Estijoje bei 100 - Lietuvoje. Dėka finansinių įstaigų darbuotojų greito sureagavimo pavyko išvengti daugiau nei 450 tūkst. eurų nuostolių[71].

Smišingo žinutes yra gavęs ir baigiamojo darbo autorius (žr. 4 pav.). Jos abi buvo siųstos neva „VMI“. Kaip matyti, šias žinutes skiria mažiau nei metai. Pirmoji buvo gauta 2019-11-04, o antroji 2020-10-01. Abejose smišingo žinutėse siūloma detalesnės informacijos ieškoti minėtuose tinklalapiuose. Pirmasis tinklalapis atvaizduojamas pasitelkiant elektroninėje erdvėje esančių adresų (angl. *domain*) keitimo paslauga *bit.ly*. Antruoju atveju yra sukurtas atskiras

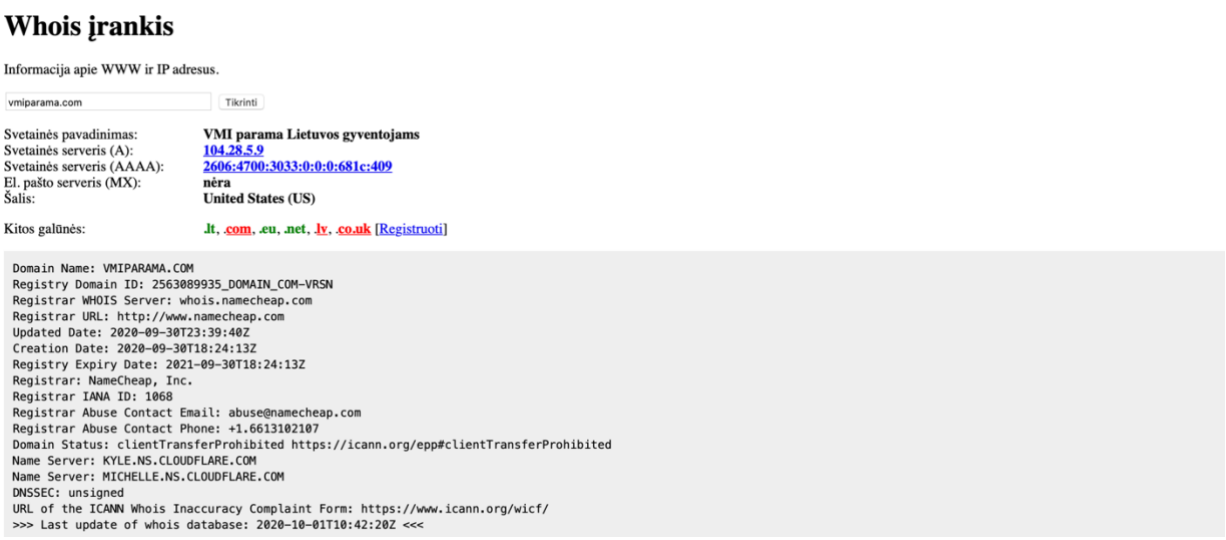
[70] SEB bankas.
[71] „Hook, line and sinker: Cybercrime network phishing bank credentials arrested in Romania“, Europol, žiūrėta 2020 m. spalio 2 d., https://www.europol.europa.eu/newsroom/news/hook-line-and-sinker-cybercrime-network-phishing-bank-credentials-arrested-in-romania.

internetinis adresas www.vmiparama.com. Pasinaudojus viešai prieinama internetinių adresų tikrinimo paslauga „WHOIS“ matyti, jog internetinis adresas įkurtas 2020-09-30, t.y. dieną prieš smišingo ataką (žr. 5 pav.)

4 pav. Smišingo žinutės pavyzdys



5 pav. Informacija apie www.vmiparama.com sukčių tinklalapį[72]



Whois įrankis

Informacija apie WWW ir IP adresus.

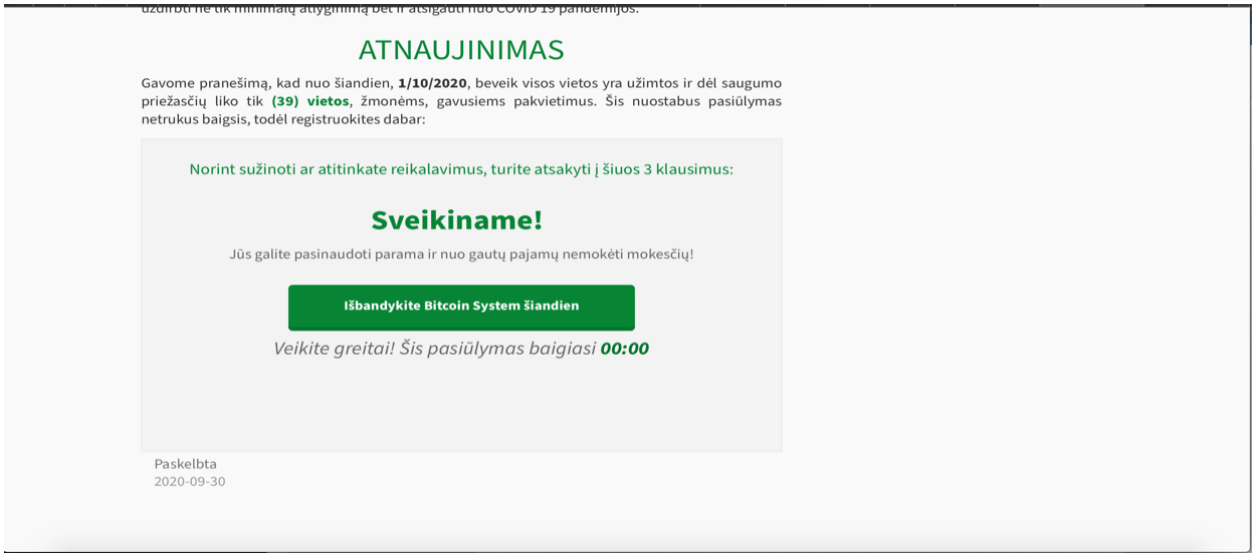
vmiparama.com Tikrinti

Svetainės pavadinimas:	**VMI parama Lietuvos gyventojams**
Svetainės serveris (A):	104.28.5.9
Svetainės serveris (AAAA):	2606:4700:3033:0:0:0:681c:409
El. pašto serveris (MX):	**nėra**
Šalis:	**United States (US)**
Kitos galūnės:	.lt, .com, .eu, .net, .lv, .co.uk [Registruoti]

```
Domain Name: VMIPARAMA.COM
Registry Domain ID: 2563089935_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2020-09-30T23:39:40Z
Creation Date: 2020-09-30T18:24:13Z
Registry Expiry Date: 2021-09-30T18:24:13Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: KYLE.NS.CLOUDFLARE.COM
Name Server: MICHELLE.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-10-01T10:42:20Z <<<
```

Atidarius minėta sukčių sukurtą tinklalapį siūloma atsakyti į tris klausimus bei sužinoti, ar dar liko vietų investicijų platformoje. (žr. 6 pav.)

6 pav. Sukčiavimo susijusio su investicijomis tinklalapio fragmentas[73]



uždirbti ne tik minimalų atlyginimą bet ir atsigauti nuo COVID 19 pandemijos.

ATNAUJINIMAS

Gavome pranešimą, kad nuo šiandien, **1/10/2020**, beveik visos vietos yra užimtos ir dėl saugumo priežasčių liko tik **(39) vietos**, žmonėms, gavusiems pakvietimus. Šis nuostabus pasiūlymas netrukus baigsis, todėl registruokites dabar:

Norint sužinoti ar atitinkate reikalavimus, turite atsakyti į šiuos 3 klausimus:

Sveikiname!

Jūs galite pasinaudoti parama ir nuo gautų pajamų nemokėti mokesčių!

Išbandykite Bitcoin System šiandien

Veikite greitai! Šis pasiūlymas baigiasi ***00:00***

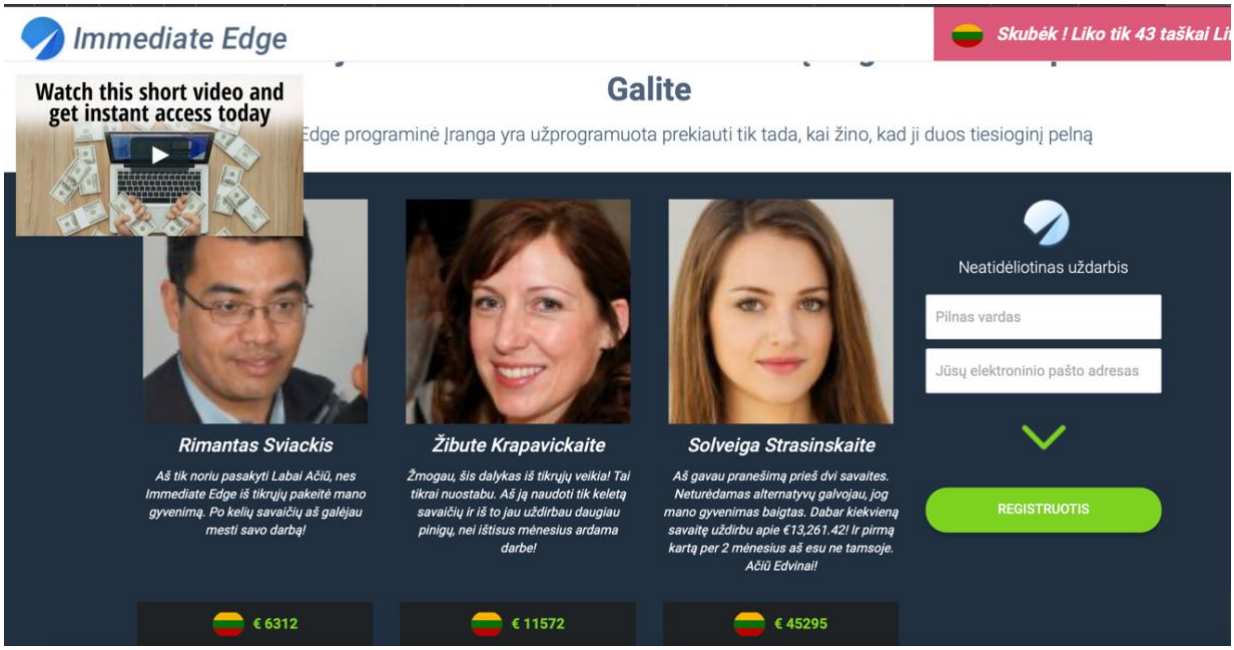
Paskelbta
2020-09-30

Paspaudus „*Išbandykite Bitcoin System šiandien*“ nuorodą nukreipiama į kitą sukčių sukurtą tinklalapį, kuriame siūloma investuoti (žr. 7 pav.). Šiame tinklalapyje prašoma įvesti savo vardą, el. pašto adresą bei telefono numerį. Nusikaltėliai turėdami šiuos duomenis gali susisiekti su auka ir pasiūlyti investuoti į kriptovaliutas, įnešant pradinį registracijos mokestį, o vėliau *immediateedgesystem.com* tinklalapyje pateikdami apgaulingą informaciją apie pelną, įgydami ir daugiau lėšų apgaule.

[72] „Informacija apie WWW ir IP adresus“, Serveriai.lt, žiūrėta 2020 m. spalio 1 d., https://whois.serveriai.lt/vmiparama.com.

[73] „Sukčių elektroninėje erdvėje sukurtas tinklalapis, tiesiogiai skirtas dayrti nusikalstamą veiką, numatytą LR BK 182 str.“, VMI parama, žiūrėta 2020 m. spalio 1 d., www.vmiparama.com.

7 pav. Sukčiavimo susijusio su investicijomis tinklalapio fragmentas[74]



Pastebėtina, jog sukčiai elektroninėje erdvėje gali apjungti kelis sukčiavimo modelius bei pasinaudodami smišingo ataka pereiti prie sukčiavimo, susijusio su investavimu modeliu.

Asmens tapatybę patvirtinančių duomenų įgijimas, pasinaudojant višingu. P.Henry teigia, jog višingas yra sukčiavimo modelis, kuomet aukai yra paskambinama telefonu ir apgaule bandoma įgyti tapatybę patvirtinančius duomenis[75]. Višingas nuo fišingo ir smišingo iš esmės skiriami padarymo būdu. Aukai gali būti paskambinama ir pateikiami apgaulinga informacija apie neva įtartiną pinigų judėjimą banko sąskaitoje bei paprašoma suteikti tapatybę patvirtinančius duomenis pokalbio metu. Aukai atskleidus sukčiaus prašomus asmens tapatybę patvirtinančius duomenis – naudotojo ID, slaptažodžius, SMART-ID kodus, sukčius kaip ir anksčiau minėtais sukčiavimo modeliai gali padaryti neteisėtą lėšų pervedimą.

Pavyzdžiui, trylika nusikaltėlių buvo sulaikyti, kai apsimesdami finansinių įstaigų Jungtinėje Karalystėje darbuotojais tarp 2013 m. gruodžio mėn. ir 2014 m. balandžio mėn. iš aukų višingo būdu įgijo asmens tapatybę patvirtinančius duomenis bei jais pasinaudodami neteisėtai įgijo apie 360 tūkst. JK svarų[76].

[74] „Sukčių elektroninėje erdvėje sukurtas, sukčiavimo, susijusio su investicijomis tinklalapis“, Immediate edge system, žiūrėta 2020 m. spalio 1 d., www.immediateedgesystem.com.

[75] Grant Gross, „First Phishing, Now Vishing.“ CIO 19, no. 22 (September 2006): 16. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=22322570&site=ehost-live,

[76] Alan Shields, „Jailed, ‘Vishing’ Fraud Pair Who Stole £360,000.“ *Daily Mail*, March 9, 2019. http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=135150998&site=ehost-live.

Taip pat pastebėtina višingo atakos atmaina, nukreipta į COVID-19 pandemijos metu nuotoliniu būdu dirbančius darbuotojus. Kaip teigia FTB[77] COVID-19 pandemijos metu didžioji dalis darbuotojų, turinčių tokią galimybę dirba iš namų ir prie savo darbovietės IT infrastruktūros jungiasi per *VPN* (angl. *virtual private network*) ryšį panaudodami jiems suteiktus prisijungimo duomenis. Višingo ataka buvo nukreipta į *VPN* prisijungimo, prie darbovietės IT infrastruktūros duomenų įgijimą. Įgijus šiuos duomenis nusikaltėliai gali juos panaudoti įgyjant vidinius įmonės klientų ar kitus juodojoje rinkoje vertę turinčius duomenis bei juos vėliau realizuoti.

Aukščiau minėtų asmens tapatybę patvirtinančių duomenų įgijimas fišingo, smišingo ar višingo būdu yra reglamentuotas Lietuvos Respublikos BK 214 straipsnyje, o tokių duomenų panaudojimas, siekiant neteisėtai įgyti asmens lėšas kvalifikuotinas kaip idealioji nusikalstamų veikų sutaptis ir pagal BK 215 ir BK 182 straipsnius. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2001 m. spalio 9 d. nutartyje pasakyta, jog: „Elektroninėje bankininkystėje visos operacijos su piniginėmis lėšomis yra tvarkomos žmogaus sudarytų kompiuterinių programų pagrindu. Klientas su banku bendrauja ne tiesiogiai, o per elektroninę sistemą. Sistema sudaryta tokiu būdu, kad ji priima komandą ir atlieka operaciją, jei surinkti tinkami sąskaitų turėtojų identifikaciniai kodai. Būtent kodas pagal programos veikimo principus identifikuoja asmens, kaip sąskaitos turėtojo, tapatybę ir pažymi teisę atlikti operacijas su sąskaitoje esančiomis piniginėmis lėšomis. Jei kodą surenka ir komandą duoda asmuo, neturintis teisės atlikti operacijų su sąskaitoje esančiomis piniginėmis lėšomis, jis pateikia operacinei sistemai ir bankui save kaip kitą asmenį, turintį tokią teisę, ir taip suklaidina elektroninę sistemą ir kartu banką.“[78]. Būtent asmens tapatybę patvirtinančių duomenų įgijimas bei tolimesnis jų panaudojimas prisijungiant prie elektroninės bankininkystės yra banko apgaulė. Sukčiai elektroninei sistemai pristatydami save kaip teisėti tos sistemos naudotojai apgauna banką bei neteisėtai inicijuoja lėšų pervedimą.

„Romantinė“ apgaulė yra gana naujas sukčiavimo modelis, kuris elektroninėje erdvėje matomas nuo 2008 m.[79] Jis išpopuliarėjo su pažinčių persikėlimu į elektroninę erdvę – susikūrė pažinčių svetainės, bendravimo programėlės. Išpopuliarėjus šiems naujų pažinčių paieškos metodams, jais suskubo pasinaudoti ir sukčiai. Šio sukčiavimo modelio metu sukčiai sukuria netikrus socialinių tinklų profilius, pasinaudodami svetimomis nuotraukomis (tai gali būti patrauklūs modeliai, karininkai) ir kito asmens tapatybe (tai gali būti vardas, amžius bei kiti

[77] „Cyber Criminals Take Advantage of Increased Telework Through Vishing campaign“, Documentcloud, žiūrėta 2020 m. spalio 1 d., http://www.documentcloud.org/documents/7041919-Cyber-Criminals-Take-Advantage-of-Increased.html.

[78] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2001 m. spalio 9 d. nutartis baudžiamojoje byloje Nr. 2K-682. Teismų praktika. 2001, 16.

[79] Monica T. Whitty ir Tom Buchanan, „The Online Romance Scam: A Serious Cybercrime.“ *Cyberpsychology, Behavior and Social Networking* 15, no. 3 (March 2012): 2. doi:10.1089/cyber.2011.0352. https://www.researchgate.net/publication/221805037_The_Online_Romance_Scam_A_Serious_Cybercrime.

asmens tapatybę identifikuojantys duomenys). Sukūrus netikrą socialinių tinklų profilį sukčiai arba patys susisiekia su būsima auka arba laukia aukos kontakto (jeigu auka galvoja, jog profilis yra tikras)[80]. Pažinčių pradžioje sukčius išsako savo jausmus aukai ir paprašo, kad pažintis iš pažinčių svetainės būtų perkelta į kitokio formato bendravimo būdą (pvz. el. laiškais, kitomis bendravimo programėlėmis), teigdami, jog jie auką mato kaip savo būsimą gyvenimo partnerį, todėl galvoja ištrinti savo profilį pažinčių svetainėje ir bendravimą perkelti kitur. Sukčius su auka bendrauja sistemingai, kad apgaule įgytų aukos lėšas bendravimas gali tęstis metų metus. Sukčius gali mėginti paskambinti aukai telefonu, tačiau tai pasitaiko retai. Aukos bendraudamos su sukčiumi atskleidžia savo paslaptis ir sukuria pasitikėjimo vertus santykius. Viliojimo stadijos metu auka įsimyli sukčių ir kai tai įvyksta, sukčius aukos paprašo dovanų (pvz. parfumerijos gaminių, išmaniojo telefono), tam kad auką patikrintų. Jeigu auka sukčiui padovanoja kvepalus bei išmanųjį telefoną sukčius aukos gali paprašyti ir smulkios sumos pinigų, kuri po to gali virsti ir didesnėmis pinigų sumomis. Kartais sukčius į apgaulę įtraukia ir bendrininkus, pavyzdžiui, gydytoją, kuris gali susisiekti su auka bei pranešti, jog jos mylimasis yra ligoninėje bei reikia apmokėti gydymo išlaidas ar lėktuvo bilietus. Romantinis sukčiavimas baigiasi tik tada, kai auka pati supranta, jog buvo apgauta ir nebeperveda pinigų sukčiui[81].

Pavyzdžiui, 82 metų karo veteranas iš JAV sukčiui, apsimetusiam moterimi per 16 mėn. laikotarpį pervedė visas savo gyvenimo santaupas, siekiančias 140 tūkst. JAV dolerių. Sukčius, apsimetęs moterimi teigė, jog dirba užsienyje, kad jai reikia pinigų paso gamybai, lėktuvo bilietams, kitoms kelionės išlaidoms, kad ji galėtų atvykti pas auką į JAV[82]. Panašų atvejį galima aptikti ir Lietuvoje, kai sukčiai iš aukos išviliojo daugiau nei 55 tūkst. eurų[83].

Atskleidus sukčiavimo modelius, nukreiptus į fizinius asmenis, toliau baigiamajame darbe bus pateikti sukčiavimo modeliai, nukreipti į juridinius asmenis - sukčiavimas, susijęs su verslo partnerio banko sąskaitos pasikeitimu bei apsimetimas įmonės vadovu.

Sukčiavimas, susijęs su verslo partnerio banko sąskaitos pakeitimu pasireiškia per įmonės darbuotojo, susijusio su finansais apgaulę pateikiant sukčių valdomą banko sąskaitą ir pranešant apgaulingą informaciją, kad tiekėjo banko sąskaita pasikeitė[84]. Šis sukčiavimo modelis gali būti įvykdomas dvejais būdais: kai sukčius neteisėtai įgyja verslo partnerio elektroninės pašto dėžutės prisijungimo duomenis ir neteisėtai prie jos prisijungęs išsiunčia kitiems verslo partneriams

[80] Whitty ir Buchanan, *supra note*, 43: 177.
[81] Whitty, *supra note*, 44: 2-3.
[82] Robert Patrick, „Florissant Man Linked to Romance Scam That Bilked Elderly Men, Women of Nearly $1 Million, Feds Say." *St. Louis Post-Dispatch (MO)*, November 26, 2019. http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=2W64180382453&site=ehost-live.
[83] „Internetinė pažintis su vyru baigėsi liūdnai – iš moters išviliojo virš 55 tūkst. eurų", *Lrytas*, 2019 m. liepos 17 d., https://www.lrytas.lt/lietuvosdiena/kriminalai/2019/07/17/news/internetine-pazintis-su-vyru-baigesi-liudnai-is-moters-isviliojo-virs-55-tukst-euru-11129419/.
[84] Archie, Turner ir Wybitul, *supra note*, 28: 13.

apgaulingą laišką, neva pasikeitė banko sąskaita ir pinigus reikia pervesti į sukčiaus nurodytą banko sąskaitą. Sekantis būdas yra, kai sukčius sukuria elektroninio pašto dėžutę, savo pavadinimu labai panašią į verslo partnerio pašto dėžutę ir tada iš jos siunčia apgaulingą laišką verslo partneriui.

Sukčiavimo, susijusio su verslo partnerio banko sąskaitos pakeitimu modus operandi. Kaip teigia W. Rash iš pradžių sukčiai, siekiantys apgaule įgyti svetimą turtą išsirenka auką. Dažniausiai tai būna įmonė su dideliu skaičiumi darbuotojų, kurie yra pavaldūs aukštesnio rango darbuotojams, juos sieja hierarchinė struktūra[85]. Tuomet sukčius gali darbuotojui nusiųsti elektroninį laišką, neva iš įmonės direktoriaus su prisegtuku, kuriame patalpinta kenkėjiška programinė įranga. Įmonės darbuotojas, pagrįstai manydamas, kad laišką jam siunčia įmonės direktorius ar jo vadovas tokį prisegtuką gali atidaryti bei tokiu būdu savo informacinę sistemą užkrėsti kenkėjiška programine įranga, kuri fiksuos konfidencialius elektroninius duomenis (pvz. elektroninio pašto dėžutės prisijungimą sudarančius duomenis). Sukčius, turėdamas aukos elektroninio pašto prisijungimo duomenis gali toliau vykdyti savo ataką bei analizuoti įmonės bendradarbiavimą su kitais juridiniais asmenimis. Vos tik kaltininkas aptinka įmonės darbuotojo sandorį su kita įmone, jis gali apsimesdamas įmonės darbuotoju nusiųsti elektroninį laišką, neva pasikeitė banko sąskaita ir pagal sąskaitą faktūrą naujas mokėjimas turi būti vykdomas į naują, sukčių valdomą sąskaitą.

Kitas būdas, kurį sukčiai gali naudoti, norėdami apgaule įgyti svetimą turtą panašus į jau aukščiau minėtą, tačiau sukčius pats sukuria elektroninio pašto dėžutę, savo pavadinimu labai panašią į įmonės darbuotojo pašto dėžutę, taip suklaidindamas kitą juridinį asmenį. Pavyzdžiui, jeigu įmonės darbuotojo, atsakingo už finansus el. pašto adresas yra *VARDENIS.PAVARDENIS@MAXIMA.LT*, sukčius gali sukurti domeną, savo pavadinimu labai panašų į MAXIMA.LT, tik vietoje pirmos I didžiosios raidės naudos l raidę, domenas atrodys taip: MAXlMA.LT bei prie jo priskirtą įmonės darbuotojo el. pašto adresą *VARDENIS.PAVARDENIS@MAXlMA.LT*[86]. Įprastai asmeniui iš pirmo žvilgsnio tai gali atrodyti identiškas pašto adresas, tačiau jis bus valdoma sukčiaus. Gavęs el. laišką iš tokio el. pašto adreso juridinio asmens verslo partneris gali pagrįstai pagalvoti, jog laiškas yra siųstas tikrojo siuntėjo ir taip apgaule pervesti lėšas pagal suklastotą sąskaitą-faktūrą.

Elektroninėje erdvėje galima aptikti įrankius, tiesiogiai skirtus ar palengvinančius minėto sukčiavimo modelio įvykdymą. Pavyzdžiui, tinklalapis *emkei.cz*[87], kuris tiesiogiai skirtas siųsti apgaulingus elektroninius laiškus. Jame asmenys gali pasirinkti kokį laiško siuntėjo elektroninio

[85] Wayne, *supra note*, 30: 1.
[86] David Zweighaft, „Business Email Compromise and Executive Impersonation: Are Financial Institutions Exposed?“ *Journal of Investment Compliance (Emerald Group)* 18, no. 1 (January 2017): 2. doi:10.1108/JOIC-02-2017-0001, https://www.batesgroup.com/publications/joic-02-2017-0001.pdf.
[87] „Emkei‘s mailer“, Emkei.cz, žiūrėta 2020 m. spalio 8 d., https://emkei.cz.

pašto adresą matys laiško gavėjas. Baigiamojo darbo autorius, norėdamas pademonstruoti, kaip šis įrankis veikia padarė eksperimentą bei sau nusisiuntė suklastotą elektroninį laišką, neva iš info@maxima.lt (žr. 8 pav.).

8 pav. Pavyzdinis verslo partnerio banko sąskaitos keitimo laiškas[88]

Kaip matyti 8 pav., „iš laukelyje“ atvaizduojamas apgaulingas siuntėjo el. pašto adresas (info@maxima.lt), baigiamojo darbo autorius siuntimo tekstą sugalvojo savo nuožiūra, tačiau panašius tekstus, tik labiau apdorotus ir pritaikytus siunčiamai įmonei naudoja ir sukčiai. Jie gali parinkti tokį patį šriftą, teksto spalvą, išanalizuoti įmonės darbuotojo laiško rašyseną ir kitus sėkmingą apgaulės įgyvendinimą nustatančius rodiklius.

Sukčiavimas, apsimetant įmonės vadovu savo esme labai panašus į prieš tai atskleistą sukčiavimo modelį, tačiau esminis skirtumas tarp šių modelių, kad sukčiavimas, apsimetat įmonės vadovu nukreiptas į toje pačioje įmonėje dirbančio, su įmonės finansais susijusio asmens suklaidinimą, kai sukčiavimas, susijęs su verslo partnerio sąskaitos pakeitimu yra nukreiptas į kito juridinio asmens suklaidinimą. Kaip teigia J.Rabkin ir kiti šis sukčiavimo modelis pasireiškia, kai įmonės buhalteris gauna apgaulingą laišką iš neva įmonės vadovo kuriame reikalaujama kuo skubiau įvykdyti nurodytą pervedimą dėl slapto įmonės susijungimo. Šiame apgaulingame laiške nurodoma sukčių banko sąskaita. Iki to laiko, kol įmonės finansininkas su įmonės vadovu pakalba fizinėje erdvėje, pinigai iš sukčių valdomos sąskaitos jau būna pervesti į kitas sąskaitas[89]. Kaip teigiama R. Grincevičiaus disertacijos E6 eksperto apklausoje: „Mažai investuoja įmonės. Trūksta ir sampratos ir švietimo, ir ta dalis žmonių, kurie yra virš 50 metų, tai dažniausiai finansininkai, buhalterės ir pan. labai jautrūs yra, nes jie su kompiuteriu neužaugo. Tas *ceo fišingas*, tos atakos kai apsimeta direktoriumi yra labai sėkmingos, o įmonei yra labai skausmingos. paprasčiausiai priežastis – nėra švietimo, jos nežino, nepatogi situacija, o kitas yra technologinė – nenaudoja

[88] Nuotrauka baigiamojo darbo autoriaus, pasinaudojant *emkei.cz* įrankiu.
[89] Rabkin ir kt., *supra note*, 31: 1.

pašto apsaugos priemonių.“[90]. Juridinių asmenų pinigų judėjimas būna didesnis nei privačių asmenų, todėl ir sukčių įgyjamos sumos yra daug didesnės.

Pavyzdžiui, *Bonnier* korporacijos vyriausiasis finansininkas sulaukė el. laiško iš įmonės vadovo su prašymu padaryti du pervedimus po 1,5 mln. JAV dolerių į Kinijos banką. Įmonės vyriausiasis finansininkas padarė pirmąjį pervedimą, tačiau prieš siunčiant antrąjį nusprendė susisiekti su įmonės vadovu ir paklausti, ar iš tikrųjų jis siuntė minėtąjį elektroninį laišką su prašymu padaryti du skubius pervedimus į Kiniją. Įmonės vadovas D. Freygang pasakė, jog jokio laiško jis nesiuntė ir neprašė pervesti lėšų į Kiniją. Dėka greito sureagavimo ir finansų įstaigos pagalbos pavyko susigrąžinti pirmąjį pervedimą. Šie laiškai rodo, kad asmuo ar asmenų grupė daug domėjosi pačiu įmonės vadovu, taip pat įmonės finansininku, kadangi pats laiškas buvo adresuotas įmonės finansininkui[91].

Apibendrinant galima teigti, jog sukčiavimas, nukreiptas į juridinius asmenis reikalauja didesnio pasiruošimo, juridinio asmens, jo verslo partnerių analizės. Sukčiai turi išsiaiškinti, kaip bendrauja įmonės vadovas su savo pavaldiniais, kaip įprastai atrodo sąskaitos-faktūros siunčiamos kitiems verslo partneriams, tam, kad pavyktų sėkmingai apgaule įgyti svetimą turtą.

Sukčiavimas elektroninėje erdvėje gali būti nukreiptas į fizinius bei juridinius asmenis. Priklausomai nuo pasirinkto elgesio varianto sukčiai naudoja atitinkamus apgaulės modelius, kurie gali skirtis atsižvelgiant į sukčiavimo auką. Visus sukčiavimo modelius elektroninėje erdvėje vienija skubumo faktorius, kai aukai apgaulingai pranešama, jog pasiūlymas galioja trumpą laiką ir ji daugiau tokia galimybe pasinaudoti nebegalės.

[90] Rokas Grincevičius, „Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose“ (daktaro disertacija, Mykolo Romerio Universitetas, 2019), 93, https://www.lvb.lt/permalink/f/16nmo04/ELABAETD36356059.

[91] Wayne Rash, „Advanced Phishing Scam Targets CEOs, CFOs for Phony Cash Transfers.“ *EWeek*, July 2015, 1. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=109363463&site=ehost-live.

2. SUKČIAVIMŲ ELEKTRONINĖJE ERDVĖJE RAIŠKA

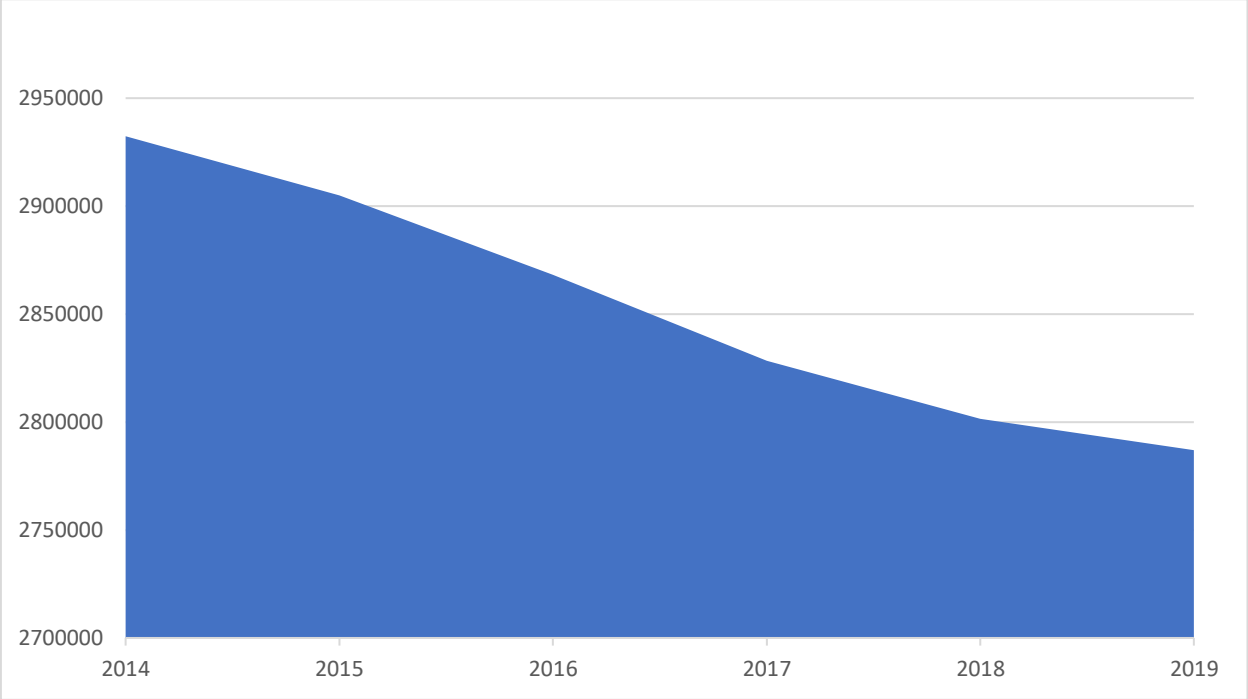
Kaip teigia T. Rudzkis: „Nusikalstamumo būklę atspindi bendras nusikalstamų veikų skaičius per tam tikrą apskaitos laikotarpį (metus, penkmetį ir t.t.) tam tikroje teritorijoje (valstybėje, apskrityje, mieste ir kt.)“[92]. Policijoje registruoto nusikalstamumo statistika buvo pagrindinis būdas, nustatyti nusikalstamumo būklę, tačiau pastaraisiais metais vyriausybės pradėjo ieškoti kitų būdų nustatyti nusikalstamumo būklę, pavyzdžiui, atliekant viktimologines apklausas. Tai yra daroma dėl dviejų priežasčių. Pirma, registruota statistika neparodo tikrosios nusikalstamumo būklės. Antra, patikima statistika galima pamatuoti teisėsaugos institucijų darbuotojų atliekamą darbą, ypač policijos, kurios tikslas yra sumažinti nusikaltimų skaičių bei suteikti saugumo jausmą gyventojams[93]. Greta registruoto nusikalstamumo egzistuoja ir latentinis nusikalstamumas. Anot T. Rudzkio: „Latentinis nusikalstamumas yra svarbus kriminogeninis faktorius, greta kitų determinuojantis nusikalstamumo gyvavimą ir permanentinius žmogaus teisių pažeidimus.“[94]

Šiame skyriuje toliau bus analizuojami 2014-2019 m. Lietuvoje užregistruoto sukčiavimo elektroninėje erdvėje statistiniai duomenys juos palyginant su Anglijos ir Velso registruoto nusikalstamumo statistiniais duomenimis. Taip pat bus palyginti Anglijos ir Velso registruoto nusikalstamumo ir viktimologinių apklausų statistiniai duomenys. Ši valstybė buvo pasirinkta, atsižvelgiant į tai, jog į nacionalinius viktimologinius tyrimus nuo 2016 metų įtraukė klausimus, susijusius su sukčiavimu bei kompiuteriniais nusikaltimais, kas labiausiai ir atitinka šio baigiamojo darbo tyrimo objektą. Taip pat bus apžvelgta 2020 m. Europos Sąjungoje užsakyta vartotojų viktimologinė apklausa.

Pradedant analizuoti užregistruoto nusikalstamumo būklę, tikėtina, svarbu išsiaiškinti, demografinius Lietuvos gyventojų pokyčius bei bendrą sukčiavimo dinamiką 2014-2019 m.

9 diagrama. Lietuvos gyventojų vidutinis gyventojų skaičius 2014-2019 m.[95]

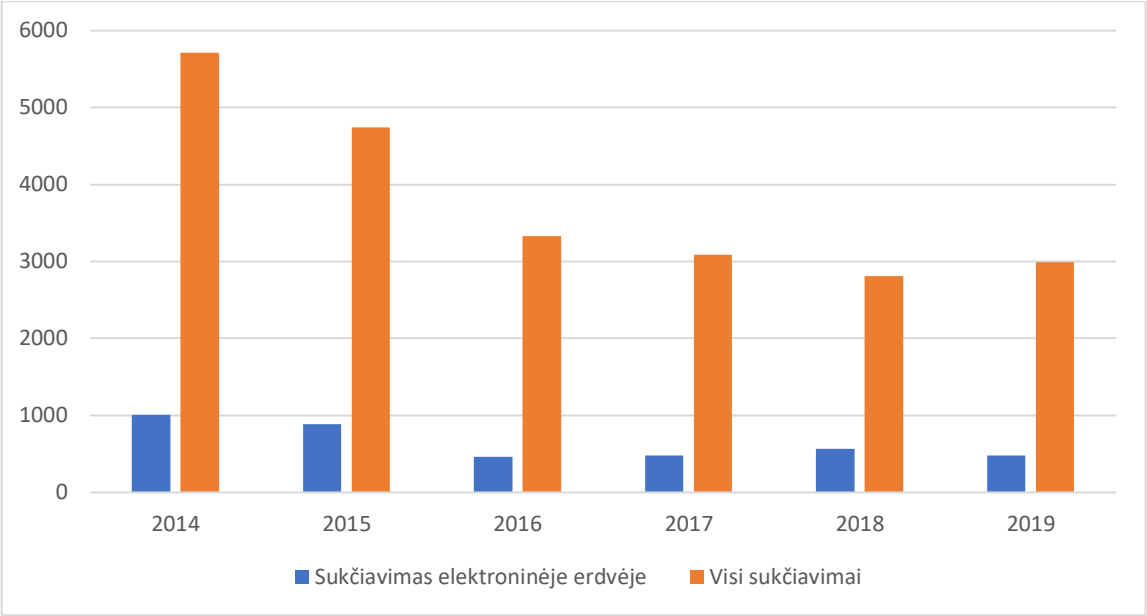
[92] Babachinaitė ir kt., *supra note*, 25: 126.
[93] Chris Hale ir kt., *Criminology* (Oxford: Oxford University Press, 2005), 41.
[94] Genovaitė Babachinaitė ir kt., *Latentinio nusikalstamumo kriminologinio tyrimo metodikos [elektroninis išteklius]: metodinis leidinys* (Vilnius: Mykolo Romerio universitetas, 2009), http://www3.mruni.eu/~akiskis/alfredo-str-latent_nus_tyrimo_metodikos2009.pdf.
[95] Sudaryta baigiamajo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš: https://data.worldbank.org/indicator/SP.POP.TOTL?locations=LT (žiūrėta 2020 m. spalio 9 d.).



Tiriamuoju laikotarpiu Pasaulio banko duomenimis Lietuvos gyventojų skaičius mažėjo. 2014 metais Lietuvoje gyveno 2 932 367 gyventojai, o 2019 metais – 2 786 844 gyventojai. Tiriamo laikotarpio pabaigoje gyveno 145 523 mažiau gyventojų nei tiriamo laikotarpio pradžioje. Iš viso gyventojų skaičius sumažėjo 4,96 proc. Lyginant tą patį laikotarpį su Jungtinės Karalystės demografiniais pokyčiais, čia gyventojų skaičius 2014 metais buvo 64 602 298, o 2019 metais – 66 834 405, kas parodo, jog Jungtinėje Karalystėje gyventojų skaičius per tiriamąjį laikotarpį padidėjo 3,46 proc. Taigi, matyti, jog Lietuvoje gyventojų skaičius tiriamuoju laikotarpiu stabiliai mažėjo, o Jungtinėje Karalystėje – didėjo.

10 diagrama. Registruotų sukčiavimų elektroninėje erdvėje 2014-2019 m. Lietuvoje palyginimas su paprastu sukčiavimu[96]

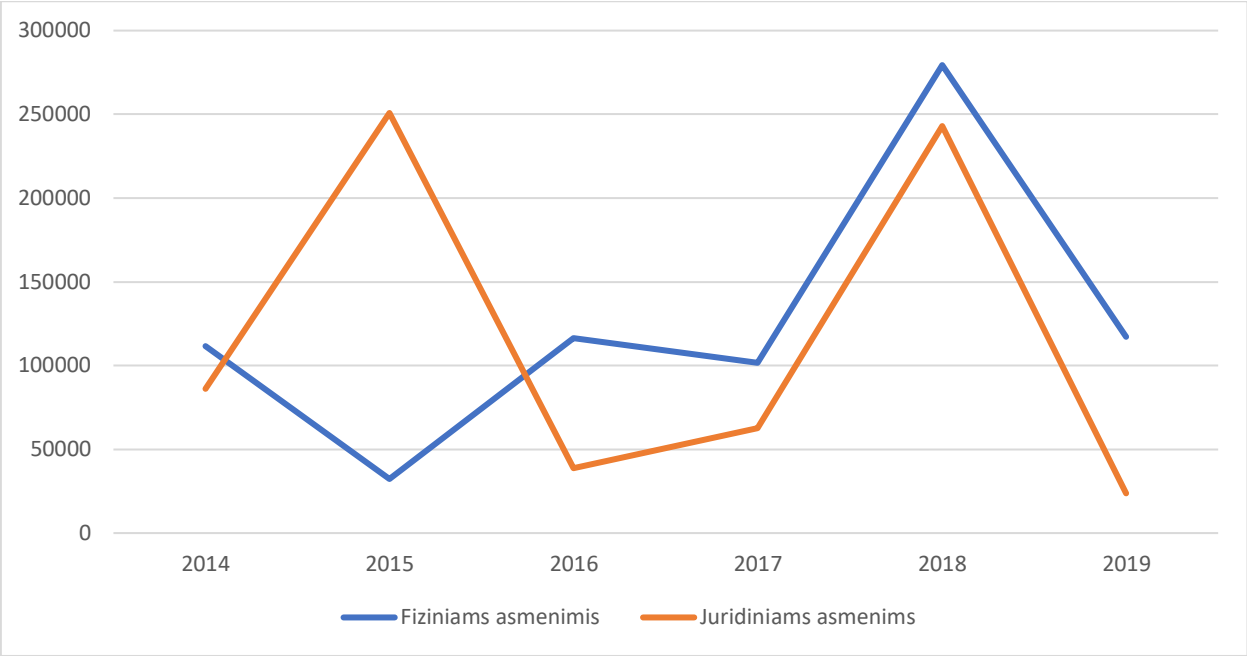
[96] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*10 forma*) ir NŽVR registro (forma_*EK-SAV*).



Tiriamojo laikotarpio pradžioje 2014 m. iš viso sukčiavimų elektroninėje erdvėje (BK 182 str. 1 d., 2 d. ir 3 d.) buvo registruota 1007 veikos, kai sukčiavimų fizinėje ervėje buvo registruota 5710 veikos. Sukčiavimo elektroninėje erdvėje veikos sudarė apie 18 proc. visų užregistruotų sukčiavimų. Tiriamojo laikotarpio pabaigoje 2019 m. sukčiavimų elektroninėje erdvėje buvo užregistruota 481 veikos, kai sukčiavimų fizinėje erdvėje buvo užregistruota 2995 veikos. Tiriamojo laikotarpio pabaigoje sukčiavimo elektroninėje erdvėje veikos sudarė apie 16 proc. visų užregistruotų sukčiavimo veikų. Galima teigti, jog viso tiriamojo laikotarpio metu sukčiavimai elektroninėje erdvėje sudarė panašią dalį visų užregistruotų sukčiavimo nusikalstamų veikų.

11 diagrama. Užregistruotais sukčiavimais elektroninėje erdvėje Lietuvoje 2014-2019 m. padaryta turtinė žala (eurais)[97]

[97] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*10 forma*).



Kaip matyti pateiktoje iš registruotų sukčiavimų elektroninėje erdvėje statistikos, turtinės žalos tiriamuoju laikotarpiu daugiau patyrė fiziniai asmenys, nei juridiniai asmenys. Išskyrus 2015 metus, kai juridinių asmenų patirta žala žymiai padidėjo. Tai lėmė vienas nukentėjusiojo juridinio asmens atvejis, kai jis patyrė 181 tūkst. eurų žalos. Nuo 2014 metų iki 2015 m. fizinių asmenų patirta žala sumažėjo daugiau nei perpus, tačiau nuo 2016 m. iki 2018 metų ji toliau augo. 2019 metais matomas ženklus žalos sumažėjimas. Ypač ženkliai, daugiau nei 2,5 karto žala padidėjo tarp 2017 ir 2018 metų. Juridinių asmenų patiriama žalos įverčiai kaip matyti diagramoje nežymiai skyrėsi nuo fizinių asmenų patiriamos žalos sukčiavimais elektroninėje erdvėje. Viso tiriamuoju laikotarpiu fiziniai asmenys apgaule prarado 758 tūkst. eurų, kai juridiniai asmenys apgaule prarado 704 tūkst. eurų. Iš to galima teigti, jog fizinių asmenų patirta turtinė žala sukčiavimais elektroninėje erdvėje yra didesnė.

12 lentelė. Investicijų sukčiavimo skundų skaičius bei turtinė žala Lietuvoje 2017-2020 m. III ketvirtį[98]

Metai	Skundų skaičius	Prarasta suma (eurais)
2017	18	683 690
2018	59	1 136 751
2019	76	305 528
2020 III ketvirtis	34	328 858

[98] Šaltinis: Lietuvos banko pateikta informacija, magistro baigiamojo darbo autoriui kreipiantis į Lietuvos banką el. paštu. Lietuvos bankas turi galimybę pateikti informaciją tik apie dėl sukčiavimo, susijusio su investicinėmis paslaugomis, Lietuvos banko gautus skundus ir tik už periodą nuo 2017 m. Tokia informacija gali būti nereprezentatyvi nes tik dalis nukentėjusių žmonių kreipiasi į Lietuvos banką ir tik dalyje kreipimųsi yra nurodoma prarasta suma.

Kaip matyti lentelėje nr. 12 2017 m. buvo gauta 18 skundų bei patirta 683 tūkst. eurų turtinė žala iš asmenų nukentėjusių nuo investicinio sukčiavimo. 2020 m. III ketvirtį buvo gauta 34 skundai, aukų patirta turtinė žala – 328 tūkst. eurų. Vien tik 2020 m. III ketvirtį buvo gauta beveik dvigubai daugiau skundų nei per visus 2017 metus. Pastebėtina, jog statistikoje atvaizduojamas ne aukų skaičius, tačiau skundų skaičius. Aukų skaičius gali būti didesnis kadangi aukos gali pateikti grupės skundą, būti nukentėję šeima, verslo partneriai. Lyginant Lietuvos banko pateiktą sukčiavimo, susijusio su investicijomis su užregistruoto sukčiavimo elektroninėje erdvėje statistika 2017-2019 m. pastebėtina, kad 2017 m. pagal užregistruoto sukčiavimo elektroninėje erdvėje duomenis Lietuvos gyventojai patyrė 164 tūkst., 2018 m. 522 tūkst., 2019 m. 140 tūkst. eurų siekiančią turtinę žalą. Už visus sukčiavimus elektroninėje erdvėje patirta žala yra beveik dvigubai mažesnė nei už sukčiavimą, susijusį su investicijomis. Užregistruoto sukčiavimo elektroninėje erdvėje statistika neparodo tikrosios padėties.

Lietuvos banko priežiūros tarnybos Finansinių paslaugų ir rinkų priežiūros departamento direktorius ginčo byloje nr. 2019-02175[99] priėmė sprendimą, kur paslaugų gavėja (vartotoja) atidavė sukčiams, apsimetusiais būsimais darbdaviais savo asmens tapatybę identifikuojančius duomenis. Sukčiai prisijungę prie elektroninės bankininkystės užpildė paraišką 1 900 EUR vartojimo kreditui gauti. Tam, kad sutartis būtų sudaryta, paraiška turėjo būti patvirtinta elektroniniu parašu, ką ir padarė nukentėjusioji. Į savo sąskaitą gavusi 1 900 EUR neva darbo priemonėms įsigyti, nepaisydama mokėjimo paskirtyje nurodytų vartojimo kredito sutarties duomenų, moteris juos pervedė menamam tiekėjui. Supratusi, kad yra apgauta, vartotoja paprašė pripažinti vartojimo kredito sutartį negaliojančia ir atleisti nuo paskolos grąžinimo. Lietuvos Bankas šį jos prašymą atmetė, nes vartotoja buvo nepakankamai rūpestinga ir atsargi, elektroniniu parašu patvirtindama vartojimo kredito sutartį ir pinigus neva darbo priemonėms įsigyti pervedusi nepažįstamiems asmenims.

Visiškai priešingas Lietuvos banko priežiūros tarnybos Finansinių paslaugų ir rinkų priežiūros departamento direktoriaus sprendimas ginčo byloje nr. 2019-01644, kai paslaugų gavėjas gavo žinutę neva iš banko ir paspaudęs apgaulingą nuorodą bei suvedęs prašomus prisijungimo duomenys patyrė 1 499 EUR nuostolių. Lietuvos bankas rekomendavo SEB bankui atlyginti apgaule pasisavintų lėšų nuostolius, nes nebuvo vartotojo neatsargumo požymių: „Atsižvelgiant į tai, kad sukčių siųsta SMS žinutė buvo įterpta į tikrų banko žinučių srautą, į tai,

[99] 2020 m. vasario 12 d. Lietuvos Banko priežiūros tarnybos finansinių paslaugų ir rinkų priežiūros departamento direktoriaus sprendimas *dėl Y.Y. ir UAB „General Financing“, ginčo nagrinėjimo* nr. 242-65. žiūrėta 2020 m. spalio 10 d., https://www.lb.lt/lt/frd-gincai-su-vartotojais/view_dispute?id=10599.

kad buvo suklastota elektroninė banko aplinka, galima teigti, kad pareiškėjas negalėjo suprasti, kad jo veiksmai yra ne banko pateiktų nurodymų vykdymas, o sukčių ataka.“[100]

Taigi, tokie Lietuvos banko sprendimai, kai vienu atveju sukčiams elektroninėje erdvėje pasisavinus aukos lėšas aukos prašymas dėl lėšų grąžinimo buvo atmestas, o kitu panašiu atveju patenkintas formuoja neaiškią praktiką. Turint tokią praktiką fizinių asmenų patiriama turtinė žala Lietuvoje kaip matyti iš registruoto nusikalstamumo statistikos galimai ilgą laiką bus didesnė nei juridinių asmenų. Manytina, kad analogija, kai pvz. SEB bankas neteisėtai panaudotos banko mokėjimo kortelės padarytą turtinę žalą sumažina iki 50 EUR[101], turėtų būti taikoma ir kai pasinaudojama neteisėtai įgytais prisijungimais prie elektroninės bankininkystės ir taip apgaule įgyjamos lėšos.

Kitaip nei Lietuvoje, Jungtinėje Karalystėje septynios finansų įstaigos 2019 m. pasirašė „Patvirtintų tiesioginių mokėjimo sukčiavimų atlyginimo“[102] aktą. Šiuo aktu įsteigė „niekas nekaltas“ fondą ir fonde iš akto narių septynių finansų įstaigų surinktais pinigais bus atlyginama turtinė nukentėjusiųjų žala, jei asmenys atitiks akte numatytą sąlygą būti pakankamai rūpestingiems ir atidiems.

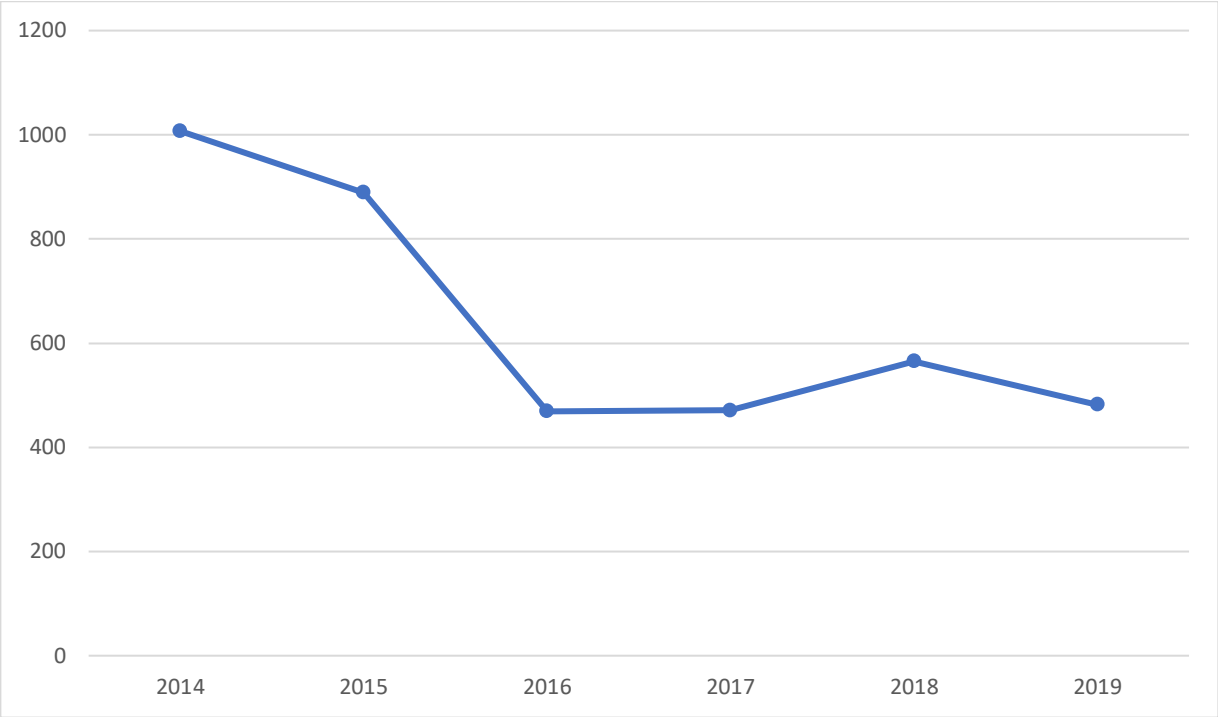
13 diagrama. Absoliutūs užregistruoto sukčiavimo elektroninėje erdvėje skaičiai Lietuvoje 2014-2019 m.[103]

[100] 2020 m. sausio 15 d. Lietuvos Banko priežiūros tarnybos finansinių paslaugų ir rinkų priežiūros departamento direktoriaus sprendimas *dėl X.X. ir banko AB „SEB bankas“, ginčo nagrinėjimo* Nr. 242-22. Žiūrėta 2020 m. spalio 10 d., https://www.lb.lt/lt/frd-gincai-su-vartotojais/view_dispute?id=10067.

[101] „SEB banko bendrosios paslaugų teikimo taisyklės“, SEB bankas, žiūrėta 2020 m. spalio 10 d., https://www.seb.lt/sites/default/files/web/pdf/Bendrosios_taisykles_2018_08_01.pdf.

[102] „Contingent Reimbursement Model Code for Authorised Push Payment Scams“, Lending standards board, 2019 m. gegužės 28 d. https://www.lendingstandardsboard.org.uk/wp-content/uploads/2019/05/CRM-code.pdf ir „App scams voluntary code sven launch“, UK Finance, https://www.ukfinance.org.uk/press/press-releases/app-scams-voluntary-code-seven-launch (žiūrėta 2020 m. spalio 10 d.). APP sukčiavimai akto kontekste aiškinami kaip sukčiavimai, kai asmuo iš savo banko sąskaitos nori lėšas pervesti vienam asmeniui, bet suklaidintas perveda kitam asmeniui ir kai asmuo lėšas perveda kitam asmeniui už atrodytų teisėtus tikslus, bet tai būna apgaulingi tikslai. Tokių sukčiavimų pavyzdžiai pagal Jungtinės Karalystės finansų institucijų industrijos kolektyvinės bendruomenės FRAUD FACTS 2019 https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf leidinyje yra **prekių nepristatymo sukčiavimai (angl. goods not received scam), sukčiavimai, susiję su investicijomis (angl. investment scam), „romantiniai nusikaltimai“ (angl. romance scam)** bei kt.

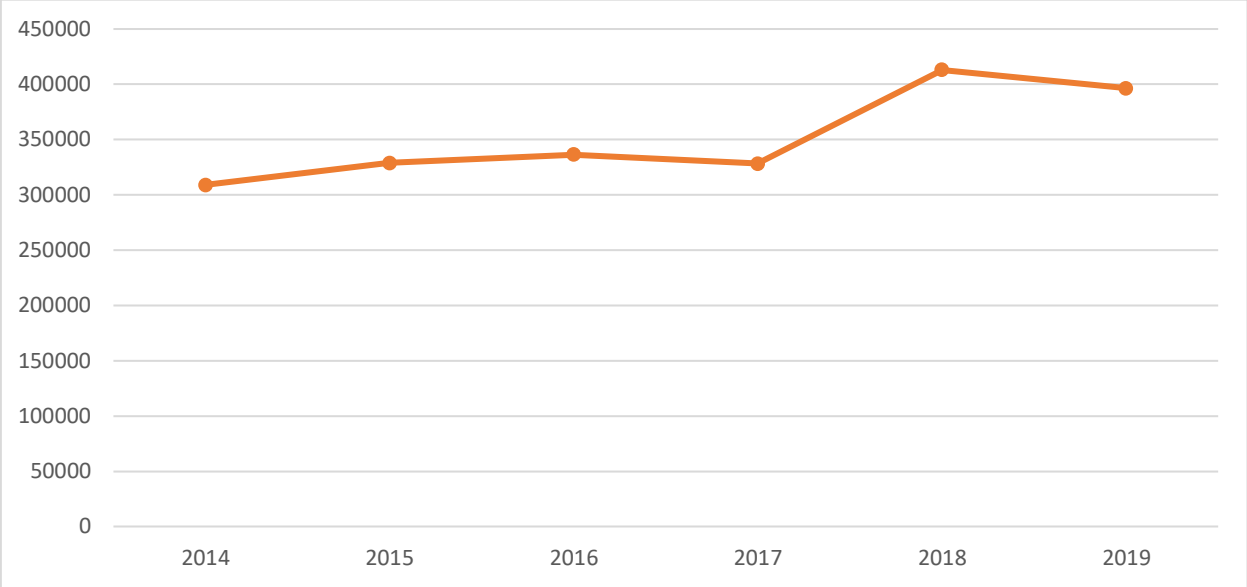
[103] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (10 forma).



Tiriamojo laikotarpio pradžioje 2014 m. absoliutus sukčiavimo elektroninėje erdvėje veikų skaičius buvo 1 007 veikos, tiriamojo laikotarpio pabaigoje buvo registruota 482 veikos. Gana ženklus registruotų sukčiavimų elektroninėje erdvėje veikų kitimas matyti nuo 2015 m. iki 2016 m., kai užregistruotų sukčiavimų elektroninėje erdvėje sumažėjo 47 proc. Lyginant tiriamojo laikotarpio pradžią bei pabaigą matomas 52 proc. užregistruotų sukčiavimų elektroninėje erdvėje sumažėjimas. Anot A. Kiškio: „Prieš užregistruojami policijoje nusikaltimai pereina keletą filtrų. Paprastai sunkesnius nusikaltimus policija yra linkusi užregistruoti, tačiau dažniausiai pasitaikančius nesunkius nusikaltimus ji vengia registruoti.“[104] Taip pat, kaip teigiama Lietuvos Respublikos Valstybės kontrolės audito ataskaitoje: „Tobulėjančios technologijos sudaro geresnes sąlygas elektroninėje erdvėje veikti anonimiškai, nusikalstamos veikos gali būti mažiau pastebimos.“ [105] Taigi, toks staigus registruoto sukčiavimo elektroninėje erdvėje kritimas galimai neparodo tikslių duomenų. Pastebėtina, jog sukčiavimo elektroninėje erdvėje metu įsijungia ir tarpvalstybinis elementas – sukčius iš Afrikos žemyno gali apgauti asmenį Lietuvoje. Natūralu, jog tokia veika gali būti net neregistruojama nematant jos ištyrimo galimybių arba auka pati gali nesikreipti į teisėsaugos institucijas dėl, pavyzdžiui kelių šimtų eurų siekiančių nuostolių.

[104] Alfredas Kiškis, „Registruoto nusikalstamumo statistikos ir viktimologinių tyrimų duomenų kompleksinio panaudojimo problemos.“ *Socialinių Mokslų Studijos: Mokslo Darbai = Social Sciences Studies: Research Papers* 4, no. 2 (2012): 700.
[105] Valstybinio audito ataskaita, *supra note*, 13: 27.

14 diagrama. Užregistruotų sukčiavimų elektroninėje erdvėje 2014-2019 m. Anglijoje ir Velse absoliutūs skaičiai[106]

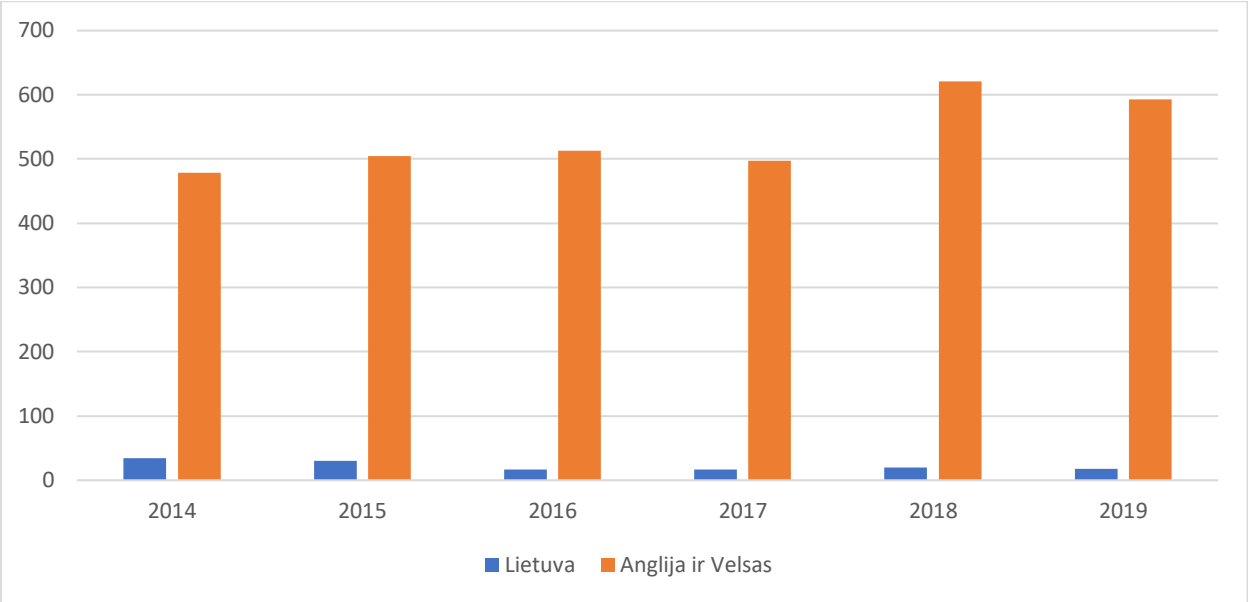


Tiriamuoju laikotarpiu Anglijoje ir Velse užregistruotų sukčiavimų elektroninėje erdvėje skaičius stabiliai didėjo nuo 2014 metų iki 2016 metų. Nuo 2016 metų iki 2017 metų registruotų sukčiavimų sumažėjo 6 tūkst. atvejų. Žymus registruoto sukčiavimo elektroninėje erdvėje šuolis matomas nuo 2017 metų iki 2018 metų. Lyginant sukčiavimus elektroninėje erdvėje tiriamojo laikotarpio pradžioje ir pabaigoje šis skaičius išaugo 30 proc.

15 diagrama. Užregistruotų sukčiavimų elektroninėje erdvėje 100 tūkst. Gyventojų 2014–2019 m. Lietuvoje bei Anglijoje ir Velse[107]

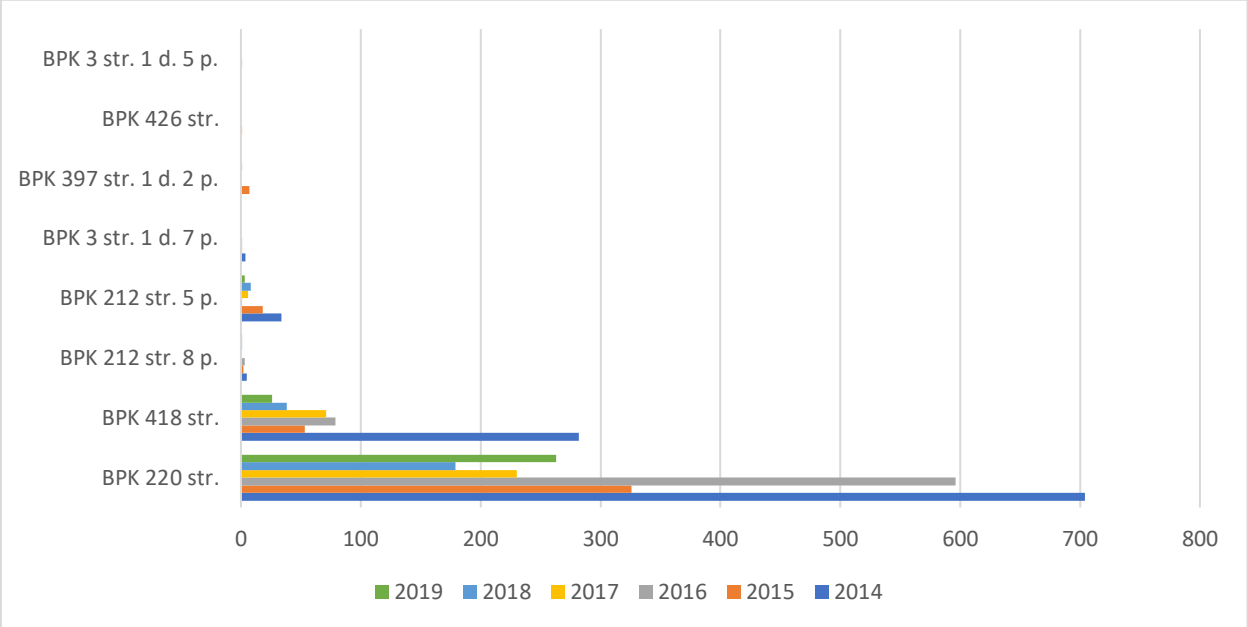
[106] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš Jungtinės Karalystės nacionalinės statistikos biuro, „Crime in England and Wales: Appendix tables“ https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables. Lentelė A5: „Fraud offences recorded by National Fraud Intelligence Bureau“ nuo 2014 m. liepos mėn. iki 2019 m. liepos mėn. Skaičiuojant absoliučius Anglijos ir Velso sukčiavimų elektroninėje erdvėje skaičius autorius pasirinko tokius lentelėse esančius rodiklius: „**Banking and credit industry fraud**: *Cheque, plastic card and online bank accounts (not PSP)*; **Advance fee payments**: *"419" Advance fee fraud, Lottery scams, Counterfeit cashiers' cheques and bankers drafts, Dating scam, Fraud recovery, Inheritance fraud, Rental fraud, Other advance fee frauds, Lender loan fraud*“, kadangi autoriaus manymu, šie sukčiavimo modeliai labiausiai atitinka sukčiavimus, padaromus elektroninėje erdvėje.

[107] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (10 forma) ir duomenys gauti iš Jungtinės Karalystės nacionalinės statistikos biuro, „Crime in England and Wales: Appendix tables“ https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables. Lentelė A5: „Fraud offences recorded by National Fraud Intelligence Bureau“ nuo 2014 m. liepos mėn. iki 2019 m. liepos mėn. Skaičiuojant absoliučius Anglijos ir Velso sukčiavimų elektroninėje erdvėje skaičius autorius pasirinko tokius lentelėse esančius rodiklius: „**Banking and credit industry fraud**: *Cheque, plastic card and online bank accounts (not PSP)*; **Advance fee payments**: *"419" Advance fee fraud, Lottery scams, Counterfeit cashiers' cheques and bankers drafts, Dating scam, Fraud recovery, Inheritance fraud, Rental fraud, Other advance fee frauds, Lender loan fraud*“, kadangi autoriaus manymu, šie sukčiavimo modeliai labiausiai atitinka sukčiavimus, padaromus elektroninėje erdvėje.



Kaip matyti diagramoje nr. 15 sukčiavimas elektroninėje erdvėje 100 tūkst. gyventojų Lietuvoje dalis sudarė 7 proc. sukčiavimų elektroninėje erdvėje 100 tūkst. gyventojų Anglijoje ir Velse. Tiriamojo laikotarpio pabaigoje šis skaičius dar labiau sumažėjo ir siekė 2,8 proc. Registruotas sukčiavimas elektroninėje erdvėje Lietuvoje stabiliai mažėjo nuo 2014 metų, o Anglijoje ir Velse šie rodikliai yra priešingi ir matomas šių veikų didėjimas.

16 diagrama. Ištirtose užregistruotų sukčiavimų elektroninėje erdvėje Lietuvoje 2014-2019 m. veikose priimti spendimai[108]



Daugiausia priimtų sprendimų sukčiavimų elektroninėje erdvėje sudaro Lietuvos Respublikos BPK 220 str. (kaltinamojo akto perdavimas teismui), 2014 metais – 704 bylos, 2015 metais – 326 bylos, 2016 metais – 596 bylos, 2017 metais – 230 bylos, 2018 metais – 179 bylos,

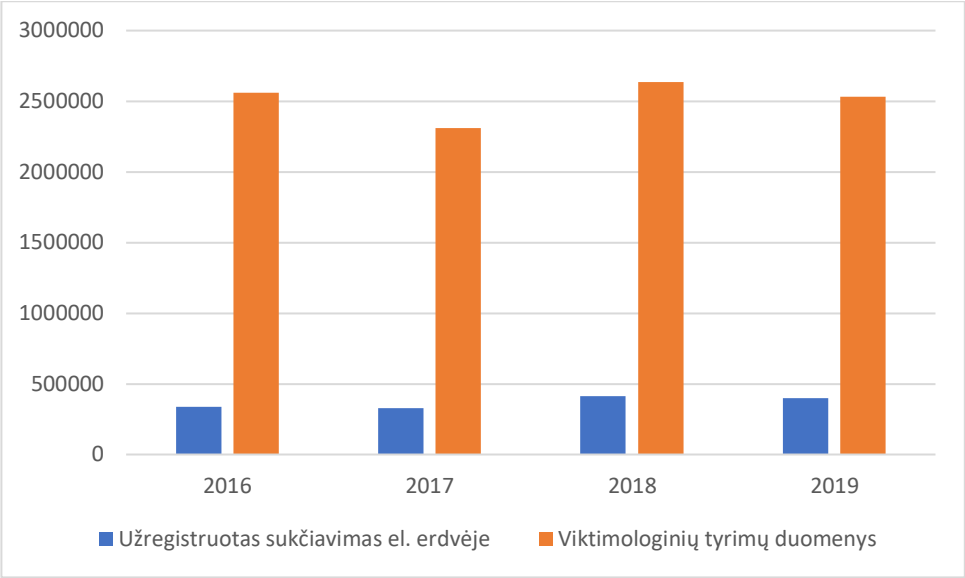
[108] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*20 forma*).

2019 metais – 263 bylos. Iš viso lyginant tiriamojo laikotarpio pradžią su tiriamojo laikotarpio pabaiga buvo kaltinamųjų aktų teismui perduota 62 proc. mažiau. LR BPK 418 str. (proceso užbaigimas baudžiamuoju įsakymu) tiriamojo laikotarpio pradžioje buvo 282 bylos, o tiriamojo laikotarpio pabaigoje buvo 26 bylos, kas reiškia, jog tiriamojo laikotarpio pabaigoje proceso užbaigimas baudžiamuoju įsakymu mažėjo 90 proc. BPK 212 str. 5 p. (ikiteisminis tyrimas nutrauktas įtariamajam ir kaltinamajam susitaikius) fiksuoti 34 atvejai tiriamojo laikotarpio pradžioje ir 5 atvejai tiriamojo laikotarpio pabaigoje. Apibendrinus, galima teigti jog visų priimtų proceso sprendimų tiriamojo laikotarpio pabaigoje lyginant su tiriamojo laikotarpio pradžia, mažėjo.

Registruoto nusikalstamumo statistika, kaip jau ir buvo minėta neparodo tikrosios nusikalstamumo būklės. Kad pamatytumėme tikrąjį nusikalstamumą, atliekamos viktimologinės apklausos. Lietuvoje viktimologinis tyrimas, apimantis sukčiavimų nusikalstamas veikas, paskutinį kartą buvo atliktas MRU mokslininkų 2012 metais. Jame buvo nurodytas klausimas apie sukčiavimą, tačiau nebuvo klausiama apie sukčiavimą padarytą elektroninėje erdvėje. Kitose valstybėse, pavyzdžiui, Jungtinėje Karalystėje į viktimologinį tyrimą (*CSEW* - Crime Survey for England and Wales) klausimas, susijęs su kibernetiniais nusikaltimais pirmą sykį buvo pateiktas 2016 metais. Baigiamojo darbo autorius norėdamas palyginti viktimologinių tyrimų duomenis su registruota statistika toliau baigiamajame darbe pateiks Anglijos ir Velso viktimologinio tyrimo ir registruotos statistikos 2016– 2019 m. duomenis.

17 diagrama. Anglijos ir Velso 2016-2019 m. užregistruoto sukčiavimo elektroninėje erdvėje palyginimas su viktimologinių tyrimų rezultatais[109]

[109] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš iš Jungtinės Karalystės nacionalinės statistikos biuro, „Crime in England and Wales: Appendix tables“ https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables. Lentelė A5: „Fraud offences recorded by National Fraud Intelligence Bureau“ nuo 2014 m. liepos mėn. iki 2019 m. liepos mėn. Skaičiuojant absoliučius Anglijos ir Velso sukčiavimų elektroninėje erdvėje skaičius autorius pasirinko tokius lentelėse esančius rodiklius: „**Banking and credit industry fraud**: *Cheque, plastic card and online bank accounts (not PSP);* **Advance fee payments**: *"419" Advance fee fraud, Lottery scams, Counterfeit cashiers' cheques and bankers drafts, Dating scam, Fraud recovery, Inheritance fraud, Rental fraud, Other advance fee frauds, Lender loan fraud*“, kadangi autoriaus manymu, šie sukčiavimo modeliai labiausiai atitinka sukčiavimus, padaromus elektroninėje erdvėje ir lentelė A1: „Trends in CSEW incidents of crime from year ending December 1981 to year ending March 2020, with percentage change and statistical significance of change“, rodikliai: **Fraud**: *Bank and credit account fraud, Advance fee fraud.*



Tiriamojo laikotarpio pradžioje 2016 m. iš viso viktimologinio tyrimo duomenimis nuo sukčiavimų elektroninėje erdvėje nukentėjo 2 562 000 asmenys, kai užregistruota buvo 336 486 veikos. 2017 metais viktimologinio tyrimo duomenimis nukentėjo 2 310 000 asmenys, kai užregistruota buvo 328 273 veikos. 2018 metais viktimologinio tyrimo duomenimis nukentėjo 2 636 000 asmenys, kai užregistruota buvo 412 853 veikos. Tiriamojo laikotarpio pabaigoje 2019 m. viktimologinio tyrimo duomenimis nukentėjo 2 534 000 asmenys, kai užregistruota buvo 396 504 veikos. Taigi, galima daryti išvadą, jog Jungtinėje Karalystėje buvo užregistruota apie 15 proc. visų veikų, nuo kurių teigė nukentėję respondentai. Registruoto nusikalstamumo statistika neparodo tikrosios nusikalstamumo būklės.

Baigiamojo darbo autorius toliau apžvelgs Europos Sąjungoje 2020 m. vykdytą apklausą „Vartotojų patirtos apgaulės ir sukčiavimai“[110] (toliau ir – Vartotojų apgaulės apklausa). Ši apklausa buvo atlikta 28-iose Europos Sąjungos valstybėse, taip pat Islandijoje ir Norvegijoje. Šioje apklausoje buvo klausiama apie viktimizacijos patirtį 2018-2019 metais: daiktų pirkimo apgaulės, tapatybės vagystė, piniginis sukčiavimas. *Daiktų pirkimo apgaulė* apima šias apgaules: kai asmuo pigiai įsigijo daiktus ar paslaugas tačiau vietoje to buvo apgaule įtrauktas į brangias mėnesinės prenumeratos paslaugas, kai asmuo įsigijo daiktą internetu, bet el. parduotuvė buvo tiesiogiai sukurta apgaule įgyti žmonių lėšas, todėl asmuo prekės negavo, kai asmuo gavo netikrą sąskaitą-faktūrą už prekes ar paslaugas, kurių niekada neužsisakė ir buvo paprašyta šią sąskaitą-faktūrą apmokėti. *Tapatybės vagystė* Vartotojų apgaulės apklausoje apima apgaulingą skambutį, laišką ar bet kurį kitą kontaktą, kai asmeniui buvo paskambinta iš banko, telekomunikacijų kompanijos ar kitos įmonės ir buvo paprašyta suteikti tapatybę identifikuojančius duomenis. Taip

[110] „Survey on “Scams and fraud experienced by consumers”, Contract n° 2018 85 04 under FWC CHAFEA/2017/CP/03 Lot 1 Written by: Ipsos, Date: January 2020“, Ipsos, žiūrėta 2020 m. spalio 14 d., https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf.

pat ši apgaulė apima atvejus, kai vartotojas internetiniame tinklalapyje aptiko informaciją, kad jo informacinė sistema yra užkrėsta, o tam, kad ją sutvarkytų reikia pateikti asmens tapatybę identifikuojančius duomenis. *Piniginis sukčiavimas* apima tokius apgaulės būdus kaip asmeniui buvo pažadėtas piniginis atlygis ar investicinė grąža, jei asmuo perves pinigus už paslaugą ar investuos savo lėšas, asmuo nusipirko bilietus, tačiau jie buvo netikri arba bilietų iš viso negavo; su asmeniu buvo susisiekta apsimetant finansine įstaiga, telekomunikacijų bendrove ar vyriausybine organizacija ir asmeniui buvo pasakyta, jog yra problemų su paskyra, asmeniui buvo grasinama, jei jis nesumokės, atsitiks kažkas negero; asmuo gavo pranešimą apie laimėjimą, o kad gautų laimėjimą turi sumokėti nustatytą mokestį arba nusipirkti tam tikrą produktą.

Turint omenyje, jog šiame baigiamajame darbe yra analizuojami specifiniai sukčiavimai, jie atitinka šiuos Vartotojų apgaulės apklausoje esančius sukčiavimo tipus – *tapatybės vagystė* ir *piniginis sukčiavimas*. Šie sukčiavimo modeliai dažniausiai yra įgyvendinami išimtinai naudojant internetą, informacines technologijas. Todėl toliau Vartotojų apgaulės apklausoje esantys duomenys šiame baigiamajame darbe bus analizuojami būtent šių sukčiavimo tipų kontekste.

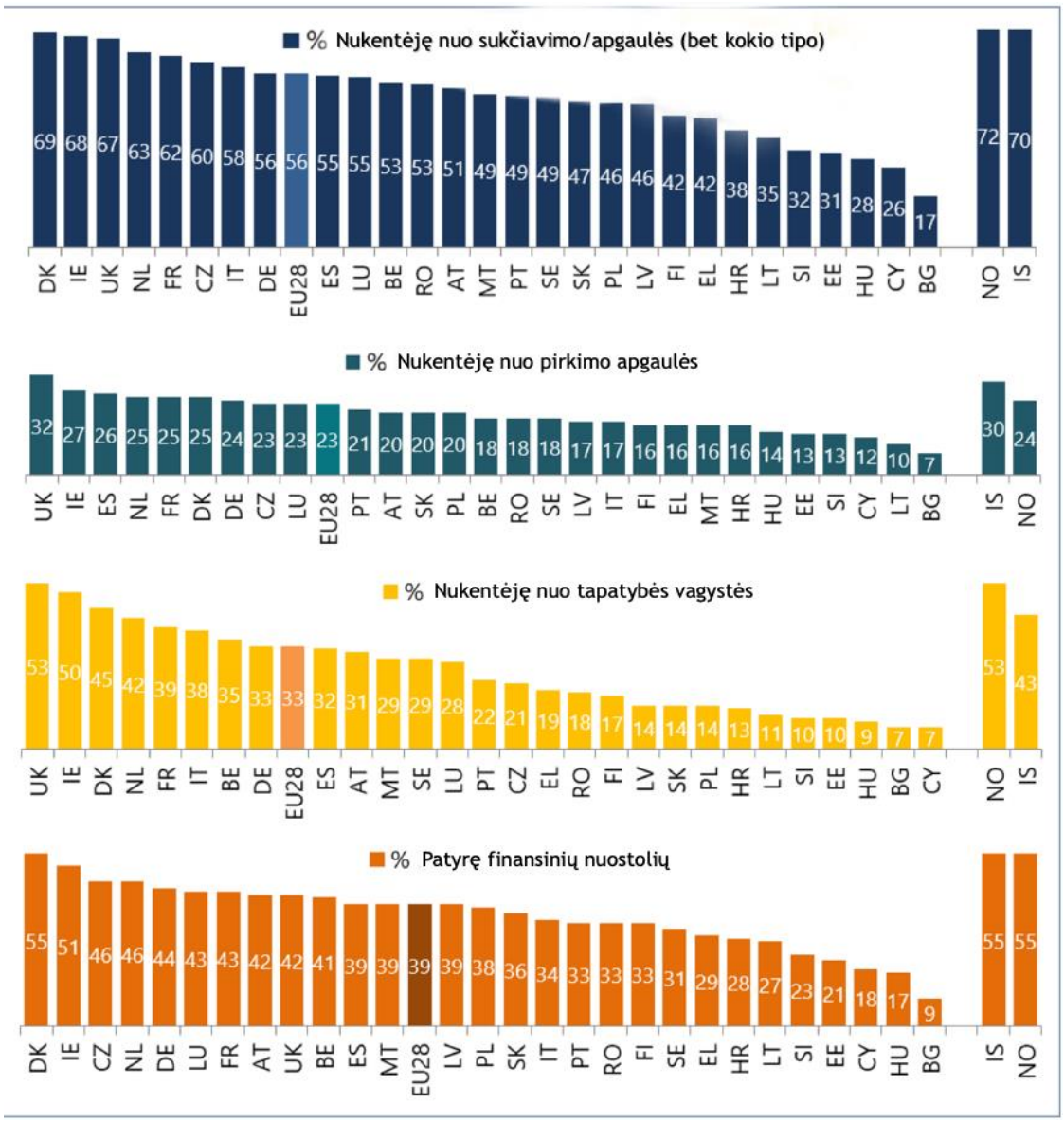
18 lentelė. Vartotojų apgaulės apklausoje atskleistų sukčiavimo tipų įverčiai už 2018-2019 metus[111] (N=26,735)

Vartotojo patirta apgaulė	Atsakiusių teigiamai skaičius procentais
Jūs gavote pranešimą apie laimėjimą loterijoje, tačiau norint atsiimti prizą jums reikės sumokėti mokestį arba nusipirkti produktą	28 proc.
Jums paskambino ir prisistatę įmonės atstovais paprašė suteikti arba patvirtinti asmens tapatybę identifikuojančią informaciją	22 proc.
Jūs patekote į tinklalapį, kuriame buvo pranešta, jog yra sutrikimų su jūsų kompiuteriu ar interneto ryšiu. Tuomet buvo paprašyta atskleisti tapatybę identifikuojančią informaciją	21 proc.
Jums buvo pažadėta, kad jūs gausite daiktą, paslaugą, nuolaidą ar didelę investicinę grąžą, jei pervesite ar investuosite lėšas	14 proc.
Jums paskambino ir prisistatę įmonės atstovais pasakė, jog yra problemų su jūsų vartotojo paskyra ar kitais duomenimis	12 proc.
Jūs gavote netikrą sąskaitą-faktūrą už produktus, kurių niekada neužsisakėte ir buvo pareikalauta šią sąskaitą-faktūrą apmokėti	10 proc.
Jūs pagalvojote, jog užsisakėte prekę (-es) ir gavote gerą pasiūlymą, tačiau prekių, užsakytų internetu niekada negavote	9 proc.
Jūs užsisakėte nemokamą arba labai pigią paslaugą, tačiau po bandomojo laikotarpio išaiškėjo, jog paslaugos mėnesinis mokestis yra labai brangus	8 proc.
Jūs nusipirkote bilietus į renginį, koncertą ar kelionę, tačiau išaiškėjo, jog bilietai yra netikri arba bilietų negavote	2 proc.

[111] *Ibid,* 12.

Kaip matyti lentelėje nr. 18, pats populiariausias sukčiavimo tipas yra apgaulingas pranešimas apie laimėjimą loterijoje ir tam, kad atsiimtų šį laimėjimą asmuo turėtų sumokėti paslaugų mokestį (7486 asmenys), antroje vietoje yra asmens tapatybę identifikuojančių duomenų įgijimas (5881 asmenys), trečioje vietoje yra asmens tapatybę identifikuojančių duomenų įgijimas, kai su asmeniu yra susisiekiama jam apsilankius apgaulingame tinklalapyje (5614 asmenys). Visi kiti sukčiavimai sudaro mažesnę dalį. Du iš trijų populiariausių sukčiavimo tipų yra asmens tapatybę identifikuojančių duomenų įgijimas, kurie gali vėliau būti panaudoti apgaule pasisavinant svetimą turtą (viso nukentėjo 43 proc. apklaustųjų).

19 diagrama. Vartotojų apgaulės apklausoje nurodytų aukų skaičius (procentais) 2018-2019 metais[112] (ES 28, N=26,735; Norvegija, N=1,004, Islandija, N=500)



[112] *Ibid*, 13.

Remiantis diagrama nr. 19, asmenų, nukentėjusių nuo bet kurio sukčiavimo tipo vidurkis Europos Sąjungoje yra 56 proc. Daugiausia nukentėjusiųjų yra Vakarų Europos valstybėse – Airijoje, Jungtinėje Karalystėje, Olandijoje ir Prancūzijoje bei Skandinavijos valstybėse – Norvegijoje ir Danijoje. Lietuva yra beveik sąrašo gale. Manytina, jog sukčiai taikosi į daugiau uždirbančiuosius, turto turinčius ES valstybių narių gyventojus. Danijos statistikos departamento duomenimis[113] 2018 metais Danijos vidutinis metinis darbo užmokestis po mokesčių buvo 227 194 kronos arba 2020 m. spalio 12 d. duomenimis 30 524 eurai, kas būtų 2 543 eurai per mėnesį. Kitose, daugiausiai nukentėjusiose valstybėse darbo užmokestis panašus į Danijoje esantį užmokestį. Lietuvos oficialiosios statistikos duomenimis[114] 2020 m. antrąjį ketvirtį vidutinis atlyginimas po mokesčių buvo 889 eurai. Taigi, lyginant vidutinį Lietuvos atlyginimą su Danijoje esančiu atlyginimu, jis sudaro maždaug trečdalį Danijoje esančio vidutinio darbo užmokesčio. Atsižvelgiant į tokius atlyginimų skirtumus, natūralu, jog sukčiai siekia apgaule įgyti kuo daugiau lėšų, todėl nuo jų daugiausiai nukenčia pažengusiose Europos Sąjungos valstybėse gyvenantys asmenys.

20 lentelė. Vartotojų apgaulės apklausoje nustatyti būdai, kaip su sukčiavimo aukomis buvo susisiekta (procentais) 2018-2019 metais[115] (N=12,850)

Elektroniniu paštu	43 proc.
Skambučiu į jūsų mobilųjį telefoną	15 proc.
Skambučiu į jūsų namų telefoną (laidinį)	14 proc.
Pagal elektroninėje erdvėje rastą reklamą (ne socialiniuose tinkluose)	7 proc.
Trumpąja SMS žinute	5 proc.
Pagal elektroninėje erdvėje rastą reklamą (socialiniuose tinkluose, pavyzdžiui, *Facebook*)	5 proc.
Laišku pašto dėžutėje	4 proc.
WhatsApp, *Facebook messenger* ar kita bendravimo programėle	2 proc.
Sukčius atėjo į mano namus	1 proc.
Sutikau sukčių fizinėje erdvėje, bet ne namuose	1 proc.
Pagal reklamą rastą laikraštyje ar žurnale	0 proc.
Faksu	0 proc.
Kitu būdu	3 proc.

Remiantis Vartotojų apgaulės apklausoje pateiktais duomenimis lentelėje nr. 20, dažniausiai su aukomis buvo susisiekta elektroniniu paštu (43 proc. arba 5526 atvejų), iš esmės naudojantis elektronine erdve bei informacinėmis technologijomis su aukomis buvo susisiekta 57 proc. arba 7325 atvejų. Tokie komunikacijos metodai kaip susisiekimas faksu ar patalpinant

[113] „Income. Statistics Denmark“, Denmark Statistics, žiūrėta 2020 m. spalio 15 d., https://www.dst.dk/en/Statistik/emner/arbejde-indkomst-og-formue/indkomster.
[114] „Darbo užmokestis šalyje.“ Oficialiosios statistikos portalas, žiūrėta 2020 m. spalio 15 d., https://osp.stat.gov.lt/informaciniai-pranesimai?articleId=7938671.
[115] Survey on “Scams and fraud experienced by consumers”, *supra note*, 110: 31.

reklamą žurnale ar naujienų portaluose iš viso nebuvo naudojami sukčių. Aukų apgaulė panaudojant komunikacijos metodus fizinėje erdvėje sudarė po 1 proc. (viso 257 atvejai). Taigi, galima teigti, jog 21 a. sukčiai su aukomis daugiausia susisiekia pasinaudodami elektroninėje erdvėje esančiais privalumais – el. paštu, socialiniais tinklais, taip pat išlieka populiarūs skambučiai telefonu.

Apibendrinant sukčiavimų elektroninėje erdvėje raišką, pabrėžtina, jog lyginant tiriamojo laikotarpio pradžią su tiriamojo laikotarpio pabaiga, užregistruotų sukčiavimų elektroninėje erdvėje Lietuvoje sumažėjo. Tačiau registruoto nusikalstamumo statistika neparodo tikrosios padėties. Anglijoje ir Velse atliktos viktimologinės apklausos duomenimis matyti, jog teisėsaugos institucijose buvo užregistruota 15 proc. sukčiavimų elektroninėje erdvėje. Europos Sąjungoje atlikto Vartotojų apgaulės tyrimo duomenimis pastebėtina, jog daugiausiai nukentėjo respondentai esantys Vakarų Europos ir Skandinavijos šalyse. Taigi, siekiant įvertinti nusikalstamumo raišką ir pamatyti realesnę statistiką būtina atlikti reguliarias viktimologines apklausas.

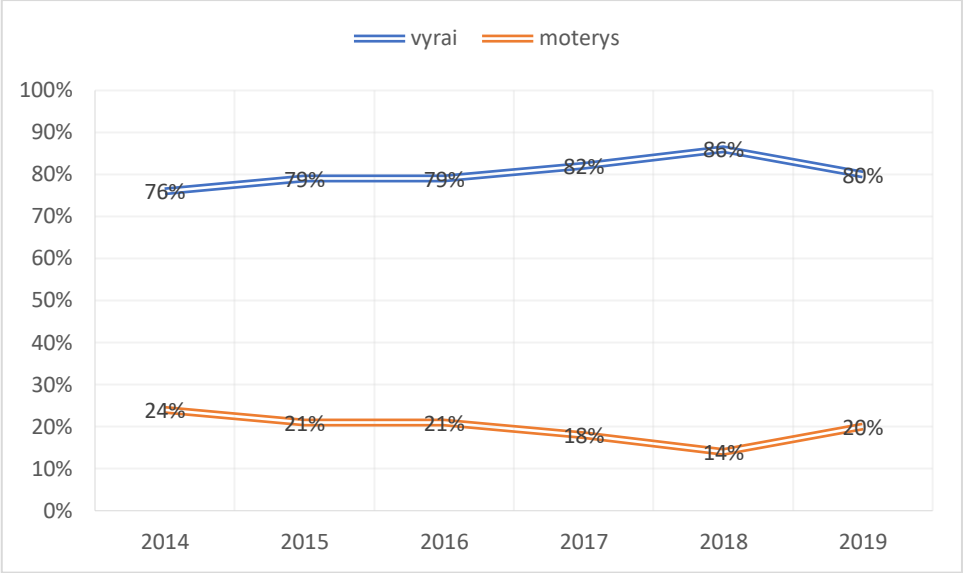
3. SUKČIAVIMUS ELEKTRONINĖJE ERDVĖJE PADARIUSIO ASMENS CHARAKTERISTIKA

Nagrinėjant sukčiavimus elektroninėje erdvėje svarbu apžvelgti ne tik nusikalstamumo raišką, bet taip pat ir registruotos statistikos duomenis, kur atsispindi sukčiavimus elektroninėje erdvėje padariusių asmenų charakteristika. Anot J. Galinaitytės: „nusikaltėlio asmenybė plačiai ir išsamiai apibūdina nusikalstamą veiką padariusį asmenį, apima daugelį įstatymu nenumatytų asmens požymių, tokių kaip psichologinės savybės, asmens vertybių samprata ir panašiai. Kriminologijoje nusikaltėlio asmenybės samprata apima tai, ko neapibrėžia baudžiamasis įstatymas.“[116] Anot F. A. Zuhri, taip, kaip mes matome kibernetinius nusikaltėlius iš dalies yra nulemta Holivudo filmų bei nusikaltimų elektroninėje erdvėje pobūdžio. Kai kurie tipiniai stereotipai apie kibernetinius nusikaltėlius anot visuomenės yra: 1) nemokantys bendrauti, bet geri žmonės; 2) turi gerus techninius įgūdžius ir žinias bei labai aukštą IQ koeficientą; 3) yra vyrai, dažniau berniukai; 4) paaugliai berniukai su kompiuteriniais įgūdžiais ir 5) kibernetiniai nusikaltėliai nenaudoja smurto[117].

Šiame skyriuje bus atskleista kaltinamųjų, padariusių sukčiavimus elektroninėje erdvėje pasiskirstymas pagal lytį, užimtumą, išsilavinimą Lietuvoje 2014–2019 m., šie rodikliai taip pat bus palyginti su mokslinių tyrimų rezultatais apie kibernetinius nusikaltėlius JAV bei Jungtinėje Karalystėje.

[116] Babachinaitė ir kt., *supra note*, 25: 246.
[117] Fadi Abu Zuhru, „The profile of a Cybercriminal.“ (2016), 3, https://www.semanticscholar.org/paper/THE-PROFILE-OF-A-CYBERCRIMINAL-ZUHRI/90a64adad75163d030214a18e9dd7897fae75101.

21 diagrama. Kaltinamųjų, padariusių užregistruotus sukčiavimus elektroninėje erdvėje Lietuvoje 2014-2019 m. pasiskirstymas pagal lytį[118] (procentais)

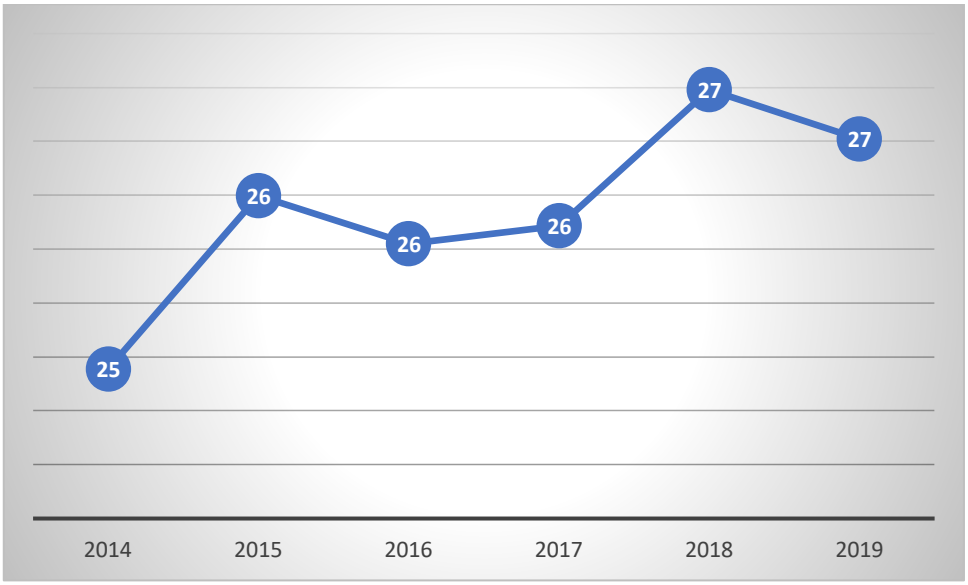


Kaip matyti diagramoje nr. 21 tiriamojo laikotarpio pradžioje vyrų, kaltinamų padariusių sukčiavimą elektroninėje erdvėje buvo 76 proc. (arba 281 atvejai), moterų buvo 24 proc. (arba 87 atvejai). Tiriamojo laikotarpio pabaigoje vyrų dalis sudarė 80 proc. (arba 162 atvejai), moterų – 20 proc. (arba 40 atvejų). Lyginant tiriamojo laikotarpio pradžią su pabaiga, vyrų nusikaltėlių padariusių sukčiavimą elektroninėje erdvėje Lietuvoje dalis padidėjo 4 procentiniais punktais, o moterų sumažėjo 4 procentiniais punktais.

Iš pateiktos statistikos matyti, jog tiriamuoju laikotarpiu vyrai vidutiniškai padarė 80 proc. visų užregistruotų sukčiavimų elektroninėje erdvėje, o moterys vidutiniškai padarė 20 proc. visų užregistruotų sukčiavimų elektroninėje erdvėje. Taigi, vyrai statistiškai padarė daugiau visų registruotų sukčiavimų elektroninėje erdvėje.

22 diagrama. Kaltinamųjų, padariusių užregistruotus sukčiavimus elektroninėje erdvėje Lietuvoje 2014-2019 m. vidutinis amžius[119]

[118] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*30 forma*).
[119] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*30 forma*).



Iš diagramoje nr. 22 pavaizduotų duomenų matyti, jog tiriamojo laikotarpio pradžioje vidutinis kaltinamųjų amžius buvo 25 metai, viso tiriamojo laikotaprio metu vidutinis kaltinamųjų amžius didėjo. Toks rodmuo išliko ir tiriamojo laikotarpio pabaigoje. Manytina, jog sukčiauti elektroninėje erdvėje linkę jaunesni asmenys, kurie susivilioja tokio uždarbio galimybėmis bei sudėtingu jų išaiškinimu. Jaunesni asmenys gali neturėti pastovių pajamų šaltinio siekti apgaule įgyti kitų asmenų turtą pasinaudojus sukčiavimo elektroninėje erdvėje modeliais.

B. Payne ir kiti atliktame 2018 m. tyrime „JAV ieškomiausi nusikaltėliai: kibernetinių nusikaltėlių ir tradicinių nusikaltėlių palyginimas“[120] buvo nustatyta, jog tarp 2017 m. ieškomiausių 235 (92,2 proc.) asmenys buvo vyrai ir 20 (7,8 proc.) asmenų buvo moterys.

H. Copes ir L. M. Vieraitis JAV atlikę nuteistų už tapatybės vagystę[121] savianalizės tyrimą 2006-2007 m. nustatė, jog iš 59 apklaustųjų, 23 buvo vyrai ir 36 buvo moterys, taigi vyrai sudarė 39 proc., o moterys 61 proc. apklaustųjų. Taip pat jie savo tyrime pabrėžė, jog tokį netolygų pasiskirstymą tarp lyčių lėmė tai, jog iš viso buvo numatoma apklausti 187 nuteistuosius vyrus bei 110 nuteistąsias moteris. Kadangi į savianalizės tyrimo klausimus daugiau buvo linkusios atsakyti moterys, nei vyrai, todėl ir matyti, jog didesnę dalį nusikaltėlių sudarė moterys.

G. R. Gordon ir kiti JAV tapatybės vagystės 2000-2006 m. tyrime analizavo ištirtus tapatybės vagystės nusikaltimus[122] iš 517 ištirtų bylų buvo 933 nuteistieji. Iš 933 nuteistųjų už tapatybės vagystę 627 (67,4%) sudarė vyrai, o 303 (32,6 proc.) – moterys.

---

[120] Brian Payne, David C. May ir Lora Hadzhidimova, „America's most wanted criminals: comparing cybercriminals and traditional criminals“, *Criminal Justice Studies*, 32:1, 6, DOI: 10.1080/1478601X.2018.1532420 https://doi.org/10.1080/1478601X.2018.1532420.

[121] Heith Copes ir Lynne M. Vieraitis, „Understanding Identity Theft: Offenders Accounts of Their Lives and Crimes.“ *Criminal Justice Review (Sage Publications)* 34, no. 3 (September 2009): 335. doi:10.1177/0734016808330589. http://cjr.sagepub.com/cgi/content/abstract/34/3/329.

[122] G. R Gordon ir kt., „Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement.“, *NY Center for Identity Management and Information Protection*, (2007): 31. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.216.6696&rep=rep1&type=pdf.

A. Hutchings ir Y. T. Chua teigia, jog kibernetiniai nusikaltimai dažniausiai būna techninio pobūdžio. Techninio pobūdžio nusikaltimai dažnai reikalauja papildomų įgūdžių ar informacinių sistemų išmanymo[123]. Taip pat jie teigia, jog elektroninėje erdvėje padaromi sukčiavimai yra socialinės inžinerijos, kaip apgaulės panaudojimas (***bendro pobūdžio kibernetiniai nusikaltimai***), tačiau kiti sukčiavimai yra sudėtingesni, reikalaujantys apgaulingų elektroninėje erdvėje veikiančių tinklalapių sukūrimo, jų apipavidalinimo ar *botnet* panaudojimo (***techninio pobūdžio kibernetiniai nusikaltimai***)[124]. Moterys JAV gali būti mokomos, jog visa, kas susiję su kompiuteriais yra vyriška, todėl jos rečiau renkasi studijas, susijusias su informacinėmis technologijomis[125]. Autoriai pasisako ir apie informacinių technologijų (toliau – IT) studijas JAV: moterys, nusprendusios studijuoti šią sritį susiduria su mažesniu palaikymu, į moteris, studijuojančias studijas, susijusias su IT žiūrima iš aukšto, neva jos neturi tam reikiamų įgūdžių, mesti IT studijas moterys gali pasirinkti ir dėl mažesnio moterų skaičiaus fakulteto administracijoje[126]. Panašią nuomonę turi ir VDU Informatikos fakulteto dekanė: „Didesnėje dalyje informatikos studijų programų merginos tesudaro 20 proc. ar net mažiau studentų“[127]. Iš to seka, jog vyrai daugiau renkasi informacinių technologijų studijas, jie įgyja techninio pobūdžio žinių, todėl sėkmingiau gali rengti techninio pobūdžio sukčiavimus elektroninėje erdvėje, nukreiptus į fizinius asmenis, pavyzdžiui, apgaulingų tinklalapių, siekiant įgyti asmens tapatybę identifikuojančius duomenis sukūrimas, jų platinimas, panaudojant *smišingo* žinutes, *fišingo* laiškus.

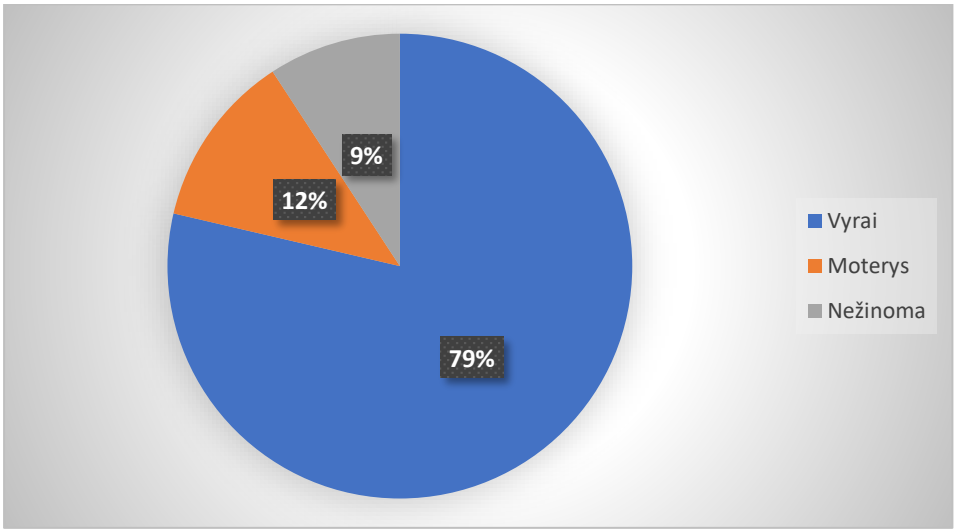
Kitas, anot A. Hutchings ir Y. T. Chua lemiantis faktorius greta techninio pobūdžio žinių, kodėl sukčiavimus elektroninėje erdvėje padaro daugiau vyrai, nei moterys, yra neformalios žinios[128]. Šios žinios yra įgyjamos kibernetinių nusikaltėlių elektroninėje erdvėje veikiančiuose diskusijų bendruomenėse. Elektroninėje erdvėje fizinė asmenų charakteristika (ūgis, svoris, plaukų spalva ir kt.) yra nematoma, viską lemia lytis. Būtent dėl lyties moterys elektroninėje erdvėje esančiuose nusikaltėlių diskusijų bendruomenėje vertinamos skirtingai – dėl moterų IT technologijų neišmanymo, žiūrėjimo į jas kaip į „silpnąją lytį“[129]. Vėlgi, dėl elektroninės erdvės specifikos bei tokio pobūdžio diskusijų bendruomenių siekiamo išlaikyti anonimiškumo registruojantis į uždarą sukčių forumą, pavyzdžiui *carders.ws*, lyties nurodyti nereikia. Net jeigu

[123] Thomas J. Holt, *Cybercrime Through an Interdisciplinary Lens* (London: Routledge, 2017), 167. https://doi-org.skaitykla.mruni.eu/10.4324/9781315618456.
[124] *Ibid*, 167.
[125] *Ibid*, 170.
[126] *Ibid*, 171.
[127] „Ar daugės moterų IT srityje?“, VDU, žiūrėta 2020 m. spalio 17 d., https://www.vdu.lt/lt/ar-dauges-moteru-it-srityje/.
[128] Holt, *supra note*, 123: 171.
[129] *Ibid*, 171.

ir reiktų nurodyti lytį, moterys galėtų pasirinkti, jog jos yra vyrai ir *vice versa*. Todėl nėra aišku, kiek tokiose uždarose sukčių bendruomenėse elektroninėje erdvėje yra vyrų ir kiek – moterų.

A. Hutchings ir Y. T. Chua taip pat atliko empirinį tyrimą – 2010-2015 m. Jungtinėje Karalystėje ištirtų kibernetinių nusikaltimų bylų tyrimą. Iš viso buvo apžvelgta 412 bylų. Šie kibernetiniai nusikaltimai apima sukčiavimą, bendrininkavimą, nusikaltimus susijusius su valstybės tarnyba, duomenų apsaugos pažeidimai, neteisėtai įgytų lėšų legalizavimą, kiek tai susiję su nusikaltimais elektroninėje erdvėje.

23 diagrama. Nusikaltėlių, pasiskirstymas pagal lytį iš ištirtų 2010-2015 m. Jungtinės Karalystės kibernetinių nusikaltimų bylų[130] (N=412)

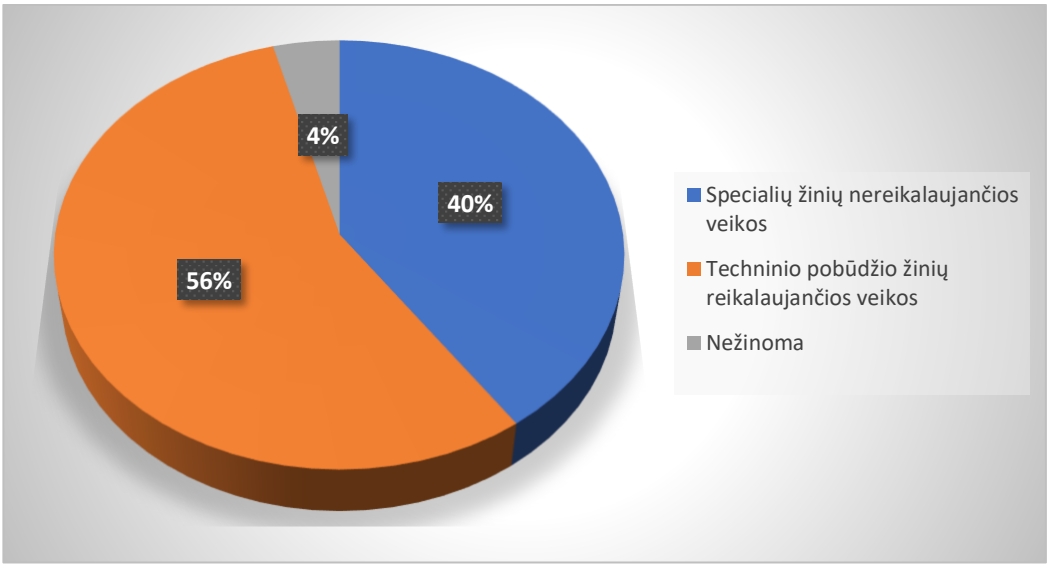


Kaip matyti diagramoje nr. 23, didžioji dalis 324 (79 proc.) nusikaltimų JK įvykdė vyrai, tik 50 (12 proc.) nusikaltimų įvykdė moterys. Greta to autoriai uždavė klausimą kibernetiniams nusikaltėliams bei tokio pobūdžio bylas tiriantiems pareigūnams: „Kiek moterų jūsų manymu dalyvauja kibernetiniuose nusikaltimuose?“[131]. Į šį klausimą kai kurie respondentai atsakė sekančiai[132]:

1. „Aš nemanau, kad kibernetiniuose nusikaltimuose dalyvauja daug moterų, asmeniškai pažinojau tik vieną merginą, kuri buvo įtraukta į visą šį reikalą.“ (Respondentas, vyras, 22 metai)
2. „Žinai, man reikia gan smarkiai pasukti galvą ir pagalvoti, ar prisimenu bent vieną moterį, kuri buvo tyrimo taikinys ir nemanau, kad aš prisiminsiu bent vieną moterį. Aš manau, kad tikrai turėtų būti bent viena moteris, bet tai yra labai retas atvejis.“ (Teisėsaugos pareigūnas nr. 8)

[130] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš Thomas J. Holt, *Cybercrime Through an Interdisciplinary Lens* (London: Routledge, 2017), 176. https://doi-org.skaitykla.mruni.eu/10.4324/9781315618456.
[131] Holt, *supra note*, 123: 176.
[132] Holt, *supra* note, 123: 176-177.

24 diagrama. Kibernetinių nusikaltimų pasiskirstymas pagal sudėtingumą iš ištirtų 2010-2015 m. Jungtinės Karalystės kibernetinių nusikaltimų bylų[133] (N=412)



Kaip matyti, diagramoje nr. 24, didesnė dalis (56 proc. arba 229) kibernetinių nusikaltimų reikalavo specifinių techninio pobūdžio žinių – IT principų išmanymo, mokėjimo pritaikyti specifinius įrankius vykdant kibernetinius nusikaltimus, tai – *skriptai*, apgaulingų laiškų siuntėjai, neteisėtas poveikis elektroniniams duomenims, informacinei sistemai ir kt. Kitos veikos, pavyzdžiui sukčiavimai elektroninėje erdvėje, nereikalaujantys papildomų specifinių techninių įgūdžių sudarė apie 40 proc. arba 166 veikas. Respondentas teisėsaugos pareigūnas pasisakė apie įgūdžių naudojimą kibernetiniuose nusikaltimuose:

1. „Na, tai yra didelis skirtumas. Mes nematome daug moterų. Buvo keletas moterų, tačiau jos buvo recidyvistės. Nebuvo jokių moterų įsilaužėlių (hakerių), jos darė nusikaltimus, nereikalaujančius specifinių žinių, pavyzdžiui, sukčiavimas internetiniuose aukcionuose.“[134] (Teisėsaugos pareigūnas nr. 10).

A. Hutchings ir Y. T. Chua tyrime taip pat respondentų kibernetinių nusikaltimų tyrėjų bei kibernetinių nusikaltėlių paklausė šio klausimo: „Kokie socialiniai veiksniai gali paaiškinti tai, jog moterys mažiau įsitraukia į kibernetinius nusikaltimus?“. Respondentai atsakė sekančiai[135]:

1. „Jeigu atvirai, tai vyrai ir moterys visuomenėje yra pasidalinę „vaidmenimis“. Dažnai matau, kaip vaikinai susitinka su draugais ir kažką veikia, merginos – skaito knygas, darosi makiažą, daro visus tuos moteriškus dalykus, na žinai.“ (Respondentas, vyras, 27 metai).

[133] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš Thomas J. Holt, *Cybercrime Through an Interdisciplinary Lens* (London: Routledge, 2017), 177, https://doi-org.skaitykla.mruni.eu/10.4324/9781315618456.
[134] Holt, *supra note*, 123: 177-178.
[135] Holt, *supra* note, 123: 179-180.

2. „Ah, aš manau, kad visa kompiuterinė industrija yra daugiau vyriška, aš nežinau, kodėl taip yra, bet manau jog, mano pirmoji pažintis su kompiuterine įranga buvo žaidžiant žaidimus, kaip ir kitų žmonių. Mano manymu visa žaidimų erdvė yra labai antifeministinė. Aš manau, kad tai yra didžiulė problema, bet yra taip, kaip yra.“ (Respondentas, vyras, 18 metų).

3. „Na, mano universitete, jeigu nueitumėte į IT studijų programų klases, nepamatytumėte daug moterų, pavyzdžiui, nuėjus į verslo studijų krypties užsiėmimus, ten jos visos susirenka.“ (Respondentas, vyras, 22 metai).

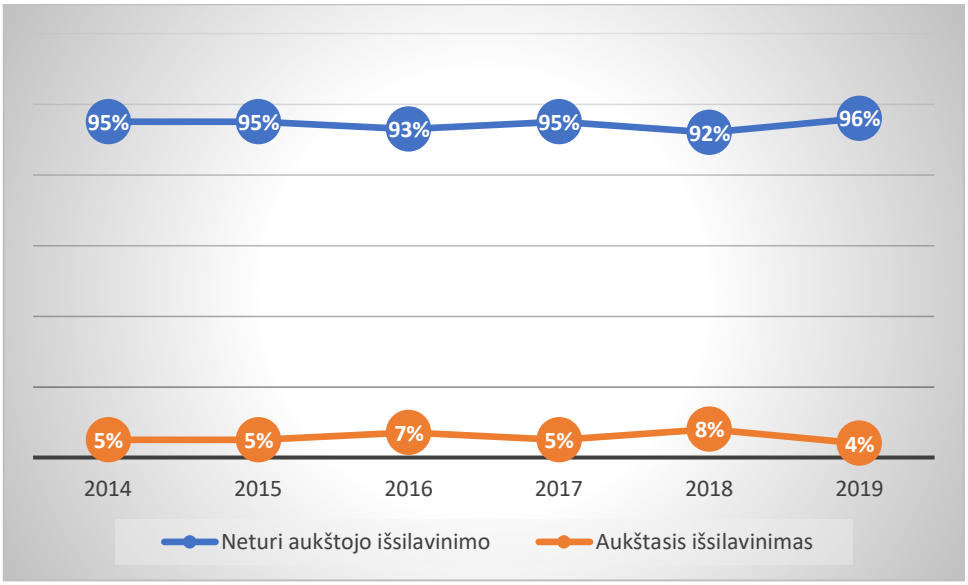
4. „Galbūt dauguma moterų nejaučia tokio potraukio IT technologijoms, kaip vyrai, Dauguma moterų iš tikrųjų turi gyvenimą, nepraleidžia tiek daug laiko internete. Vyrai kibernetiniai nusikaltėliai yra dažniausiai pamišę dėl kompiuterinės įrangos. Vyrai dažnai neskiria realaus pasaulio nuo kibernetinės erdvės.“ (Teisėsaugos pareigūnas nr. 9).

5. „Vyrai lengviau pasirinktų sekantį variantą – praleisti prie kompiuterio 8 valandas per dieną, 7 dienas per savaitę su niekuo nekalbėdami. Moterims svarbesnė socializacija, bendravimas. 19 metų paauglys vyras greičiausiai per daug negalvodamas praleistų prie savo kompiuterio visą naktį, kai tuo tarpu moterys – pagalvotų prieš tai darydamos, kadangi jos turi geresnių užsiėmimų praleisti savo laisvą laiką.“ (Teisėsaugos pareigūnas nr. 14).

Taigi, sukčiavimas elektroninėje erdvėje apima ne tik įprastos apgaulės panaudojimą, specialių žinių nereikalaujančias veikas (tokios kaip romantinis sukčiavimas, investicinis sukčiavimas), bet ir techninio pobūdžio žinių reikalaujantys sukčiavimai (smišingas, fišingas), kur norint sėkmingai įgyti asmens tapatybę identifikuojančius duomenis sukčiai turi sukurti bei sufalsifikuoti finansų įstaigos ar kito juridinio asmens tinklalapį, taip pat paskleisti informaciją apie netikrą tinklalapį, tam, kad įgytų konfidencialią informaciją. Būtent tokio pobūdžio žinių galima įgyti studijuojant su IT susijusią specialybę. Tačiau kaip ir parodė atskleista informacija, maža dalis moterų renkasi tokio tipo studijas, kadangi, jos yra daugiau „vyriškos“.

25 diagrama. Kaltinamųjų, padariusių užregistruotus sukčiavimus elektroninėje erdvėje Lietuvoje 2014-2019 m. pasiskirstymas pagal išsilavinimą[136] (procentais)

[136] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*30 forma*). Baigiamojo darbo autorius aukštąjį universitetinį (aukštesnįjį) bei aukštąjį universitetinį išsilavinimus diagramoje atvaizduoja po „Aukštasis“ žyma. Pradinį, pagrindinį, vidurinį, profesinį bei neturi išsilavinimo autorius vaizduoja po „Neturi aukštojo išsilavinimo“ žyma.



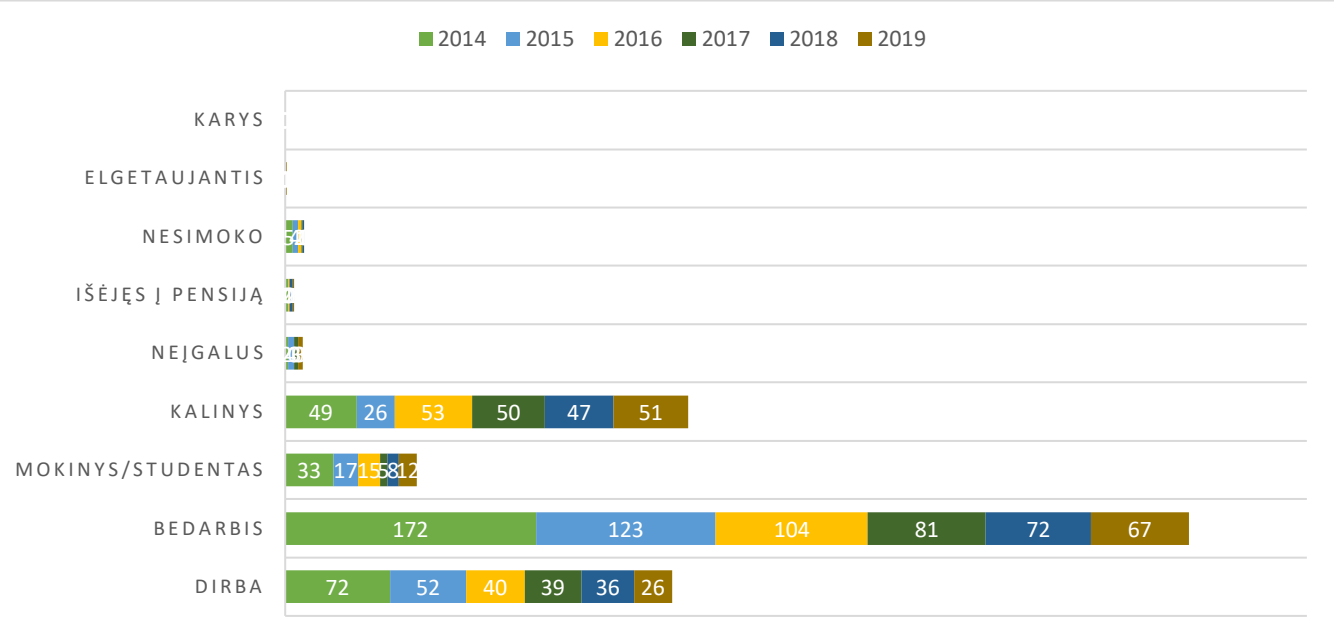
Kaip matyti diagramoje nr. 25 tiriamojo laikotarpio pradžioje nusikaltėliai su aukštuoju išsilavinimu padarė 5 proc. visų veikų (20 atvejų), kai nusikaltėliai neturintys aukštojo išsilavinimo padarė 95 proc. visų veikų (348 atvejai). Didžiausias sukčių turinčių aukštąjį išsilavinimą skaičius fiksuotas 2018 m., kai jie sudarė 8 procentinius punktus. Tiriamojo laikotarpio pabaigoje lyginant su tiriamojo laikotarpio pradžia sukčių, turinčių aukštąjį išsilavinimą sumažėjo 1 procentiniu punktu, atitinkamai padidėjo sukčių, neturinčių aukštojo išsilavinimo procentinė dalis.

Manytina, jog dažniausiai būna ištiriamos tik nežinančių kaip apsaugoti savo identitetą elektroninėje erdvėje, neturinčių specialių įgūdžių sukčių veikos. Anot. V. Kalpoko: „[...] dėl interneto teikiamo anonimiškumo tikimybė atskleisti tokį nusikaltimą gali būti vertinama kaip labai menka.“[137]. Elektroninėje erdvėje asmenis identifikuoja IP adresas bei techniniai naršyklės, kuri naudojama duomenys. Pavyzdžiui, *whatsmyuseragent.org* tinklalapyje galima sužinoti savo informacinės sistemos duomenis bei IP adresą. Būtent tokį virtualų pėdsaką elektroninėje erdvėje palieka sukčiai. Tačiau šiuos identifikatorius galima pakeisti. Tam yra naudojama speciali programinė įranga, pavyzdžiui, *VPN* (angl. *virtual private network*), kuri pakeičia asmens IP adresą bei šifruoja asmens naršymo informaciją. Taip pat sukčiai elektroninėje erdvėje gali naudoti kelių lokacijų *VPN*. Tai gali būti *Rusija -> Malta ->* sukčiaus originalus *IP* adresas arba dar daugiau kintamųjų. Neteisėtai paveikus ir prisijungus prie finansų įstaigos informacinės sistemos, jos darbuotojai matys, kad sukčius pagal IP adresą yra iš Rusijos. Tačiau iš tikrųjų Rusija yra tik priedanga ir tikrojo IP adreso gali net nepavykti išsiaiškinti. Aukštesnio intelekto sukčiai, kurie elektroninėje erdvėje sukčiauja profesionaliai, jiems tai yra vienas iš pagrindinių pragyvenimo šaltinių, manytina, jog tam, kad sumažintų nusikalstamos veikos atskleidimo riziką, naudoja

[137] Gintautas Sakalauskas ir kt., *Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai. Teisės instituto mokslo tyrimai, 7 tomas* (Vilnius: Eugrimas, 2011), 175.

panašias „apsaugos“ priemones. Baigiamojo darbo autoriaus nuomone, tokias apsisaugojimo priemones naudoja aukštąjį išsilavinimą turintys sukčiai, tačiau savo gebėjimus panaudoja nusikalstamiems tikslams.

26 diagrama. Nusikaltėlių, padariusių užregistruotus sukčiavimus elektroninėje erdvėje Lietuvoje 2014-2019 m. pasiskirstymas pagal užimtumą[138]



Kaip matyti diagramoje nr. 26 tiriamojo laikotarpio pradžioje 2014 m. didžiausią dalį (47 proc.) sudarė bedarbiai asmenys. Bedarbių asmenų padaromi sukčiavimai elektroninėje erdvėje tiriamojo laikotarpio metu mažėjo – 2015 m. - 49 proc., 2016 m. - 38 proc., 2017 m. - 39 proc., 2018 m. - 34 proc., tiriamojo laikotarpio pabaigoje – 33 proc.

Greta bedarbių kaltinamųjų tiriamojo laikotarpio pradžioje 2014 m. didžiausias skaičius buvo ir dirbančių kaltinamųjų – 20 proc., šių asmenu padaromi sukčiavimai elektroninėje erdvėje stabiliai mažėjo – 2015 m. sudarė 20 proc., 2016 m. – 15 proc., 2017 m. – 19 proc., 2018 m. – 17 proc., tiriamojo laikotarpio pabaigoje – 13 proc. Taigi, lyginant dirbančių nusikaltėlių ir bedarbių santykį, galima teigti, jog bedarbiai nusikaltėliai padarė dvigubai daugiau sukčiavimų elektroninėje erdvėje, nei dirbantieji. Anot J. Galinaitytės: „nusikalstamumo kilmę ir raidą lemia ne tik konkretūs socialinės būties faktai [...] bet ir neigiamas socialinis klimatas valstybėje, socialinių institutų disfunkcija, neigiamos ekonominių santykių raidos pasekmės. Iš pastarųjų išskirtini du reiškiniai, darantys tiesioginę įtaką nusikalstamumo dinamikai: nedarbas bei socialinė diferenciacija.“[139]. Būtent nedarbas, asmenų socialinė nelygybė gali padidinti nusikalstamumą.

[138] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*30 forma*).
[139] Babachinaitė ir kt., *supra note*, *25*: 183.

Lengvas uždarbis elektroninėje erdvėje gali bedarbius paskatinti daryti sukčiavimus elektroninėje erdvėje.

Teistumą turintys asmenys tiriamojo laikotarpio pradžioje 2014 m. kaltinami padarę 13 proc. sukčiavimų elektroninėje erdvėje, 2015 m. šis skaičius išliko panašus, nuo 2016 m. pastebėtinas padidėjęs teistumą turinčių asmenų padaugėjimas - 19 proc. Šio skaičiaus didėjimas matomas ir 2017 m. – 24 proc. 2018 metais teistumą turinčių nusikaltėlių padaromų sukčiavimų dalis šiek tiek sumažėja iki 22 proc., tačiau tiriamojo laikotarpio pabaigoje 2019 m. vėl padidėja ir siekia beveik 2 kartus didesnę procentinę dalį nei tiriamojo laikotarpio pradžioje – 25 proc. Būtent kaliniams sukčiavimą elektroninėje erdvėje palengvina pats veikos pobūdis, kad ši gali būti vykdoma iš bet kurio pasaulio taško, nebūtina aukos-nusikaltėlio tiesioginė interakcija. Kaliniai veikdami su laisvėje esančiais bendrininkais, paskambina aukai ir prisistatydami policijos pareigūnu, banko darbuotoju ar kitu asmeniu praneša apgaulingą informaciją ir *višingo* būdu įgyja asmens tapatybę identifikuojančius duomenis.

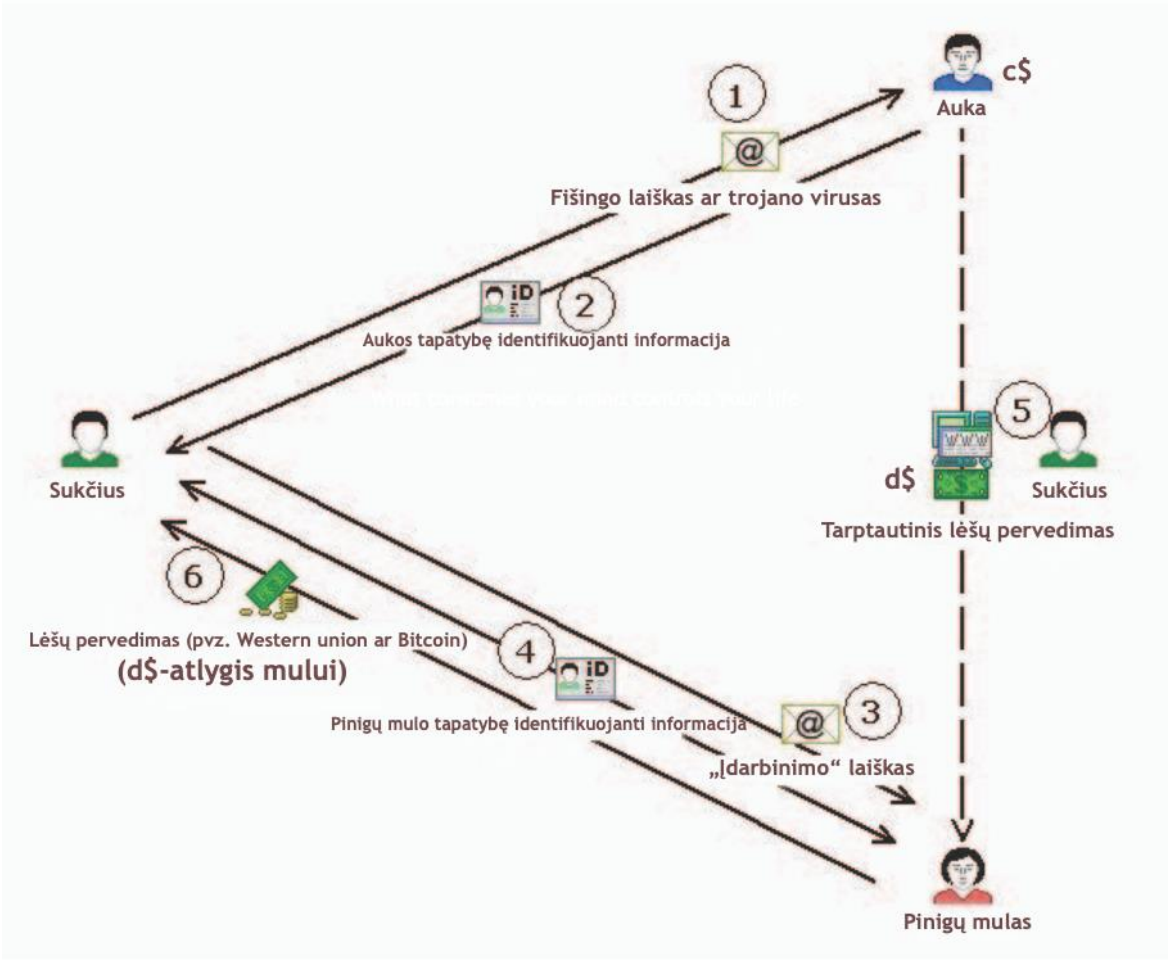
Sukčiai elektroninėje erdvėje panaudoję pirmoje darbo dalyje aptartus sukčiavimo modelius, norėdami pabaigti savo nusikalstamą veiką ir neteisėtai įgyti lėšas jas turi pervesti į kitą finansų įstaigoje esančią sąskaitą. Dažniausiai sukčiai elektroninėje erdvėje neperveda pinigų iš aukos sąskaitos tiesiogiai į savo asmeninę sąskaitą, kadangi taip būtų nesudėtinga atsekti pinigų judėjimo kelią[140]. Nusikaltėliai naudojasi pinigų mulais (angl. *money mule*). Šie asmenys, net patys to nesuprasdami gali tapti sukčių elektroninėje erdvėje bendrininkais. Jie už tai, jog duoda pasinaudoti sukčiams savo elektroninės bankininkystės duomenimis gauna 7–10% fiksuotą atlygį nuo neteisėtai įgytų lėšų[141].

27 pav. Aukos-sukčiaus-pinigų mulo interakcija, schema[142]

[140] Bart HM Custers, Ronald LD Pool ir Remon Cornelisse, „Banking Malware and the Laundering of Its Profits.“ *European Journal of Criminology* 16, no. 6 (November 2019): 735. doi:10.1177/1477370818788007. https://journals.sagepub.com/doi/pdf/10.1177/1477370818788007.

[141] Manuel Aston, Stephen McCombie, Ben Reardon, ir Paul Watters, „A Preliminary Profiling of Internet Money Mules: An Australian Perspective. In Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing“ *IEEE Computer Society, USA* (July 2009): 483. doi:10.1109/UIC-ATC.2009.63 https://research-management.mq.edu.au/ws/portalfiles/portal/62417793/Publisher+version+%28open+access%29.pdf.

[142] *Ibid*, 484.



Pirmos stadijos metu sukčius ar sukčių grupuotė išsiunčia aukai (-*oms*) apgaulingą *fišingo* laišką. Antros stadijos metu kai kurios aukos atidariusios *fišingo* laišką suveda savo asmens tapatybę identifikuojančius duomenis. Trečios stadijos metu sukčius masiškai siunčia „įdarbinimo“ laiškus pinigų mulams, neva tai yra „apskaitininko“, „finansų darbuotojo“ ir kt. darbas. Ketvirtos stadijos metu, pinigų mulai susidomėję daug laiko neįpareigojančiu skirti darbo pasiūlymu ir už tai galintys gauti pinigį atlygį sukčiams elektroninėje erdvėje perduoda savo prisijungimo prie elektroninės bankinkystės kodus ir slaptažodžius. Penktos stadijos metu sukčius pasinaudodamas aukos duomenimis inicijuoja lėšų pervedimą į pinigų mulo sąskaitą. Šeštos stadijos metu, pinigų mulas pasilieka nustatytą procentą, pavyzdžiui, jeigu iš aukos penktos stadijos metu buvo išviliota 10 tūkst. eurų, tai galėtų būti 700-1000 eur., o likusią sumą (apie 9 tūkst. eurų) išgrynina ir perveda sukčiui per *Western Union* (toliau – WU) ar bitkoinais. Pinigus vedant per WU platformą sukčius gali nurodyti ne savo, o kito pinigų mulo, kuris pinigus pasiims grynais, duomenis. Taigi, visos šios schemos tikslas yra nuslėpti neteisėtai įgytų pinigų kilmę pasinaudojant tarpiniu asmeniu – pinigų mulu. Aukai kreipiantis į teisėsaugos institucijas, vienintelis įtariamasis bus pinigų mulas, nes į jo banko sąskaitą buvo pervesti *fišingu* įgytos lėšos.

Apibendrinant didesnė dalis sukčių elektroninėje erdvėje yra vyrai. Dažniau statistiškai yra pagaunami aukštojo įsilavinimo neturintys asmenys, nevykėliai, galimai dėl nemokėjimo paslėpti

savo identiteto elektroninėje erdvėje. Sukčiai, siekdami legalizuoti neteisėtai įgytas lėšas kaip bendrininkus pasitelkia pinigų mulus.

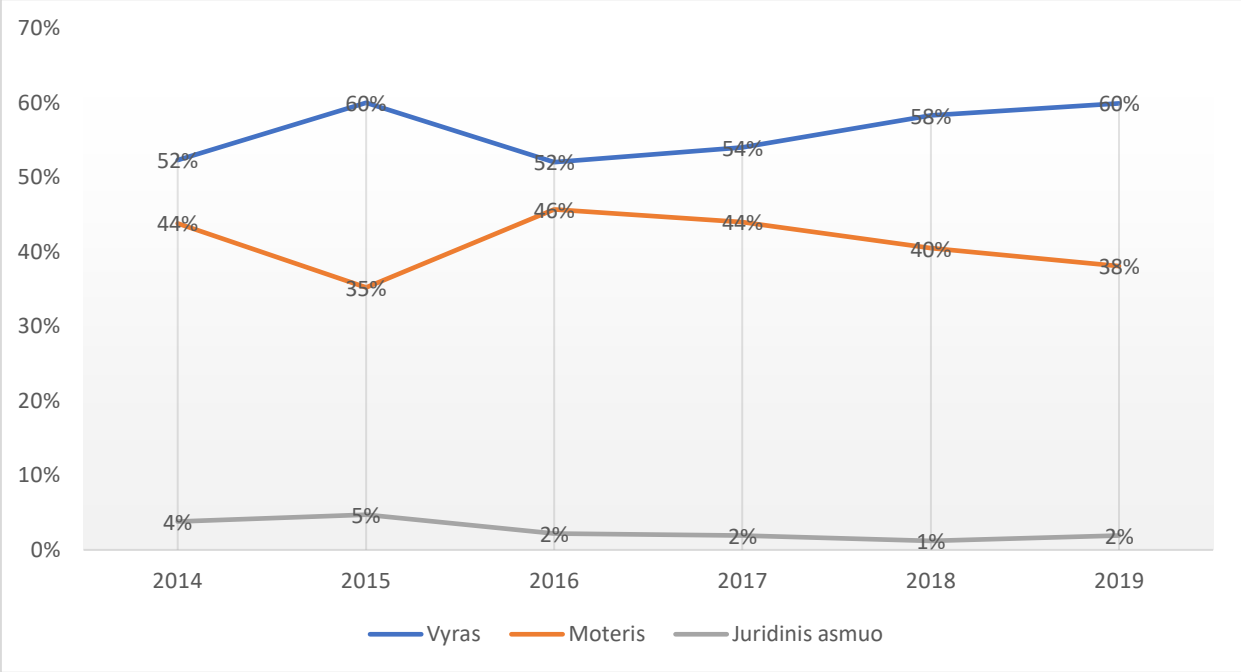
4. NUKENTĖJUSIOS NUO SUKČIAVIMŲ ELEKTRONINĖJE ERDVĖJE AUKOS CHARAKTERISTIKA IR PASEKMĖS JAI

Aptarus nusikaltėlio charakteristiką, taip pat būtina apžvelgti kitos sukčiavimo elektroninėje erdvėje pusės – aukos charakteristiką. Anot Jūratės Galinaitytės: „kiekvienas žmogus yra pažeidžiamas [...] Auka viktimologijoje – tai konkretus žmogus arba įvairias integracijos formas turinti žmonių bendruomenė, kuriai nusikalstama veika tiesiogiai arba netiesiogiai padaryta moralinė, psichinė, fizinė arba materialinė žala, nesvarbu, ar jie įstatymo nustatyta tvarka pripažinti nukentėjusiais ir save tokiais laiko.“[143] Australų kriminologai C. Cross ir kiti sukčiavimą elektroninėje erdvėje apibrėžė kaip: „asmuo, kuris naudojasi elektronine bankininkyste bei atsako į nesąžiningą kvietimą, prašymą, pranešimą ar pasiūlymą bei pateikia konfidencialią informaciją ar perveda lėšas ir dėl to patiria turtinę ar neturtinę žalą“[144]. C. Cross taip pat pasisako apie sukčiavimo elektroninėje erdvėje vietą: „nusikaltėliai vienoje valstybėje gali mėginti apgauti auką kitoje valstybėje, auka gali pervesti lėšas į dar kitas valstybes“[145]. Taigi, elektroninėje erdvėje auka niekada nežino ir galimai negali įsivaizduoti, su kuo ji iš tikrųjų bendrauja ir kam perveda lėšas.

Šiame skyriuje bus atskleista užregistruotų sukčiavimų elektroninėje erdvėje Lietuvoje 2014-2019 m. aukų charakteristika.

28 diagrama. Aukų pasiskirstymas pagal rūšį už užregistruotus sukčiavimus elektroninėje erdvėje Lietuvoje 2014-2019 m. (procentais)[146]

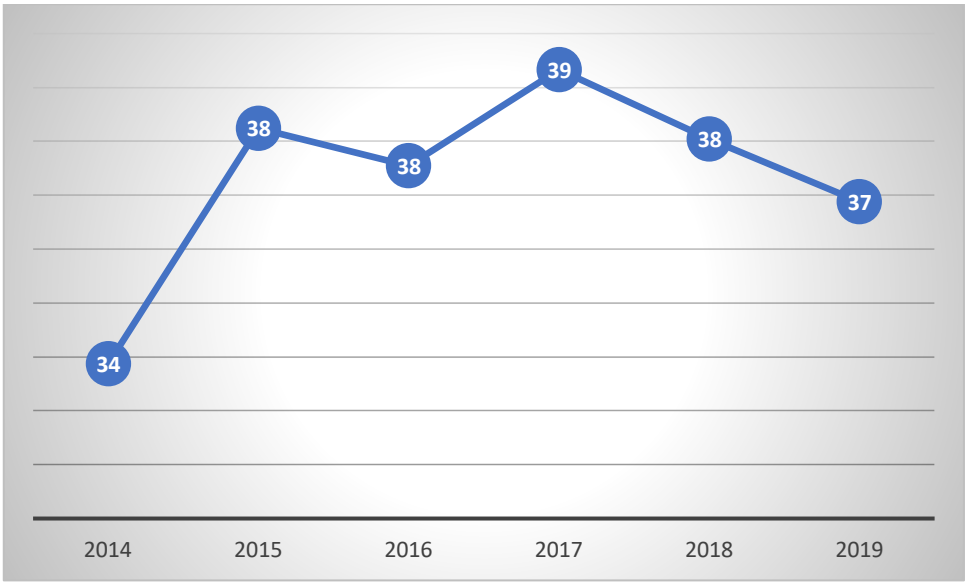
[143] Babachinaitė ir kt., *supra note*, 25: 322.
[144] Cassandra Cross, Russell G. Smith ir Kelly Richards, „Challenges of Responding to Online Fraud Victimisation in Australia.“ *Trends & Issues in Crime & Criminal Justice*, no. 474 (May 2014): 1. https://www.aic.gov.au/publications/tandi/tandi474.
[145] Cassandra Cross, „Oh We Can't Actually Do Anything about That': The Problematic Nature of Jurisdiction for Online Fraud Victims.“ *Criminology & Criminal Justice: An International Journal* 20, no. 3 (July 2020): 1. doi:10.1177/1748895819835910. https://journals.sagepub.com/doi/pdf/10.1177/1748895819835910.
[146] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*50 forma*).



Kaip matyti diagramoje nr. 28 tiriamojo laikotarpio pradžioje 2014 m. aukos vyrai sudarė 52 proc., moterys 44 proc, o juridiniai asmenys 2 proc. Tiriamojo laikotarpio pabaigoje 2019 m. pastebėtina, jog aukos vyrai nukentėjo nuo sukčių elektroninėje erdvėje 8 proc. daugiau, aukų moterų procentinė dalis lyginant su tiriamojo laikotarpio pradžia, atvirkščiai – sumažėjo 6 procentiniais punktais, matomas dvigubas juridinių asmenų aukų dalies mažėjimas. Baigiamojo darbo autoriaus nuomone, vyrai yra linkę daugiau rizikuoti nei moterys, todėl galimas vyrų aukų skaičiaus didėjimas investicijų sukčiavime. M. T. Whitty[147] 2018 m. psichologinių romantinio sukčiavimo aukų Australijoje savybės tyrime pabrėžė, jog romantinio sukčiavimo aukomis dažniau tampa moterys. Taigi, manytina, jog užregistruoto nusikalstamumo statistikoje atvaizduojami duomenys gali nesutapti su moksliniuose tyrimuose esančiais duomenimis dėl sukčiavimo modelių statistinėse kortelėse neišskyrimo į atskiras kategorijas.

29 diagrama. Lietuvoje užregistruotų sukčiavimų elektroninėje erdvėje 2014-2019 m. aukų vidutinis amžius[148]

[147] Whitty, *supra note*, 42: 106.
[148] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*50 forma*).

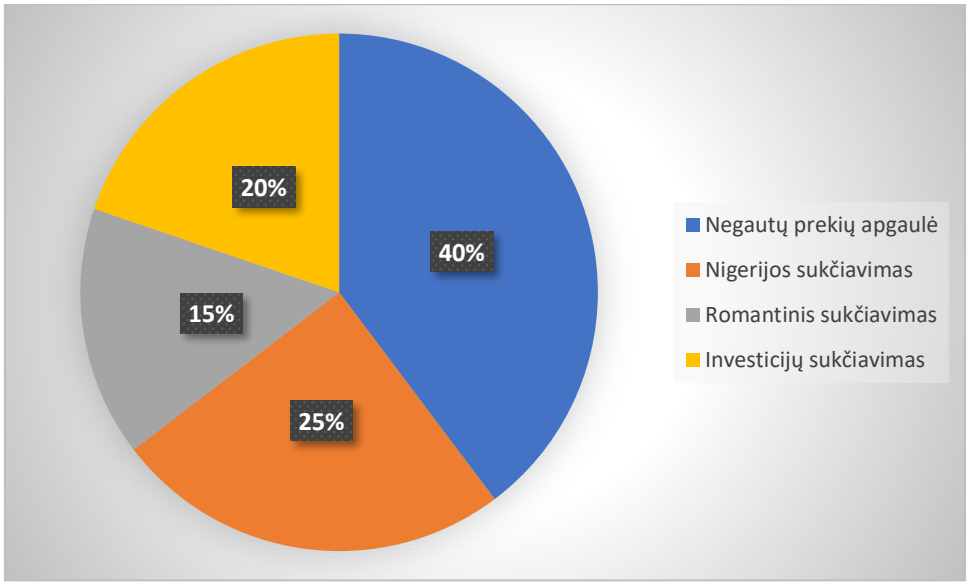


Kaip matyti iš diagramos nr. 29 vidutinis aukų amžius už užregistruotus sukčiavimus elektroninėje erdvėje Lietuvoje tiriamojo laikotarpio pradžioje 2014 m. buvo 34 metai. 2015 metais pastebimas vidutinės aukos amžiaus padidėjimas 4 metais. Šis skaičius išliko panašus iki 2017 metų. 2017 metais matomas didžiausias vidutinis aukų amžius – 39 metai. Tiriamojo laikotarpio pabaigoje 2019 m. vidutinis aukų amžius sumažėjo iki 37 metų. Manytina, jog sukčiai elektroninėje erdvėje taikosi į vyresnius, darbo rinkoje įsitvirtinusius, gaunančius stabilias pajamas ir daugiau uždirbančius asmenis. Pastebėtina, jog, pavyzdžiui, 25 metų studentas gali neturėti darbo ir vis dar būti išlaikomas tėvų, todėl iš tokio asmens neteisėtai fišingo būdu įgijus asmens tapatybę identifikuojančius duomenis sukčius banko sąskaitoje gali nieko nerasti.

M.T. Whitty 2020 m. Jungtinėje Karalystėje atliko empirinį tyrimą bei apklausė 531 nukentėjusįjį nuo sukčiavimo elektroninėje erdvėje. Nukentėjusiųjų buvo paprašyta nurodyti, nuo kokio sukčiavimo elektroninėje erdvėje modelio jie patyrė žalą.

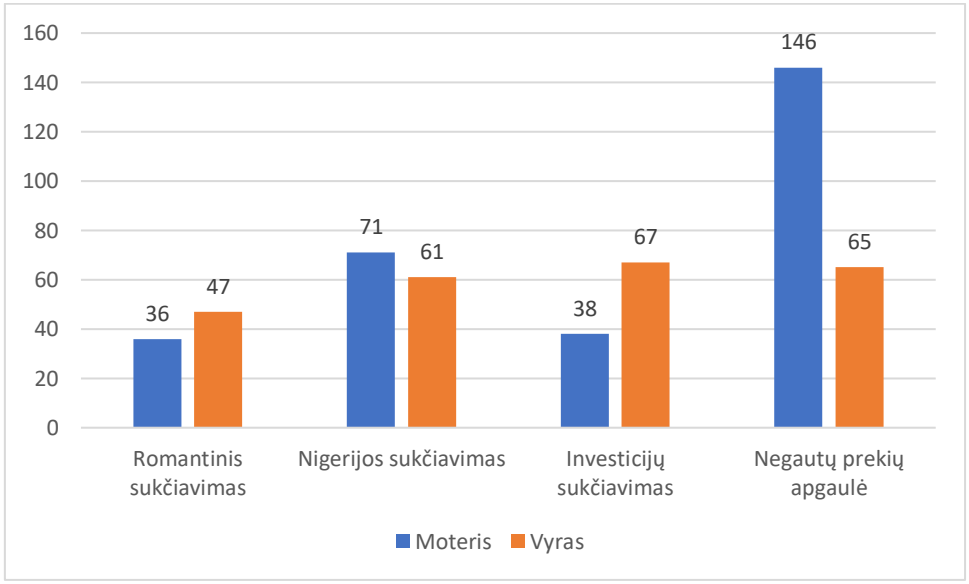
30 diagrama. 2020 m. Jungtinėje Karalystėje atliktos apklausos, nukentėjusių nuo sukčių respondentų pasiskirstymas pagal sukčiavimo modelį (N=531)[149]

[149] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš Monica Therese Whitty, „Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims.“ *European Journal on Criminal Policy & Research* 26, no. 3 (September 2020): 404. doi:10.1007/s10610-020-09458-z. https://www.deepdyve.com/lp/springer-journal/is-there-a-scam-for-everyone-psychologically-profiling-cyberscam-SfX3P9WJTi?key=springer.



Kaip matyti iš diagramos nr. 30, didžioji dalis nukentėjusiųjų nuo sukčių elektroninėje erdvėje Jungtinėje Karalystėje nukentėjo nuo negautų prekių apgaulės, panašią procentinę dalį sudarė „Nigerijos“ bei investicijų sukčiavimai, o nuo romantinio sukčiavimo nukentėjo mažiausia dalis aukų – 15 proc. Baigiamojo darbo autoriaus nuomone, ne visos aukos galimai sutiko atsakyti į tai, jog jos nukentėjo nuo romantinio sukčiavimo. Skirtingai nuo kitų sukčiavimo modelių, romantinio sukčiavimo modelio metu auka ne tik apgaule praranda turtą, bet ir savo mylimąjį (-ą), kuriam jautė jausmus.

31 diagrama. 2020 m. Jungtinėje Karalystėje atliktos apklausos, nukentėjusių nuo sukčių respondentų pasiskirstymas pagal sukčiavimo modelį ir nukentėjusiojo lytį (N=531)[150]



[150] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš Monica Therese Whitty, „Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims.“ *European Journal on Criminal Policy & Research* 26, no. 3 (September 2020): 407. doi:10.1007/s10610-020-09458-z. https://www.deepdyve.com/lp/springer-journal/is-there-a-scam-for-everyone-psychologically-profiling-cyberscam-SfX3P9WJTi?key=springer.

Kaip matyti diagramoje nr. 31, moterys daugiausia nukentėjo nuo Nigerijos sukčių bei negautų prekių apgaulės, o vyrai – dėl romantinio sukčiavimo bei investicijų sukčiavimų.

Toliau baigiamajame darbe bus aptarta romantinio bei investicijų sukčiavimo aukų charakteristika bei sukčiavimais elektroninėje patiriamos pasekmės aukai.

A. K. Archer JAV 2017 metais atliktame tyrime už 2014-2016 metus apklausė 82 nukentėjusiuosius nuo *romantinio sukčiavimo*. Auka sutiko papasakoti istoriją, kaip prasidėjo jos pažintis su romantiniais sukčiais elektroninėje erdvėje[151]:

1. „Jis mane surado per *Linkedin* platformą ir atsiuntė trumpąją žinutę, nes nori su manim susipažinti bei tapti daugiau nei draugais... Man prireikė kelių dienų, kad aš jam atrašyčiau, kadangi nenumaniau, ar tai nėra kažkokia apgaulė. Taigi, kai pamačiau žinutę nuo gražaus, išvaizdaus 55 metų vyriausiojo inžinieriaus, aš pasijaučiau labai svarbi.“ (Nukentėjusioji moteris, amžius nežinomas)

Taigi, šiuo atveju, sukčius per apgaulingą anketą su auka susisiekė pirmasis per *Linkedin* platformą. Sukčius naudojo gražaus, išvaizdaus vyro nuotrauką ir moteris matydama žinutę nuo išvaizdaus vyro pasijautė pamaloninta, labai svarbi, neva, pilna moterų *Linkedin* ir be jos, o 55 metų vyriškis pasirinko būtent ją. Taip auka gali pradėti idealizuoti sukčių bei bendrauti su juo.

Romantiniai sukčiai anot A. K. Archer naudoja dramatiškas istorijas, tam, kad sujaudintų aukas:

1. „Jis pasakė, jog persikraustė iš Maklyno, Virdžinijos, turėjo žmoną, kuri žuvo autoįvykyje prieš ketverius metus su jų 7 metų dukrele Reičele ir neseniai persikraustė į Pietinę Kaliforniją.“ (Nukentėjusioji moteris, amžius nežinomas)
2. „Jis pasakė, jog yra statybos inžinierius, dirbantis pas Arabų rangovus Naujajame Orleane. Jis pasiėmė savo 6 metų sūnų su savimi į Kombodžą, bet jo sūnus mirė nuo apendicito komplikacijų.“ (Nukentėjusioji moteris, amžius nežinomas)

Panašiose istorijose sukčiai naudoja dramatiškus gyvenimo įvykius – artimųjų mirtys, neįgalumai ir kt. Visa tai gali sušvelninti aukos širdį bendraujant su sukčiu, neva aukos mylimajam gyvenime nutiko skaudūs įvykiai ir auka jo gailės.

Kitos aukos pasidalino savo pasakojimu, kaip jos buvo apgautos romantinių sukčių ir iš jų buvo išvilioti pinigai:

1. „Jis keliavo iš Irano į Kalgarį per Dalaso fortą. Su savimi jis pasiėmė savo įrangą, muitinė Dalaso forte jį sulaikė ir pranešė, jog tai, ką jis gabena yra kontrabanda ir jeigu jis nori išvykti į Kalgarį, turintis muitininkams susimokėti. Man buvo suteikta Kanados banko sąskaita, kur reikia

[151] Aaron K. Archer, „I Made a Choice: Exploring the Persuasion Tactics Used by Online Romance Scammers in Light of Cialdini's Compliance Principles“ (2017). *All Regis University Theses*: 15-20. https://epublications.regis.edu/theses/823.

pervesti pinigus, neva Dalaso forto muitinės pareigūnai turėjo draugų Kanados muitinėje. Kai jis nuvyko į Kalgarį, buvo vėl sulaikytas. Jam vėl reikėjo pinigų. Kai aš vėl sumokėjau, po dienos ar dviejų jis su manim susisiekė ir pasakė, jog jį deportavo iš Kalgario, nes sumokėtų pinigų buvo per mažai.“ (Nukentėjusioji moteris, amžius nežinomas)

2. „Jis pasakė, jog kai jis išėjo iš armijos, armija jam nesumokėjo ir jis neturįs lėktuvo bilietui atgal. Po to prasidėjo krizė. Jis turėjo sumokėti 5 000 JAV dolerių armijai, kad galėtų išvykti iš šalies. Jis pasakė, jog jo draugas gali pervesti reikiamą sumą į mano banko sąskaitą ir po to pinigus pervesčiau jam, o už pagalbą pasilikčiau 300 JAV dolerių.“ (Nukentėjusioji moteris, amžius nežinomas)

Pirmasis atvejis yra tipinis romantinio sukčiavimo modelis, kai aukai sutikus pervesti pinigus savo „mylimajam“, jis sugalvoja naują priežastį, dėl ko jam vėl reikalingi pinigai ir auka nenorėdama prarasti savo „mylimojo“ pasitikėjimo vykdo jo nurodymus. Antruoju atveju aukai greičiausiai siūloma būti pinigų mulu, tačiau kyla abejonės, dėl ko mylimojo draugas negali tiesiogiai jam pervesti pinigų į banko sąskaitą, o į pervedimo grandinę būtinai turi įtraukti auką. Be to tokio dydžio atlygis už pagalbą, manytina, yra neproporcingas teikiamos pagalbos mastui.

Viena iš aukų tyrime pasidalino savo emocine būsena po to, kai ją apgavo romantinis sukčius:

1. „Aš esu nevykėlė. Aš jaučiuosi sužlugdyta, man labai gėda. Po to, kai išsiskyriau su savo buvusiu vyru pagalvojau, jog radau vyrą, su kuriuo praleisiu visą likusį savo gyvenimą. Aš patikėjau viskuo, ką jis man sakė. Aš galėjau bet kada pasakyti ne... Bet aš juo patikėjau. Jis manim pasinaudojo – dabar tą suprantu. Jis išdavė mane vienu skaudžiausiu būdu. Policijos pareigūnai bei psichologai sakė, jog tai nėra mano kaltė... Bet, ką kita kaltinti, jei ne mane? Aš leidau tam įvykti. Niekas manęs nevertė. Aš priėmiau sprendimą, atsižvelgiant į tai, ką jis man sakė. Nepaisant to, jog aš toliau eisiu į terapijos užsiėmimus, tačiau tai neatims mano gėdos, mano kaltės, jog nepasakiau jam „ne“. Jie sako, jog laikas gydo visas žaizdas ir aš su tuo sutinku. Man reikės kelių metų, tam, jog sugrąžinčiau savo finansus į pradinę padėtį. Bet kiek prireiks laiko tam, jog užgytų mano sudaužyta širdis?“ (Nukentėjusioji moteris, amžius nežinomas)

M. T. Whitty kartu su T. Buchanan interviu būdu apklausė 20 nukentėjusiųjų 2016 m. nuo *romantinio sukčiavimo* Jungtinėje Karalystėje. Respondentai buvo parinkti gavus sutikimą iš Jungtinės Karalystės teisėsaugos institucijų bei pačios autorės atliktos apklausos duomenimis[152]. M. T. Whitty apklausos rezultatus padalino į 7 kategorijas[153]:

1. **„Emocinė/psichologinė būsena po romantinio sukčiavimo“**. Visi apklaustieji, neatsižvelgiant į tai, ar jie patyrė turtinę/neturtinę žalą buvo neigiamai paveikti romantinio

[152] Whitty ir Buchanan, *supra note*, 43: 179.
[153] *Ibid*, 180-188.

sukčiavimo. Jie patyrė emocinius išgyvenimus – gėdos jausmą, sumišimą, šoką, pyktį, susirūpinimą ir stresą (ypač tie, kurie buvo įtraukti į pinigų plovimą ar padėjo nusikaltėliams įgyti vizą), baimę ir pyktį dėl to, jog buvo *psichiškai išprievartauti*.

2. **„Kiti asmenys nukentėjusiųjų gyvenime“**. Svarbūs asmenys romantinio sukčiavimo aukai, pavyzdžiui nukentėjusiojo šeima, draugai, bendradarbiai dažniausiai nesuteikė socialinės paramos. Aukos teigia, jog kiti asmenys galvojo, jog jos yra kvailos, jie buvo pikti ar nusivylę dėl to, jog aukos patyrė turtinę žalą (iššvaistė jų palikimą) ir dėl to nesuteikė jokios socialinės paramos. Didžioji dalis respondentų dėl galimo neigiamo požiūrio į juos apie tai, jog buvo apgauti nepranešė niekam išskyrus teisėsaugos institucijų pareigūnus bei apklausos atlikėją.
3. **„Aukos pasikeitimas ir socialinė situacija“**. Aukos patvirtino, jog jų elgesys pasikeitė. Tai buvo neigiamo pobūdžio pasikeitimas. Kai kuriems šis pasikeitimas sumažino pasitikėjimą kitais žmonėmis. Taip pat aukos sumažino bendravimą su savo draugais, aplinkiniais asmenimis. Viena iš aukų visiškai nutraukė bendravimą su savo geru draugu, kuris gyveno netoliese, kadangi draugas bandė auką sudrausminti ir sakė, jog ją bando apgauti. Kai auka suprato, jog tai yra romantinė apgaulė, jai buvo labai gėda ir nejauku pasakyti apie tai draugei.
4. **„Prarastų romantinių santykių problema“**. Skirtingai nuo kitų sukčiavimo modelių, romantinio sukčiavimo metu aukos ne tik praranda turtą (pinigus, parduoda ar užstato savo nekilnojamąjį turtą ir kt.) bet ir praranda savo virtualų „mylimąjį (-ą)“. Daugelis respondentų (įskaitant ir tuos, kurie neprarado jokių pinigų) suprato, jog „mylimojo (-sios)“ praradimas yra sukrečiantis. Kai kuriems respondentams „mylimojo (-sios“ praradimas buvo daug skausmingesnis nei turtas, kuris iš jų buvo išviliotas apgaule. Vienas iš respondentų (nukentėjusiajam heteroseksualiam vyrui policijos pareigūnai pasakė, jog jis bendravo su vyru nusikaltėliu), interviu metu:
    - *Apklausos atlikėja*: Ar tu nors kiek pasiilgsti savo virtualių santykių?
    - *Auka (Paulas)*: Taip
    - *Apklausos atlikėja*: Net kai tu supratai, jog tavo mylimasis buvo vyras?
    - *Auka (Paulas)*: Taip
    - *Apklausos atlikėja*: Prašau, papasakok plačiau, kaip tu jauteisi.
    - *Auka (Paulas)*: Na suprantama, jog aš jaučiausi labai piktas ir nusivylęs, kai supratau, jog visa tai yra apgaulė bet aš iš esmės pasiilgstu to virtualaus žmogaus, su kuriuo aš bendravau.
5. **„Sielvarto stadija“**. Po to, kai aukos suprato, jog jos buvo apgautos romantinio sukčiaus, aukos praėjo „sielvarto stadijas“ – neigimą, derėjimąsį, pyktį, depresiją ir susitaikymą.

Būtent neigimo stadijos metu aukai išliko didžiausia tikimybė patirti pakartotinę viktimizaciją. Kai kurios aukos norėjo derėtis su sukčiais, netgi mokėti pinigus jiems, kad jų sukčiai ir toliau su aukomis bendrautų, netgi žinodami, jog jų santykiai yra netikri.

6. **„Savęs kaltinimas“**. Didžioji dalis respondentų kaltino save dėl to, jog jas apgavo.

- *Auka (Džeinė)*: Galų gale kaltinu save, dėl to, kas įvyko.
- *Apklausos atlikėja*: Kodėl tu kaltini save?
- *Auka (Džeinė)*: Aš tiesiog taip darau. Aš galvoju, jog visos mano dukterys gali pasakyti, kaip tu galėjai pervesti visas savo santaupas kažkam, ko tu net nebuvai mačiusi realybėje, kai už tuos pinigus aš galėjau kiekvienai iš dukterų nupirkti po namą.

7. **„Susitaikymas su apgaule“**. Visi respondentai bandė susitaikyti su tuo, jog juos sukčiai apgavo, bet tik daliai iš tikrųjų pavyko viską pamiršti. Kai kurių aukų aplinkiniai buvo iš dalies geranoriški ir aukoms padėjo, bet pagrinde aplinkiniai buvo neigiamo požiūrio į aukas. M. T. Whitty apklaustajai Marinai labiausiai pavyko susitaikyti su apgaule. Nepaisant to, jog Marina mąstė apie savižudybę, jos mąstymas pasikeitė po to, kai ji papasakojo apie apgaulę savo vaikams. Nors ne visi jos vaikai buvo palaikantys, tačiau keletas buvo. Marinos vaikai padėjo mamai atskirti nusikaltėlį nuo išgalvotos asmenybės (mylimojo):

Auka (Marina): Ir galų gale Douglas, jauniausias sūnus dvynys nusprendė man padėti. Jo brolis, gyvenantis Glazge (Škotijoje) mane nusivežė į banką ir viską taip sutvarkė, kad aš dabar jam esu skolinga. Vyriausiasis sūnus, kuris gyvena Šiaurės Afrikoje man pasakė, mama – tu idiotė. Jis su manim negyvena. Jis nieko nesupranta. Ir mano vaikai man sakė: mama, kiekvieną kartą, kai apie jį pagalvosi, įsivaizduok, kad jis yra apkūnus juodaodis... Ir taip man pavyko užmiršti virtualų mylimąjį, kuris net neegzistavo...

8. **„Ateities požiūris į romantinius santykius“.** Kai kurie respondentai po apgaulės nusprendė išsiregistruoti iš elektroninėje erdvėje veikiančių pažinčių svetainių, kai kiti iš vis atsisakė bet kokių romantinių santykių ateityje. Dvi aukos nusprendė santykių toliau ieškoti elektroninėje erdvėje. Daugelis respondentų pabrėžė, jog jokie kiti santykiai neprilygs tiems, kuriuos jie susikūrė su nusikaltėliu.

Taigi, aukos romantinio sukčiavimo modelio metu patiria ne tik turtinę žalą, bet ir psichologinę – negali užmiršti savo virtualių mylimųjų – nusikaltėlių. Tačiau šie nusikaltėliai galimai vienu metu bendrauja su keliomis aukomis ir jokių santykių su auka užmegzti nenori. Pastebėtina, jog sukūrus netikrą anketą pažinčių portaluose sukčiai vyrai apsimeta tiek jaunomis merginomis (jei auka yra vyras) tiek sėkmingais našliais karininkais (jei auka yra moteris).

Aukų, nukentėjusių nuo *investicinio sukčiavimo* apklausą telefonu Jungtinėse Amerikos Valstijose 2016 m. atliko M. Deliema ir kiti. Buvo apklausta 214 asmenų, nukentėjusių nuo investicinio sukčiavimo.

32 lentelė. Apklausos, nukentėjusiųjų nuo investicinio sukčiavimo 2016 m. duomenys[154]

(N=214)

Amžius	70,7 m.
Lytis (vyrai proc.)	80,8 proc.
Rasė/tautybė	
Baltaodis (ne Ispanas)	89 proc.
Ispanas	3 proc.
Juodaodis	2 proc.
Kita	6 proc.
Šeimyninė padėtis	
Vedęs/gyvenantis santuokoje nesusituokęs	68,3 proc.
Našlys	15,4 proc.
Išsituokęs/išsiskyręs	8,2 proc.
Niekada nesusituokęs	8,2 proc.
Išsilavinimas	
Vidurinis ar žemesnis	17,3 proc.
Nebaigę kolegijos	18,7 proc.
Aukštasis neuniversitetinis	27,6 proc.
Aukštasis universitetinis	34,6 proc.
Namų ūkio metinės pajamos	
Mažiau nei 24,999 JAV dolerių	8,9 proc.
25,000-49,999 JAV dolerių	12,6 proc.
50,000-74,999 JAV dolerių	14,0 proc.
75,000-124,999 JAV dolerių	19,6 proc.
125,000 ir daugiau JAV dolerių	12,6 proc.
Nėra duomenų	32,2 proc.
Užimtumas	
Dirba pilnu etatu	24,3 proc.
Dirba puse etato	14,5 proc.
Išėjęs į pensiją	52,2 proc.
Bedarbis	1,9 proc.
Kita	2,8 proc.

Kaip matyti lentelėje nr. 32 vidutinis nukentėjusiųjų amžius yra 71 metai, didžioji dalis nukentėjusiųjų nuo investicinio sukčiavimo JAV buvo vyrai, baltaodžiai, vedę, turintys aukštąjį neuniversitetinį bei aukštąjį universitetinį išsilavinimą, šeimos vidutinės pajamos – aukštesnės nei vidutinės ir asmenys išėję į pensiją. M. Deliema ir kt. atlikto tyrimo rezultatais buvo nustatyta jog:

[154] Marguerite Deliema, Doug Shadel ir Karla Pak, „Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors.“ *Journal of Consumer Research* 46, no. 5 (February 2020): 909. doi:10.1093/jcr/ucz020. http://web.a.ebscohost.com/ehost/detail/detail?vid=11&sid=b72d32f9-9e28-4188-be85-98f36cce2937%40sdc-v-sessmgr02&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=141139652&db=bth.

1. Nukentėjusieji investavo į labiau rizikingus finansinius instrumentus, jie pasitikėjo su jais susisiekusiais nežinomais investicijų brokeriais.
2. Aukos norėjo per kuo trumpesnį laikotarpį gauti didelę grąžą ir sutiko investuoti į nereguliuojamus, didesnę finansinę grąžą suteikiančius finansinius instrumentus. Aukos, kurios yra suinteresuotos kuo didesne finansine grąža gali ignoruoti tai, jog tokio dydžio finansinė grąža normaliomis rinkos sąlygomis yra neįmanoma arba galvoti, jog aukoms pateiktas pasiūlymas persveria potencialius nuostolius.
3. Vyrai dažniau yra linkę prisiimti rizikingus sprendimus, nei moterys. Moterų mažesnis pasitikėjimas savo investicijų žiniomis lemia tai, jog jos rizikingų pasiūlymų atsisako dažniau nei vyrai.
4. Vyresni asmenys turi sukaupę didesnį kapitalą, nei jaunimas, todėl į juos dažniau yra nusitaikę investiciniai sukčiai.

Taigi, tipinė investicijų sukčiavimo auka – išėjęs į pensiją vyresnio amžiaus vyras, turintis susitaupęs turto, norintis padidinti savo turimą kapitalą.

Pastebėtina ir tai, jog aukos investicinio sukčiavimo metu būna įrašomos į *„nevykėlių sąrašus*“ (angl. *suckers list*).

Pavyzdžiui, 2014 m. duomenimis 14 tūkst. škotų bei 143 tūkst. britų buvo įrašyti į *„nevykėlių sąrašus“*. Policijos pareigūnų duomenimis į šiuos sąrašus patenka asmenys, iš kurių apgaule jau buvo išviliotos didelės pinigų sumos[155]. *„Nevykėlių sąrašais“* sukčiai elektroninėje erdvėje tarpusavyje dalinasi ir aukoms padidėja rizika patirti pakartotinę viktimizaciją.

Baigiamojo darbo autorius toliau atskleis atvejį, kai į *„nevykėlių sąrašą“* galimai buvo įtraukta Lietuvoje gyvenanti 79 metų investicijų sukčiavimo auka[156]:

Apklausos atlikėjas: Po to sakėte, jog skambino kažkokie teisininkai, kurie sakė, kad išpres šią problemą, kaip čia buvo?

Auka: Tai čia buvo vienas Aleksandr Leonov pirmasis. Tai jau čia triukšmas, kad pinigai dingsta, aš negaliu jų pasiimti, tai matomai triukšmas mūsų firmai ir kitoms. Paskambino iš *whatsapp'o*, jis *whatsapp'e* dirba. Europos Sąjungoje išieško skolas.

Apklausos atlikėjas: Jis pats rado jūsų kontaktus kažkokiu būdu?

Auka: Na taip, internete viskas yra.

Apklausos atlikėjas: Jūsų telefonas yra?

Auka: Taip.

[155] Alan Simpson, „How Scammers Track down Their Victims... Use 'the Suckers List.'"*Daily Mail,* September 6, 2014. http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=97929064&site=ehost-live.
[156] „Senolė pardavė butą ir sukčiam pervedė 36 000 EUR", *supra note,* 12: 24:40 min.

Apklausos atlikėjas: Tas Leonovas, kur skambino pasakė, kad internete rado jūsų kontaktus?

Auka: Aš jo net neklausiau.

Apklausos atlikėjas: Jis paskambino ir sako – sveiki, čia jūs nukentėjote?

Auka: Taip, viską žino, konkrečiai kiek, reiškiasi žmonės domisi ir sekamos firmos, kaip jos dirba. Aš jums galiu padėti susigrąžinti tuos pinigus. Aišku, laikas buvo labai trumpas.

Apklausos atlikėjas: Ką jis pasakė, ką jūs turite padaryti, kad tuos pinigus susigrąžinti?

Auka: Pasirašyti dokumentą, nuskanuoti paso kopiją ir nusiųsti banko išrašą.

Apklausos atlikėjas: Tai nuskanuoti pasą bei banko išrašą ir viskas?

Auka: Taip, dar aš nusiunčiau savo banko sąskaitą, kur pervesti pinigus.

Apklausos atlikėjas: Jūs išsiuntėte jiems viską elektroniniu paštu? Bet tiems „teisininkams“ nemokėjote?

Auka: Ne, daugiau nieko nemokėjau.

Apklausos atlikėjas: O jie prašė apmokėti?

Auka: Ne, aš daugiau nieko jiems nemokėjau.

Taigi, šiuo atveju Lietuvoje gyvenančiai garbaus amžiaus moteriai, kuri investavo į kriptovaliutą bei prarado didžiąją dalį santaupų, neva „nespėjo uždaryti“ sandorio, paskambino „teisininkai“. Jie jau žinojo viską apie pirminę sukčių įmonę, tikslią sumą, kurią prarado nukentėjusioji. Galima teigti, jog galimai aukai skambino pirminių sukčių bendrininkai, siekdami apgaule įgyti daugiau lėšų. Tokiais atvejais aukos dažnai patiria pakartotinę viktimizaciją. Jos patiki sukčių bendrininkų apgaulinga informacija, neva jie gali padėti susigrąžinti apgaule išviliotas lėšas už tam tikrą mokestį. Šis mokestis dažniausiai būna įvardijamas kaip „dokumentų ruošimo“, „advokatų konsultacija“ ir kt. Manytina, jog aukos praradusios didžiąją dalį santaupų yra apimtos nusivylimo, pykčio, kad jų investicija, neva žlugo. Todėl, norėdamos susigrąžinti bent jau pirminę investiciją, sukčių bendrininkams perveda dar daugiau pinigų. Aukai esant įrašytai į *„nevykėlių sąrašą“* po kiek laiko gali skambinti kiti sukčiai ir vėl siūlyti investuoti lėšas į kriptovaliutas ar kitą finansinį instrumentą.

Fišingo atakos, anot tyrimo, atlikto 2016 lapkritį ir 2017 m. gruodį N. Akdemir ir C. J. Lawless[157] pasireiškia, kai asmuo savanoriškai atskleidžia tapatybę identifikuojančią informaciją bei, kai tapatybę atskleidžianti informacija yra įgyjama neteisėtai paveikus kitos informacinės sistemos duomenų bazę. N. Akdemir ir C. J. Lawless. tyrime apklausė 32 respondentus iš

[157] Naci Akdemir ir Christopher James Lawless, „Exploring the Human Factor in Cyber-Enabled and Cyber-Dependent Crime Victimisation: A Lifestyle Routine Activities Approach.“ *Internet Research* 30, no. 6 (November 2020): 1677–88. doi:10.1108/INTR-10-2019-0400. https://www.emerald.com/insight/content/doi/10.1108/INTR-10-2019-0400/full/pdf?title=exploring-the-human-factor-in-cyber-enabled-and-cyber-dependent-crime-victimisation-a-lifestyle-routine-activities-approach.

Jungtinės Karalystės struktūrinės apklausos būdu. Buvo pažymėta, jog dažniausiai *fišingo* atakos, kai asmuo savanoriškai atskleidžia savo tapatybę identifikuojančią informaciją būna įvykdomos pasitelkiant socialinius tinklus, elektroninėje erdvėje veikiančius prekybos tinklalapius bei nemokamus Wifi tinklus:

- „Greičiausiai *fišingo* laišką gavau dėl naudojimosi socialiniais tinklais. Tu kartais paspaudi ant nuorodos... Jie paprašo tavo elektroninio pašto, kad gautum naujienlaiškius. Po kurio laiko sulaukiau apgaulingų laiškų dėl mokesčių grąžinimo“ (Respondentas D)

Elektroninėje erdvėje patalpinus parduodamo daikto skelbimą asmeniui padidėja tikimybė tapti *fišingo atakos* taikiniu. Dėl nurodomų asmenį identifikuojančių duomenų – el. pašto ar telefono numerio, aukos tampa patrauklesnės sukčiams.

- „Aš patalpinau skelbimą, kad parduodu savo seną automobilį portale X. Tik mano telefono numeris ir elektroninio pašto adresas buvo matomi.“ (Respondentas E)

Didžioji dalis respondentų nesusimąstė apie riziką, kai jungdamiesi prie nemokamo Wifi bevielio ryšio atskleidė savo asmens duomenis.

- „Aš kartais naudojuosi nemokamu Wifi oro uoste ar kavinėje. Mano manymu, jie jungiantis prie bevielio tinklo neprašo labai asmeninės informacijos, dėl to aš nebijau atskleisti jos.“ (Respondentas G)

Taigi, šiais trimis atvejais aukos pačios pasirinko tokį elgesio variantą, kuris galimai nulėmė, jų tapimą fišingo atakų aukomis. Jos įtartinuose tinklalapiuose ar jungiantis prie nemokamo Wifi bevielio ryšio atskleidė savo tapatybę identifikuojančią informaciją, kuri vėliau gali būti personalizuota ir panaudota apgaulingiems fišingo laiškams siųsti.

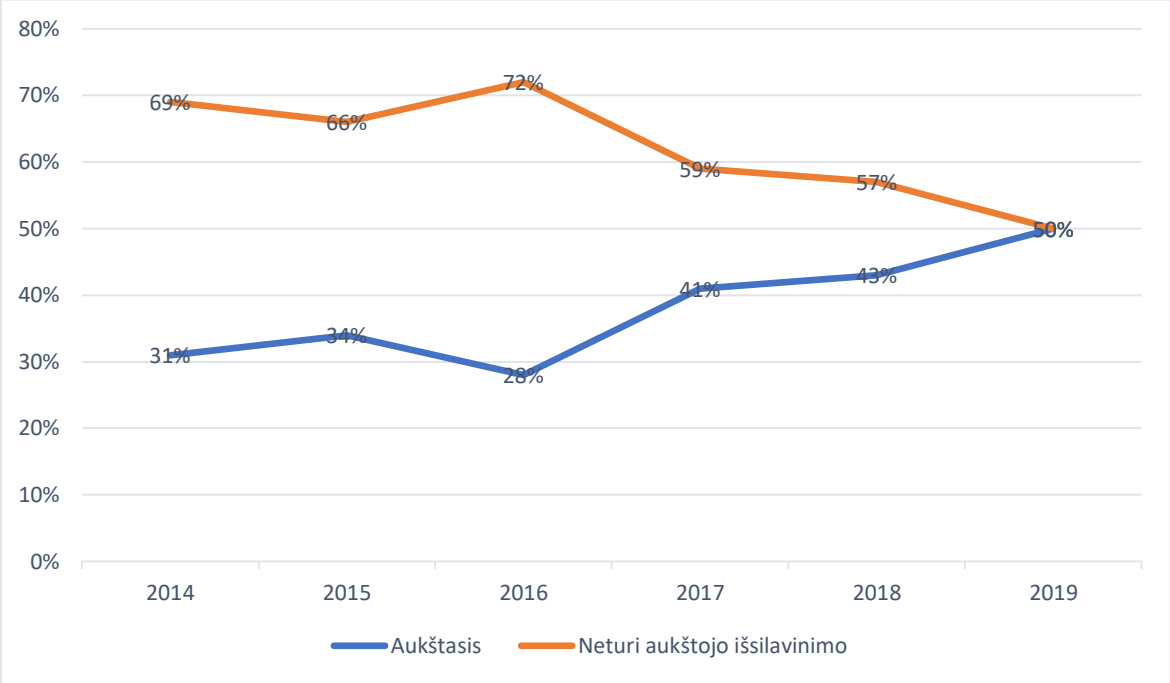
Tapatybę identifikuojančių duomenų įgijimas, kai neteisėtai paveikiama kitos informacinės sistemos duomenų bazė yra nesavanoriškas tapimas fišingo atakų taikiniu. Respondentai sutiko su tuo, jog jie pastebėjo didesnį fišingo atakų mastą, kai neteisėtai buvo paveiktos kitų informacinių sistemų duomenų bazės.

- „Aš gavau daugybę fišingo laiškų, ir jų skaičius ženkliai padidėjo po to, kai buvo neteisėtai paveikta T... elektroninės parduotuvės klientų duomenų bazė. Atrodo, jog mano elektroninio pašto adresą dabar žino visas pasaulis.“ (Respondentas H)
- „Taigi, kai G informacinė duomenų bazė buvo neteisėtai paveikta, kažkodėl ten buvo išsaugoti mano kreditinės kortelės duomenys. Niekada apsiperkant aš nepasirenku, jog kortelės duomenys būtų išsaugoti. Tas G tinklalapis be mano sutikimo išsaugojo kortelės duomenis.“ (Respondentas I)

Taigi, fišingo atakos auka galima tapti net ir saugantis bei bet kur neatskleidžiant savo tapatybę sudarančių duomenų. Asmenų tapatybė sudaranti informacija gali būti pasisavinama neteisėtai paveikus kitos informacinės sistemos duomenų bazę.

Sukčiavimai elektroninėje erdvėje, nukreipti į fizinius asmenis – romantinis bei investicijų sukčiavimas yra panašūs tuo, jog abiejų sukčiavimų modelių atvejais aukos patiria finansinę žalą, jos gali prarasti viso gyvenimo santaupas. Tačiau greta romantinio sukčiavimo aukos patiria psichinę žalą – neapykantą, liūdesį, nusivylimą santykiais. Nukentėję įsimyli virtualų mylimąjį (-ąją) bei būtent psichinė žala aukai gali būti skaudesnė nei apgaule išviliotos viso gyvenimo lėšos. *Fišingo atakų* metu aukos gali savanoriškai atskleisti savo tapatybę identifikuojančią informaciją arba atakų auka tapti po neteisėtos informacinės sistemos poveikio, kurio metu įgyjama konfidenciali klientų informacija.

33 diagrama. Nukentėjusiųjų, nuo užregistruotų sukčiavimų elektroninėje erdvėje Lietuvoje 2014-2019 m. pasiskirstymas pagal išsilavinimą[158]



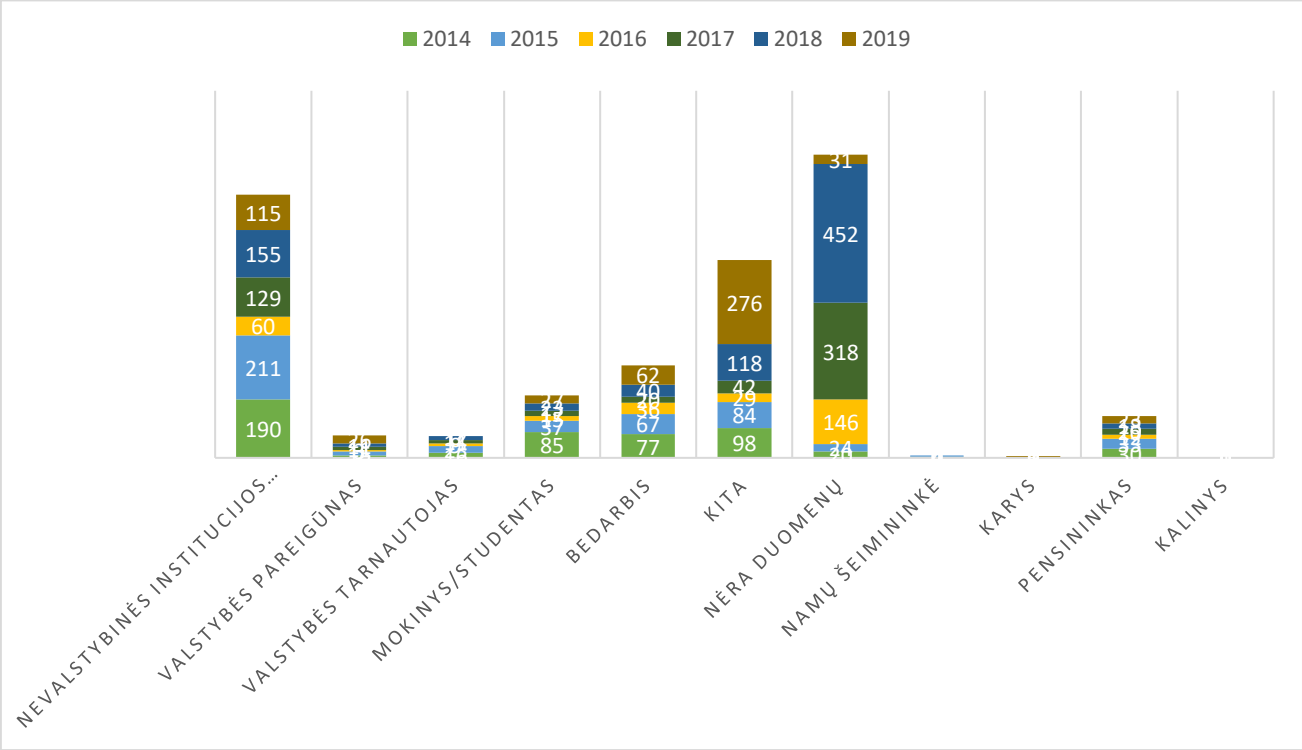
Kaip matyti diagramoje nr. 33 tiriamojo laikotarpio pradžioje 2014 m. nukentėjusieji, neturintys aukštojo išsilavinimo sudarė 69 proc., kai turintys aukštąjį išsilavinimą – 31 proc. Tiriamojo laikotarpio pabaigoje 2019 m. turinčių aukštąjį išsilavinimą ir neturinčių aukštojo išsilavinimo dalis tapo lygi ir sudarė po puse nukentėjusiųjų.

Kaip teigia J. Wentz: „įsilaužėliai tampa vis protingesni, net išsilavinę profesionalai gali tapti internetinio sukčiavimo aukomis.“[159]. Daug kam atrodo, jog elektroninėje erdvėje sukčių aukomis tampa tik mažai technikoje išmanantys asmenys, pavyzdžiui, pensininkai. Išsilavinę

[158] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (50 forma).
[159] Jennifer Wentz, „SCAMMED: As Hackers Get Smarter, Even Educated Professionals Can Fall Victim to Fraud.“ *Central Penn Business Journal* 33, no. 20 (May 12, 2017): 15. http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=123070717&site=ehost-live.

teisininkai, atrodytų, jog netaptų sukčių aukomis. Tačiau dėl sukčių prisitaikymo, jų tobulėjimo elektroninėje erdvėje pensininkus ir, pavyzdžiui, advokatus ar net įmonės vadovus nuo aukos statuso skiria tik vienas žingsnis[160]. Taigi, sukčiai savo aukų nesirenka, ir skirtingai nei nuo fizinės erdvės, sukčiavimui elektroninėje erdvėje būdinga „vienas ir daugelis“ nusikaltimo schema[161]. Sukčiai masiškai aukoms gali išsiųsti apgaulingus elektroninius laiškus. Manytina, jog nuo 2017 m. užregistruotų sukčiavimų elektroninėje erdvėje statistikoje Lietuvoje matomas aukų, neturinčių aukštojo išsilavinimo bei aukų, turinčių aukštąjį išsilavinimą susilyginimas sietinas su tuo, jog sukčiai nusitaikė į turto įgijimą apgaule iš juridinių asmenų ir su jais susijusių darbuotojų – buhalterių, finansininkų, įmonės vadovų. Tai yra asmenų, turinčių aukštąjį išsilavinimą, apgaulė. Beveik visi įmonės darbuotojai tarpusavyje bendrauja elektroniniu paštu ir tik nedaugelis paskambina savo kolegai ar įmonės vadovui, norėdami patikrinti elektroninio laiško tikrumą[162].

34 diagrama. Nukentėjusiųjų, nuo užregistruotų sukčiavimų elektroninėje erdvėje Lietuvoje 2014-2019 m. pasiskirstymas pagal užimtumą[163]



Iš diagramoje nr. 34 pavaizduotų duomenų matyti, jog tiriamojo laikotarpio pradžioje didžioji dalis nukentėjusiųjų dirbo nevalstybinėse institucijose (36 proc.). 22 proc. atvejų

[160] *Ibid*, 16.
[161] Sakalauskas ir kt., *supra note*, 137: 173.
[162] Wentz, *supra note*, 159: 16.
[163] Sudaryta baigiamojo darbo autoriaus naudojant Microsoft Excel programą. Duomenys gauti iš NŽVR registro (*50 forma*).

informacija apie aukas buvo nežinoma arba kita. Valstybės tarnautojai bei valstybės pareigūnai, kaip dirbantys asmenys, sudarė 4 proc. Pastebėtina, kad viso tiriamojo laikotarpio metu policijos pareigūnai nukentėjo nuo sukčių 11 kartų iš kurių, 2014 metais - 2 kartus, 2015 metais – 2 kartus, 2016 – 2 kartus, 2017 – 2 kartus, 2018 – 1 kartą ir tiriamojo laikotarpio pabaigoje – 2 kartus. Visi nukentėję policijos pareigūnai buvo su aukštuoju išsilavinimu. 2015 metais fiksuotas vienas atvejis, kai sukčių elektroninėje erdvėje auka tapo FNTT pareigūnė. Manytina, jog FNTT pareigūnai, specializuojantys finansinių nusikaltimų tyrime galėtų suprasti, jog su jais susisiekia sukčius. Taigi, nors ir pareigūnų misija yra „ginti, saugoti, padėti“, tačiau fiksuota atvejų, kai jie patys tapo sukčių elektroninėje erdvėje aukomis. 2015 metais pastebėtinas išaugęs dirbančių nevalstybinėse institucijose aukų skaičius (42 proc.). Didžioji dalis užregistruoto sukčiavimo elektroninėje erdvėje statistinių duomenų atvaizduojama po žymomis „kita“ bei „nėra duomenų“. Manytina, jog pareigūnams, kurie priima pareiškimus, dėl didelio darbo krūvio statistinėse kortelėse kartais lengviau pažymėti „kitą“ užimtumą ar tiesiog jo nežymėti. Bedarbiai, pensininkai ir namų šeimininkės tiriamojo laikotarpio pradžioje 2014 m. sudarė 21 proc. visų aukų, o tiriamojo laikotarpio pabaigoje 2019 m. – 15 proc. iš visų aukų. Tiriamojo laikotarpio pabaigoje matomas beveik dvigubas dirbančių nevalstybinėse institucijoje aukų mažėjimas – nuo 36 proc. tiriamojo laikotarpio pradžioje iki 20 proc. tiriamojo laikotarpio pabaigoje. Taigi, nors ir matomas dirbančių aukų mažėjimas, tačiau galimai toks pokytis yra dėl neteisingo statistinių kortelių duomenų pildymo.

Viso tiriamojo laikotarpio metu, didžiausia dalis aukų dirbo. Galima teigti, jog dirbantys asmenys gali turėti daugiau lėšų savo banko sąskaitose, kurias sukčiai gali pasikėsinti įgyti apgaule. Taip pat dirbantys asmenys po darbo dienos gali neatkreipti dėmesio į pasikeitusią nuorodą el. pašte ar trumpojoje SMS žinutėje (*fišingo*/*smišingo* ataka). Darytina išvada, jog iš tiriamojo laikotarpio pateiktų duomenų sukčiai elektroninėje erdvėje dažniau apgauna ir apgaule įgyja lėšas iš dirbančių asmenų.

C. Cross ir kt.[164] Australijoje atliko struktūrizuotą apklausą gyvai ir apklausė 80 nukentėjusiųjų nuo sukčiavimo elektroninėje erdvėje nuo 2011 iki 2014 metų, kurie sukčiavimo elektroninėje erdvėje metu prarado daugiau nei 10 tūkst. Australijos dolerių. Respondentų amžius svyravo nuo 30 iki 77 metų. 46 respondentai buvo vyrai ir 34 respondentai – moterys. Apie trečdalis nukentėjusiųjų nukentėjo nuo romantinio sukčiavimo, trečdalis – investicinio ir likusi dalis – nuo „Nigerijos“ sukčiavimo.

[164] Cassandra Cross, Kelly Richards ir Russell G. Smith, „The Reporting Experiences and Support Needs of Victims of Online Fraud.“ *Trends & Issues in Crime & Criminal Justice*, no. 518 (August 2016): 3-4. doi:10.1177/1748895815603773, https://www.aic.gov.au/sites/default/files/2020-05/tandi518.pdf.

Tyrimo metu buvo išsiaiškinta, jog finansinis sukčiavimo poveikis aukoms priklauso nuo to, kiek pinigų jie prarado, dabartinės turtinės padėties, ir turimų resursų, siekiant susigrąžinti savo *status quo*. Kai kuriems iš respondentų finansinis sukčiavimo poveikis buvo minimalus:

- „Na, mes ilgimės pinigų, bet sukčiavimas mūsų nenugalėjo.“ (Respondentas nr. 8)
- „Buvo nepatogumų, tačiau tai nebuvo kažkas tokio, kad aš pagalvojau, Dieve mano! Aš buvau apgautas, praradau savo gyvenimo santaupas, dabar einu nusižudyti.“ (Respondentas nr. 15)
- „Tai buvo pinigai, kuriuos mes galėjome sau leisti prarasti.“ (Respondentas nr. 69)

Kai kurios sukčiavimo elektroninėje erdvėje aukos labai sumenkino sukčiavimo faktą arba išvis jį neigė:

- „Aš nieko nepraradau. Man viskas gerai. Aš esu čia. Vis dar turime savo namus bei savo automobilius. Visus tuos dalykus.“ (Respondentas nr. 65)

Kitos aukos pajuto poveikį savo laisvalaikio malonumams:

- „Buvo stiprus diržų susiveržimas... privalėjome pakeisti savo laisvalaikio praleidimo būdus. Atidėjome visas savo atostogas keleriems metams.“ (Respondentas nr. 26)

Deja, bet kai kurios sukčiavimo elektroninėje erdvėje aukos patyrė didelį ir stiprų finansinį poveikį. Kai kurie respondentai neteko savo sukauptų senatvės pensijų, turi grąžinti dideles paskolas, prarado viską, visas savo santaupas, negalėjo nusipirkti net maisto, išleido daug pinigų advokatams ir teisininkams, pateikdami civilinius ieškinius prieš sukčius. Didžioji dalis respondentų netgi skolinosi pinigų pas savo draugus, gimines, taip pat minėtini atvejai, kai aukos pardavė ar įkeitė savo kilnojamąjį ir nekilnojamąjį turtą. Sukčių elektroninėje erdvėje aukos liko be nieko:

- „Šiuo metu aš dirbu. Man sukaks 65 metai šį šeštadienį.“ (Respondentas nr. 16)
- „Aš turėjau apsigyventi globos įstaigoje, vaikai buvo tuo nepatenkinti. Man yra apribotas laikas, kiek aš galiu juos matyti.“ (Respondentas nr. 17)
- „Dėl to, kad patekau į didžiulę finansinę bėdą, dabar negaliu gauti paskolos. Aš negaliu gauti paskolos ir niekada neturėsiu savo būsto net ir dirbant pilnu etatu.“ (Respondentas nr. 32)

Darytina išvada, jog sukčiai elektroninėje erdvėje aukų nesirenka. Jiems nesvarbu, ar auka yra jaunas ar senas žmogus. Sukčiai apgavę žmones iš jų stengiasi įgyti kuo daugiau lėšų apgaule. Kai kurios aukos patikėjusios apgaulingomis žiniomis praranda visas savo santaupas ir netgi parduoda namus.

Sukčiavimų elektroninėje erdvėje, nukreiptų į *juridinius asmenis* aukos visų pirma patiria turtinę žalą. Juridinio asmens turtinės žalos dydis priklauso nuo pačio juridinio asmens dydžio. Didelės korporacijos, valdydamos didžiulius pinigų srautus, gali būti pažeidžiamos ir patirti

didelių nuostolių[165]. Tačiau, kaip pažymi C. Cassandra, ne visada prarasti pinigai įmones paveikia vienodai[166]. Kai kurioms vidutinėms-mažoms korporacijoms net ir kelių tūkstančių eurų turtinė žala gali turėti didžiulį poveikį. Ne visos didelės korporacijos, nukentėjusios nuo verslo partnerio banko sąskaitos keitimo sukčiavimo toliau veikia rinkoje.

Pavyzdžiui, vienas iš veiksnių, kodėl JAV *Diesel* korporacija, gaminusi *Diesel* džinsus inicijavo juridinio asmens bankroto procedūrą, buvo elektroninėje erdvėje veikiančių sukčių apgaule įgytas 1,2 mln. JAV dolerių[167].

Taip pat JAV kompanija *Tillage Commodities* sukčiams, apsimetusiems Hong Konge registruotiems verslo partneriams pervedė 5,4 mln. JAV dolerių, kas sudarė jos 64% įstatinio kapitalo[168].

Juridiniai asmenys, tapę verslo partnerio banko sąskaitos keitimo aukomis taip pat rizikuoja būti patraukti atsakomybėn už duomenų apsaugos reglamento pažeidimus. Privati informacija apie klientus, sandorius, kuri gali būti rasta atakos metu gali vėliau būti panaudojama šią informaciją realizuojant juodojoje rinkoje[169].

Anot R. Smith, didžioji dalis sukčiavimo veikų nėra pranešamos policijai[170]. Manytina, jog nuo sukčių elektroninėje erdvėje nukentėję juridiniai asmenys dėl didesnio latentiškumo sudaro nedidelę dalį aukų lyginant su fiziniais asmenimis. Korporacijos, tapusios sukčių aukomis (verslo partnerio banko sąskaitos keitimo ar apsimetimo įmonės vadovu sukčiavimo modeliais) gali nepranešti teisėsaugoms institucijoms apie patirtą turtinę žalą dėl reputacijos, neigiamo požiūrio į jas poveikio. Neabejotinai, juridiniam asmeniui pranešus, kad jis tapo auka apie tai gali parašyti žiniasklaidos atstovai. Tai gali lemti juridinio asmens akcijų kainos kritimą, neigiamą visuomenės požiūrį, neva, juridinis asmuo neturi pakankamai priemonių, kad apsaugotų savo turtinius interesus. Galų gale juridinio asmens būsimi akcininkai gali nebenorėti investuoti į tokią įmonę, kurią sąlyginai lengva apgauti ir išvilioti iš jos lėšas.

Apibendrinant, aukos, fiziniai asmenys, nukentėję nuo sukčiavimo elektroninėje erdvėje gali patirti ne tik turtinę žalą, bet ir psichologinę žalą. Juridiniai asmenys gali nepranešti teisėsaugoms institucijoms apie patirtą žalą dėl savo reputacijos, akcijų vertės mažėjimo.

---

[165] Cassandra Cross ir Rosalie Gillett, „Exploiting Trust for Financial Gain: An Overview of Business Email Compromise (BEC) Fraud.“ *Journal of Financial Crime* 27, no. 3 (July 2020): 875. doi:10.1108/JFC-02-2020-0026, https://eprints.qut.edu.au/200621/1/BEC_fraud_CROSS_GILLETT_submit.pdf.

[166] *Ibid*, 875.

[167] Tiffany Kary ir Anne Riley Moffat, „Jeans Brand Diesel USA Files for Bankruptcy as Turnaround Lags.“ *Bloomberg.Com*, March 5, 2019, N.PAG. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=140631142&site=ehost-live.

[168] Kate Fazzini, „CFTC Settlement Shows New Era of Third Party Cyberrisk.“ *Wsj.com*, October 4, 2017. https://www.wsj.com/articles/cftc-settlement-shows-new-era-of-third-party-cyberrisk-1507151448.

[169] Cross ir Gillett, *supra note*, 166*:* 875.

[170] Russell Smith, „Coordinating Individual and Organisational Responses to Fraud.“ *Crime, Law & Social Change* 49, no. 5 (June 2008): 380. doi:10.1007/s10611-008-9112-x, https://link.springer.com/article/10.1007/s10611-008-9112-x.

5. SUKČIAVIMŲ ELEKTRONINĖJE ERDVĖJE VEIKSNIAI

Niekas negimė būdamas sukčiu, tik situacija ir aplinka motyvuoja asmenį nusikalsti[171]. Anot J. Galinaitytės: „nusikalstamumo priežastimis (jų visuma) laikytini tokie visuomenės gyvenimo reiškiniai, procesai, kurie sąveikaudami su sąlygomis, determinuoja nusikalstamumo, kaip socialinio teisinio reiškinio kilmę ir raidą, veikia jo kaitą.“[172]. A. Petkus teigia, jog: „labiausiai paplitusių Lietuvoje turtinio pobūdžio nusikalstamų veikų priežastingumui įtakos turi ir bendri veiksniai, veikiantys visus žmones, ir specifiškesni veiksniai, veikiantys turtinius nusikaltimus pasiekiamas, t.y. gaunamas pelnas, tačiau kalbant apie profesionalus atkreiptinas dėmesys į jų labai aukšto lygio pasirengimą, „kvalifikaciją““[173]. Sukčiavimas elektroninėje erdvėje, atskirai LR BK neišskiriamas, todėl jį galima priskirti prie turtinio pobūdžio nusikaltimų. Veiksnius, turinčius įtakos turtinio pobūdžio nusikalstamoms veikoms galima išskirti į šias grupes:

1. Socialiniai ekonominiai - didėjanti visuomenės diferenciacija pagal gaunamas pajamas, kuri didina socialinę įtampą; Skurdas; Mokesčių politikos netobulumas; Nedarbas tarp asmenų, paleistų iš laisvės atėmimo vietų; Neužimtumas; Išsimokslinimo stoka; Žmonių mobilumas; Saviugda vertybinių orientacijų, poreikių sistemoje; Valstybės nepajėgumas užtikrinti socialinį-ekonominį teisingumą; Materialinių poreikių išaukštinimas prieš realias galimybes; Valstybės nepajėgumas padėti socialiai remtiniems asmenims.

2. Politiniai. Šiems veiksniams priklauso: Politinis nestabilumas, kuris sąlygoja socialinį, ekonominį ir teisinį nestabilumą; Baudžiamosios politikos nestabilumas; baudžiamosios ir bausmių vykdymo politikos neefektyvumas; Pataisos įstaigų reformos nepakankamumas; Visuomenės pasyvumas, nusikaltėlių palaikymas; Korupcija.

3. Teisiniai. Šiems veiksniams priklauso: Įstatymų ir kitų teisės aktų kaita bei netobulumas; Oficialaus autentiškojo teisės aiškinimo trūkumas;

4. Socialiniai psichologiniai. Šiems veiksniams priklauso: Dorovinė-moralinė krizė; Visuomenės ir baudžiamojo teisingumo sistemos solidarumo trūkumas; Didelis turtinių nusikalstamų veikų latentiškumas ir „sėkminga neigiama“ patirtis,

5. Techninio pobūdžio. Šiems veiksniams priklauso: Tyrimo neaprūpinimas techninėmis priemonėmis; Nusikaltimus darančių asmenų apsirūpinimas techninėmis priemonėmis; Bendruomenės narių per mažai naudojamos techninės apsaugos priemonės; Turtinius nusikaltimus įtakoja ir miestų architektūra[174].

---

[171] Shivam Kakati ir Chandana Goswami, „Factors and Motivation of Fraud in the Corporate Sector: A Literature Review.“ *Journal of Commerce & Accounting Research* 8, no. 3 (July 2019): 86. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=bth&AN=138408217&site=ehost-live.
[172] Babachinaitė ir kt., *supra note*, 25: 170.
[173] *Ibid*, 454.
[174] *Ibid*, 454-460.

Aukščiau įvardinti veiksniai priskiriami prie bendrojo turtinio pobūdžio nusikaltimų, tačiau, manytina, jog visi tinka ir sukčiavimui elektroninėje erdvėje. Baigiamojo darbo autoriaus nuomone sukčiavimus elektroninėje erdvėje gali įtakoti ir techninio pobūdžio veiksniai. Sukčiavimus elektroninėje erdvėje darantys asmenys nusikalstamas veikas daro specifinėje erdvėje – elektroninėje erdvėje. Šioje erdvėje nusikaltėlis ir auka sąveikauja nuotoliniu būdu, vienas kito nematydami. Sukčius vienu metu apgaule pasikėsinti įgyti aukų lėšas gali iš nenustatyto skaičiaus aukų. Pavyzdžiui, fišingo laiškais ar smišingo žinutėmis nusikaltėliai naudodami technines priemones siunčia neindividualizuoto teksto laiškus ar sms žinutes aukoms. Apgaulingo pobūdžio laiškai ar sms žinutės vienu metu gali pasiekti tūkstančius gavėjų bei aukos gali prarasti savo tapatybę identifikuojančius duomenis, kurie vėliau gali būti panaudoti neteisėtai įgyjant lėšas.

Sukčiavimus fizinėje erdvėje padarantys nusikaltėliai lėšas neteisėtai įgyja grynųjų pinigų forma. Kitas techninio pobūdžio veiksnys, manytina, yra aukos->nusikaltėlio lėšų pervedimo kelias. Siekiant išlaikyti anonimiškumą ir sumažinti veikos atskleidimo riziką sukčiai gali pasirinkti decentralizuotas valiutas. Kaip teigiama 2016 m. IOCTA apžvalgoje nusikaltėliai pirkdami prekę ar paslaugą iš kitų nusikaltėlių elektroninėje erdvėje siekia išlaikyti anonimiškumą. „Juodojo interneto“ (angl. *darknet*) parduotuvėse yra integruota *Bitcoin* kriptovaliutų sistema. Šią sistemą dažnai naudoja ir sukčiai, kai elektroninėje erdvėje neteisėtai įgyja aukų lėšas[175].

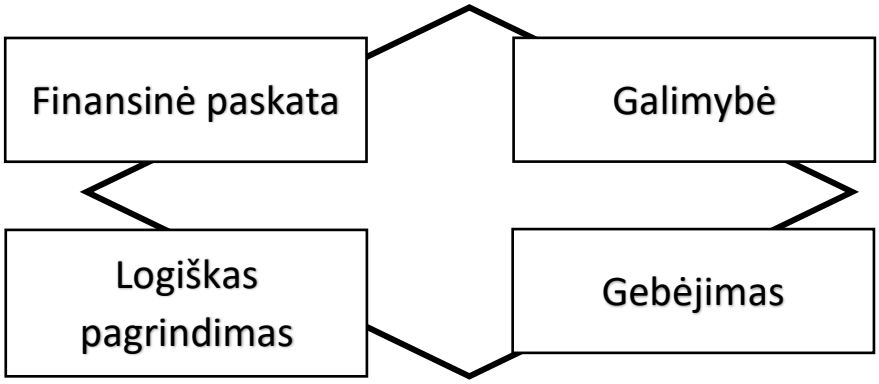
2020 m. liepos 16 d. Lietuvos Respublikos Valstybės kontrolės audito ataskaitos duomenimis: „Mokymų (nusikaltimų elektroninėje erdvėje – *aut. pastaba*) organizuojama nepakankamai. 70 proc. apklausoje dalyvavusių nusikaltimų elektroninėje erdvėje (toliau ir – NEE) specializuotų pareigūnų ir prokurorų nurodė, kad mokymų NEE srityje nepakanka. Atlikus Kriminalinės žvalgybos mokymo centro mokymų dalyvių sąrašų analizę nustatyta, kad 2015–2019 m. 30 proc. specializuotų pareigūnų nė karto juose nedalyvavo, kiti tik fragmentiškai, nes mokymų organizuojama nepakankamai. Pažymėtina, kad šiuose mokymuose nedalyvavo 36 proc. pareigūnų, kurie pradėjo specializuotis (NEE tyrime – *aut. pastaba*) 2019 m. Prokurorų (NEE – *aut. pastaba*) mokymai 2015–2019 m. vyko kasmet, bet 61 proc. apklausoje dalyvavusių specializuotų prokurorų juose dalyvavo fragmentiškai.“[176]. Taigi sukčiavimui elektroninėje erdvėje būdingas pasiruošimas, anoniminių nusikaltėlio tapatybę apsaugančių priemonių naudojimas. Iš ataskaitos matyti, jog 70 proc. pareigūnų mano, jog mokymų nepakanka. Magistro baigiamojo darbo autoriaus nuomone, sukčiavimai elektroninėje erdvėje prisitaiko prie socialinėje erdvėje vykstančių reiškinių ir sistemiški pareigūnų mokymai yra reikalingi. Sukčiai galimai

[175] „The internet organised crime threat assesment (IOCTA) 2016“, IOCTA, žiūrėta 2020 m. spalio 24 d., https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 p. 42.
[176] Valstybinio audito ataskaita, *supra note*, 13: 52.

naudojasi sukčiavimus elektroninėje erdvėje tiriančių pareigūnų neaprūpinimu reikiama įranga ir mokymais.

Sukčiavimo, kaip nusikalstamos veikos priežastingumą mokslininkai išskiria į keturis veiksnius, sudarančius „sukčiavimo deimantą“:

35 paveikslas. „Sukčiavimo deimantas“[177]



- Pirmasis sukčiavimo veiksnys įvardijamas kaip finansinė paskata. Aš noriu, arba man reikia padaryti sukčiavimą.
- Galimybė. Atsiradus sistemos ar žmogaus pažeidžiamumui, sukčius tuo gali pasinaudoti.
- Logiškas pagrindimas. Aš save įtikinau, kad nesąžiningas elgesys vertas rizikos.
- Gebėjimas. Aš turiu reikiamus įgūdžius, tam, kad neteisėtai įgyčiau kito asmens turtą. Aš viską apgalvojau ir galiu tai įgyvendinti.[178]

Taigi, nors šis „sukčiavimo deimantas“ yra sukurtas įprastam sukčiavimui fizinėje erdvėje, galima jį pritaikyti ir sukčiavimui elektroninėje erdvėje. Manytina, jog vienas iš pagrindinių sukčiavimo elektroninėje erdvėje požymių yra gauti finansinės naudos, kurios ir siekia sukčiai. Antrasis požymis, sietinas su galimybe apgaulingai pranešus informaciją ar kitus faktus įgyti žmogaus pasitikėjimą ir jį apgauti. Trečiasis požymis, manytina, jog siejamas su „savęs pateisinimu“, kuomet sukčiai iš mažiau išsivysčiusių valstybių, pavyzdžiui, Nigerijos, kurioje minimalus atlyginimas siekia 30 tūkst. Nigerijos nairų arba 75 eurus[179], gali nuotoliniu būdu apgauti auką iš Vokietijos ir save teisinti, jog jis mažai uždirba ir 200 eurų Vokietijos piliečiui galimai nėra didelė suma, tačiau nusikaltėliui iš Nigerijos yra 2,5 mėn. atlyginimas. Paskutinis požymis sietinas su gebėjimu. Šis požymis aiškintinas per techninius veiksnius, kuomet sukčiams elektroninėje erdvėje norint sėkmingai įgyvendinti ataką ir apgaule įgyti žmonių lėšas būtina

[177] Rasha Kassem ir Andrew Higson, „The New Fraud Triangle Model (June 1, 2012). Journal of Emerging Trends in Economics and Management Sciences (JETEMS)“, Vol. 3, No. 3, (ISSN: 2141-7024), 2012: 194, https://www.researchgate.net/publication/256029158_The_New_Fraud_Triangle_Model.

[178] D. Wolfe ir D. Hermanson, „The Fraud Diamond: Considering the Four Elements of Fraud.“, (2004): 2/5, https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=2546&context=facpubs.

[179] „National minimum wage act, 2019“, žiūrėta 2020 m. spalio 26 d., https://placbillstrack.org/8th/upload/National%20Minimum%20Wage%20Act,%202019.pdf,

prisitaikyti prie potencialių aukų. Pavyzdžiui, siunčiant fišingo ar smišingo žinutes Lietuvoje, manytina, jog reikia mokėti lietuvių kalbą, nes, gavus *fišingo* ar *smišingo* žinutę su netaisyklingu tekstu auka gali pagalvoti, jog institucija (finansų įstaiga, VMI ar kt.) tikrai nepadarytų tokių grubių teksto klaidų ir toki laišką ar žinutę ištrinti.

Toliau baigiamajame darbe bus atskleisti veiksniai, kurie skatina bendrai nusikalstamų veikų elektroninėje erdvėje darymą, juos susiejant su sukčiavimais elektroninėje erdvėje. Xingan Li išskiria šiuos veiksnius, dėl ko asmenys elektroninėje erdvėje linkę daryti nusikaltimus[180]:

1. **Informacijos sklaida**. Elektroninėje erdvėje asmenys turi požiūrį, jog visa informacija yra viešai prieinama ir kiekvienas asmuo gali aptikti ir naudoti viešai prieinamą informaciją. Darbo autorius nori pabrėžti, jog sukčiavimui elektroninėje erdvėje nukreiptam į juridinius asmens įtakos gali turėti būtent nenutrūkstama ir viešai įmonės skelbiama informacija. Sukčiai socialinių tinklų platformose gali aptikti, pavyzdžiui, įmonei vadovaujančių asmenų laisvalaikio planus, kada jie atostogauja. Žinodami šią informaciją, sukčiai gali numatyti, kada įmonės vadovas bus sudėtingiau pasiekiamas ir taip inicijuoti sukčiavimą, nukreiptą į juridinius asmenis.
2. **Realizuojamas nusikaltėlio „ego“**. Pasak Xingan Li, kai kurie nusikaltėliai elektroninėje erdvėje daro nusikalstamas veikas norėdami parodyti, jog jie skiriasi nuo kitų žmonių savo turimų žinių kiekiu. Šis veiksnys sietinas su nusikaltėlių elektroninėje erdvėje organizuotomis grupuotėmis, pavyzdžiui Nigerijos „Yahoo-boys“[181]. Šie Nigerijos piliečiai, manytina, netgi didžiuojasi, esantys „Yahoo-boys“ grupuotės nariai.
3. **Techninių žinių išbandymas.** Techninių žinių išbandymas jau nuo seniau sietinas su motyvuojančiąja priemone. Pavyzdžiui, asmenys paskleidę *botnet'ą* ir užkrėtę tūkstančių aukų kompiuterius gali manyti, jog jų programinė įranga, tiesiogiai sukurta daryti nusikalstamą veiką veikia.
4. **Naujų iššūkių ieškojimas.** Nusikalstamos veikos, kurias motyvuoja iššūkių ieškojimas, nėra retos praktikoje. Kevinas Mitnikas, vienas žymiausių pasaulio hakerių neteisėtai paveikė kitas informacines sistemas, norėdamas išsiaiškinti jų netobulumą. Manytina, jog sukčiai elektroninėje erdvėje, pavyzdžiui, apgaule įgiję

[180] Xingan Li, „A Review of Motivations of Illegal Cyber Activities.“ *Criminology & Social Integration: journal for criminology, penology and behaviour problems*, Vol. 25 No. 1, 2017: 110-123. https://doi.org/10.31299/ksi.25.1.4 https://hrcak.srce.hr/file/266976.

[181] Suleman Lazarus ir Geoffrey U. Okolorie, „The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents.“ *Telematics & Informatics* 40 (July 2019): 9-14. doi:10.1016/j.tele.2019.04.009, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331970.

10 eurų turtą, pamatę, kad jiems tai pavyko gali pamėginti įvykdyti didesnio masto ataką.

Y. O. Ogunleye ir kt. [182] atliko 17 sukčių moterų Nigerijoje elektroninėje erdvėje apklausą interviu metodu. Šiuo empiriniu tyrimu buvo nustatyta, jog pagrindiniai veiksniai, kurie lėmė sukčiavimo elektroninėje erdvėje padarymą buvo finansinės naudos ieškojimas ir aplinkinių spaudimas. Tik keletas iš respondentų pasakė, jog sukčiavimą elektroninėje erdvėje daro dėl malonumo ir pramogos:

- „Mano brolis, kuris daro sukčiavimus elektroninėje erdvėje yra jaunesnysis brolis. Aš jo vyresnioji sesuo. Aš tiesiog pagalvojau, jeigu mano brolis daro sukčiavimus elektroninėje erdvėje ir taip užsidirba pinigų, kodėl to pačio negaliu padaryti ir aš bei taip uždirbti pinigų savo šeimai? Galų galiausiai, tai ką gali padaryti vyrai, moterys gali padaryti dar geriau. Tai ir motyvavo mane įsitraukti į sukčiavimus elektroninėje erdvėje.“ (Sukčius moteris, 24 metai)
- „Kas mane motyvavo, tai, jog man reikėjo pinigų. Kai aš pamačiau, jog mano draugai kažką perka, ko aš sau negaliu leisti, man pasidarydavo labai bloga. Dėl to ir pasirinkau sukčiauti elektroninėje erdvėje. Mano manymu tai yra geriau, nei tapti prostitute.“ (Sukčius moteris, 22 metai)
- „Aš dirbau mokytoja prieš tai, kai buvau priimta į šį universitetą. Aš mokiau vaikus pradinėje mokykloje, kur mano mėnesinis atlyginimas siekė 4,500 Nigerijos nairų (*aut. past.* – 9,82 eurai). Tada, galiausiai man pavyko įstoti į universitetą, tačiau turėjau problemų po įstojimo. Aš beveik pasidaviau iki kol mano senelis, kuris man parodė būdą užsidirbti sukčiaujant elektroninėje erdvėje.“ (Sukčius moteris, 21 metai)
- „Niekas iš tikrųjų manęs nemotyvavo įsitraukti į sukčiavimą elektroninėje erdvėje. Tai buvo tiesiog kažkas, ką aš nusprendžiau daryti, kai turiu laisvo laiko. Linksmai praleisti laiką bei galimai užsidirbti pinigų.“ (Sukčius moteris, 20 metų)

Taigi, tyrimo metu buvo nustatyta, jog didžioji dalis respondentų į sukčiavimą elektroninėje erdvėje Nigerijoje įsitraukė dėl to, jog jautė skurdą bei aplinkinių spaudimą. Didžioji dalis respondentų teigė, jog jiems pinigų reikėjo, siekiant įvykdyti savo finansinius įsipareigojimus – mokestį už studijas, apmokėti ir įgyti reikmenis, naudojamus mokykloje. Sukčiavimas elektroninėje erdvėje respondentams pasirodė geresnė veika, nei užsiimti prostitucija[183].

[182] Yetunde O. Ogunleye, U. Ojedokun ir A. A. Aderinto, „Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria.“ (2020): 315-316. https://www.researchgate.net/publication/339941723_Pathways_and_Motivations_for_Cyber_Fraud_Involvement_among_Female_Undergraduates_of_Selected_Universities_in_South-West_Nigeria.
[183] *Ibid*, 316.

I. Arpad greta aukščiau atskleistų veiksnių taip pat išskiria visuomenės nežinojimą, kaip sukčiavimo elektroninėje erdvėje veiksnį. Anot I. Arpad didžioji dalis interneto naudotojų net nesusimąsto apie riziką, kokią jie gali patirti kiekvieną kartą prisijungiant prie interneto, atveriant elektroninį laišką ar atsisiuntus „nemokamą“ programinę įrangą. Yra tokia dalis visuomenės, kuri apie nusikaltėlius elektroninėje erdvėje sužino tik tada, kai jie tampa sukčių elektroninėje erdvėje aukomis[184]. Manytina, jog šis veiksnys yra vienas iš lemiančių, skatinančių sukčius padaryti sukčiavimą elektroninėje erdvėje. Esant visuomenės, ypač vyresnio amžiaus žmonių, švietimo trūkumui bei nežinant apie sukčiavimo veikas elektroninėje erdvėje jie lengviau gali tapti sukčių aukomis. Jeigu asmuo anksčiau nėra girdėjęs apie tai, jog, pavyzdžiui, nerekomenduojama spausti ant nuorodų, esančių trumpojoje SMS žinutėje ar užsiregistravus pažinčių portale reikia patikrinti informaciją apie pašnekovą elektroninėje erdvėje, sukčiai elektroninėje erdvėje tuo ir naudojasi.

Apibendrinant, išskiriami šie sukčiavimo elektroninėje erdvėje veiksniai: techninio pobūdžio veiksniai, pareigūnų, tiriančių sukčiavimus elektroninėje erdvėje mokymų trūkumas, informacijos sklaida, nusikaltėlio „ego“, techninių žinių išbandymas, naujų iššūkių ieškojimas, skurdas, aplinkinių spaudimas, visuomenės nežinojimas.

[184] Incze Árpád, „A Greater Involvement of Education in Fight Against Cybercrime“. Procedia - *Social and Behavioral Sciences Volume* 83, 4 July 2013: 374, https://doi.org/10.1016/j.sbspro.2013.06.073.

6. SUKČIAVIMŲ ELEKTRONINĖJE ERDVĖJE PREVENCIJOS BŪDAI

Kiek daugiau nei prieš du amžius buvo pasakyta, kad bausmės, kad ir kokia ji būtų, neužtenka, kad būtų galima iš esmės paveikti nusikalstamumą. Nusikalstamumo prevencijos teorijos pradininkas Šarlis Monteskjė iškėlė mintį, jog: „gerą įstatymų leidėją labiausiai domina ne bausmės už padarytus nusikaltimus, o kelio nusikaltimams užkirtimas“ vėliau tapęs kriminologų, kūrusių nusikalstamumo prevencijos teoriją ir tobulinusių jos praktiką, šūkiu[185].

Nusikalstamumo prevencija literatūroje aiškinama kaip valstybinio arba visuomeninio pobūdžio priemonių daugiapakopė sistema, nukreipta į nusikalstamumą lemiančių priežasčių neutralizavimą (veikimo apribojimą, įtakos silpninimą), siekiant mažinti nusikalstamumo lygį. Nusikalstamų veikų prevencija kriminologine prasme yra visų viešų ir privačių pastangų, kuriomis siekiama užkirsti kelią nusikalstamoms veikoms, visuma[186].

Lietuvos Respublikos viešojo saugumo plėtros programos patvirtinimo[187] vienas iš tikslų valstybiniu lygiu, nuosekliai, mažinti nusikalstamų veikų darymo elektroninėje erdvėje galimybes. Siekiant įgyvendinti šį tikslą yra iškeliami uždaviniai:

- plėtoti teisėsaugos, kitų valstybės institucijų ir įstaigų ir privataus sektoriaus partnerystę;
- didinti gyventojų informuotumą apie nusikalstamų veikų elektroninėje erdvėje grėsmes ir priemones bei būdus joms išvengti;
- sustiprinti nusikalstamų veikų elektroninėje erdvėje tyrimus atliekančių įstaigų darbuotojų pajėgumą ir gebėjimus;
- aktyviai bendradarbiauti su Europos kovos su elektroniniu nusikalstamumu centru ir užtikrinti tarptautinių įsipareigojimų teisėsaugos srityje vykdymą.

Lietuvos Respublikos kibernetinio saugumo strategijoje[188] antrame skirsnyje iškeltas tikslas: „užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą.“. Šiam tikslui įgyvendinti yra iškeliami uždaviniai:

- plėtoti valstybės pajėgumus ir gebėjimus kovoti su nusikalstamomis veikomis kibernetinėje erdvėje. Šis uždavinys bus įgyvendinamas tobulinant teisinę sistemą, stiprinant teisėsaugos institucijų profesinius gebėjimus tirti nusikalstamas veikas kibernetinėje erdvėje, kuriant analizės sistemas, diegiant pažangius veiklos

[185] Babachinaitė ir kt., *supra note*, 25: 334.
[186] *Ibid*, 336.
[187] Lietuvos Respublikos Seimo 2015 m. gegužės 7 d. nutarimas Nr. XII-1682 „Dėl Viešojo saugumo plėtros 2015–2025 metų programos patvirtinimo“ (TAR, 2015-05-13, Nr. 2015-07293).
[188] Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (TAR, 2018-08-21, Nr. 2018-13252).

metodus ir procedūras, techninius įrankius, skirtus kovai su nusikalstamomis veikomis kibernetinėje erdvėje;

- stiprinti nusikalstamų veikų kibernetinėje erdvėje prevenciją ir kontrolę. Šis uždavinys bus įgyvendinamas propaguojant visuomenės savisaugos kultūrą ir atsakingą elgesį kibernetinėje erdvėje, tobulinant teisėsaugos institucijų kovos su nusikalstamomis veikomis kibernetinėje erdvėje funkcijų vykdymą ir užtikrinant operatyvesnį tarptautinį bendradarbiavimą tiriant šias nusikalstamas veikas, plėtojant teisėsaugos institucijų efektyvų bendradarbiavimą su mokslo ir studijų institucijomis, viešojo ir privataus sektorių atstovais bei visuomene.

Taigi, remiantis šiomis strategijomis prevencija yra nukreipiama į visuomenės švietėjišką veiklą, privataus ir valstybinių įstaigų bendradarbiavimą.

Gyventojų informuotumas sietinas su viktimologine prevencija, kuri suprantama kaip: „vyriausybinių ir nevyriausybinių organizacijų arba pavienių asmenų specifinė veikla, kuria siekiama šalinti arba sumažinti viktimogeninius veiksnius bei jų keliamus padarinius.“[189]. Europol 2015 m. organizuoto nusikalstamumo elektroninėje erdvėje pranešime teigiama, jog kova su nusikaltimais elektroninėje erdvėje be kita ko turi apimti ne tik šių nusikalstamų veikų atskleidimą, bet ir švietėjišką veiklą. Kiekvienas išsilavinęs bei informuotas visuomenės narys ar organizacija yra viena auka mažiau. Tačiau vien tik švietėjiška veikla niekada nesumažins nusikalstamumo, nes vis tiek atsiras tokių asmenų, kurie „užkibs“ ant sukčių elektroninėje erdvėje kabliuko. Kaip buvo atskleista šio baigiamojo darbo ketvirtajame skyriuje, sukčių aukomis tampa net tie asmens, kurie patys tiria tokio pobūdžio nusikalstamas veikas. Toliau baigiamajame darbe bus atskleistos švietėjiškos veikos, nukreiptos į sukčiavimo modelių, atskleistų pirmajame šio darbo skyriuje, apžvalgą.

J. C. Archie ir kt.[190] išskiria šias prevencijos priemones, nukreiptas į sukčiavimą elektroninėje erdvėje prieš juridinius asmenis – prieš darant pervedimą visada pasitikrinti mokėjimo duomenis su siuntėju telefonu, turėti el. pašto dėžutės apsisaugojimo priemones, sukurti vidinę įmonės procedūrą, kaip bus tvirtinami mokėjimai, nustatyti asmenį, kuris bankui kreipiantis patvirtins mokėjimą telefonu,. Taip pat pabrėžiama būtinybė įmonės pašto dėžutei naudoti saugų slaptažodį. Slaptažodis negali būti naudojamas niekur kitur. Nusikaltėliams neteisėtai paveikus kitos informacinės sistemos duomenų bazę ir naudojant tą patį slaptažodį, sukčiai gali įgyti prieigą ir prie įmonės el. pašto dėžutės. Taip pat juridiniams asmenims rekomenduojama sukurti dviejų

[189] Rokas Uscila, *Viktimologijos pagrindai* (Vilnius: Nusikalstamumo prevencijos Lietuvoje centras, 2005), 175.
[190] Archie, Turner ir Wybitul, *supra note,* 28: 14.

lygių prisijungimo prie el. pašto dėžutės prieigą. M. Weinstein[191] greta sukčiavimo modelio, nukreipto į juridinius asmenis taip pat pabrėžia, jog įmonei bendradarbiaujant su kitu juridiniu asmeniu nenaudoti nemokamų el. pašto paslaugų teikėjų paslaugų – *Gmail* ar *Yahoo.* Svarbiausias prevencijos būdas anot M. Weinstein yra įmonės darbuotojų, susijusių su finansais, mokymas.

Baigiamojo darbo autorius pritaria tam, jog svarbiausia prevencija yra darbuotojų mokymas. Visi kiti prevencijos būdai, manytina, yra pagalbiniai. Turbūt nesuklysime sakydami, jog įmonėse, kur vidutinis buhalterių, ar kitų asmenų, susijusių su įmonės finansais amžius yra virš 50 metų ar daugiau gali būti palikta spragų nusikaltėliams sėkmingai įgyvendinti šį sukčiavimo elektroninėje erdvėje modelį. Manytina, jog kai kurie įmonių finansininkai gali būti iš viso negirdėję apie sukčiavimą, nukreiptą į juridinius asmenis ir įmonėse nėra sukurtų vidinių procedūrų, kaip turi būti elgiamasi, kai gaunami prašymai pakeisti verslo partnerio banko sąskaitą. Kai kurie darbuotojai gavę prašymą pakeisti verslo partnerio sąskaitą nežinodami apie šį sukčiavimo modelį ar praeityje su juo nesusidūrę gali naują mokėjimą daryti į kitą banko sąskaitą, o apie tai sužinoti tik tada, kai tikrasis lėšų gavėjas kreipiasi su užklausa apie pervedimo būseną.

Europol kartu su Lietuvos policija, sukčiavimo susijusio su investicijomis išskiria šias prevencines aukų apsisaugojimo galimybes[192] – prieš perduodant pinigus ar investuojant pasikonsultuoti su pažįstamu ar savo banko finansininku; atmesti skambučius, susijusius su investavimo galimybėmis; atsargiai vertinti pasiūlymus, žadančius didžiulę grąžą ir didelį pelną; nepamiršti, jog su sukčiavimu galima susidurti ir ateityje – vieną kartą atsisakius sukčių pasiūlymo galima sulaukti sukčių bendrininkų skambučio su pasiūlymu investuoti. Lietuvos bankas siekdamas apsaugoti vartotojų finansinius interesus savo tinklalapyje skelbia sąrašą įmonių, kurios neturi teisės verstis finansine veikla (įskaitant ir investicinių paslaugų siūlymą) Lietuvos Respublikoje kartu su jų administruojamais tinklalapiais[193]. Greta to Lietuvos bankas taip pat pateikia kelis prevencinius žingsnius, prieš sukčiavimą, susijusį su investicijomis – neinvestuoti į produktus, kurių vartotojas neišmano; patikrinti, ar investavimo paslaugas teikianti įmonė turi licenziją; vengti ypač patrauklių, greitą pelną žadančių investicinių paslaugų teikėjų.

Lietuvos bankas pažymi, jog jie gali užblokuoti sukčiavimo, susijusio su investicijomis sukčių administruojamą tinklalapį, tačiau, manytina, jog šis prevencijos būdas nesuteikia gyventojams tinkamos apsaugos. Sukčiai vos per kelias minutes gali sukurti „veidrodinį“ domeną ir toliau vykdyti savo veiklą iki, kol bus užblokuotas naujas domenas. Galima manyti, jog tikslinga

[191] Michael Weinstein, „Business Email Compromise and Wire Fraud: How to Protect Your Clients and Firm in the Year Ahead.“ National Real Estate Investor, January 2017, 14. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=f5h&AN=121064686&site=ehost-live.

[192] „Europol prevencijos metodai“, Europol, žiūrėta 2020 m. lapkričio 14 d., https://www.europol.europa.eu/sites/default/files/documents/lt_0.pdf.

[193] „Subjektų, neturinčių teisės verstis investicine veikla Lietuvos Respublikoje, sąrašas“, Lietuvos bankas, žiūrėta 2020 m. lapkričio 14 d., https://www.lb.lt/lt/subjektu-sarasas.

būtų kreiptis į hostingo teikėją su prašymu nutraukti bei blokuoti patį sukčių tinklalapio talpinimą, tačiau sukčiai tinklalapius, susijusius su investicijomis gali patalpinti į „neperšaunamos tarnybinės stoties“[194] (angl. *bullet-proof hosting*) paslaugų teikėją, kuris nereaguos į valstybinių įstaigų prašymus nutraukti sukčių tinklalapio talpinimo paslaugų teikimą.

Kaip teigia M. Tiwari ir kt.[195] nors ir ne visi *ICO* (liet. Pirminiai tokenų siūlymai) kriptovaliutų investiciniai pasiūlymai tiesiogiai sukurti apgaule įgyti investuotojų lėšas, tačiau patiems investuotojams svarbu imtis proaktyvių veiksmų siekiant netapti sukčių auka. M. Tiwari ir kt. išskiria šias *ICO* kriptovaliutų prevencines priemones[196]:

- *ICO* „baltoji knyga“. Investuotojai neturėtų aklai pasitikėti pateikta *ICO* leidėjo informacija, marketinginiais triukais. Investuotojas turi nuosekliai susipažinti su visa *ICO* leidėjo pateikta informacija, kad suprastų pasiūlymo pobūdį ir nustatytų jo įgyvendinamumą. Investuotojas turi įvertinti ilgalaikius *ICO* kriptovaliutos perspektyvas, didžioji dalis informacijos turi būti atskleista pačio *ICO* leidėjo. Ilgalaikių tikslų ir uždavinių neaiškumas gali būti vienas iš sukčiavimo rodiklių.
- Investavimo rentabilumas. Investuotojams rekomenduojama nuodugniai išanalizuoti per *ICO* siūlomos kriptovaliutos vertės pasiūlymą, siekiant nustatyti, ar pasiūlymas turi pakankamai naudos, kad būtų galima investuoti, ir ar įmanoma, kad ši nauda būtų įgyvendinta. Ši informacija gali būti naudinga siūlomos ICO kriptovaliutos teisėtumo požymis.
- *ICO* kriptovaliutų leidėjo patikrinimas. Investuotojai turėtų patikrinti viešai prieinamą informaciją apie *ICO* kriptovaliutų leidėjų vadovybę. Investuotojai turėtų patikrinti *ICO* kriptovaliutų leidėjų socialinių tinklų profilius, viešai prieinamą informaciją apie darbo patirtį. Baigiamojo darbo autoriaus nuomone šis prevencijos būdas, nukreiptas į *ICO* kriptovaliutų sukčiavimo prevenciją yra svarbiausias. Pavyzdžiui, viena didžiausių Estijoje veikusių tarpusavio skolinimosi platformų *Envestio* dingo su visais investuotojų pinigais, kai ją įsigijo investuotojas iš Vokietijos, vardu „Mr. Arkadi Ganzin“[197]. Minėtas asmuo neturėjo jokios patirties finansų rinkoje. Pasinaudojus viešai prieinama vardų ir pavardžių paieškos

[194] Bullet-proof hosting tarnybinės stotys dažniausiai būna valstybėse, kuriose tam tikra veika nėra nusikalstama, todėl specialistai gali talpinti neteisėtų EMP duomenų įgijimo, sukčiavimo susijusio su investicijomis, vaikų pornografijos, kompiuterio tinklų pažeidžiamumo (angl. botnet) ir kitas nusikalstamos veikos, numatytos LR BK 198 straipsnyje atitinkančią sudėtį tinklalapius.

[195] Milind Tiwari, Adrian Gepp ir Kuldeep Kumar, „The Future of Raising Finance - a New Opportunity to Commit Fraud: A Review of Initial Coin Offering (ICOs) Scams.“ *Crime, Law & Social Change* 73, no. 4 (May 2020): 435. doi:10.1007/s10611-019-09873-2. https://www.deepdyve.com/lp/springer-journals/the-future-of-raising-finance-a-new-opportunity-to-commit-fraud-a-QCSgDt0asJ?key=springer.

[196] *Ibid,* 435.

[197] „Envestio has vanished. This is why“, Explorep2p, žiūrėta 2020 m. lapkričio 29 d., https://explorep2p.com/envestio/.

sistema *forebears.io* ir įvedus pavardę „Ganzin“ šis asmuo gali būti iš Benino. Taigi, asmuo save pristatęs kaip Vokietis neteisėtai įgyjo investuotojų lėšas ir dingo. Nors šis pavyzdys sietinas su tarpusavio skolinimosi platforma, tačiau investuotojams patartina išsamiai išanalizuoti *ICO* kriptovaliutos leidėjų profilį.

- *ICO* reitingas ir atsiliepimai. Investuotojai turėtų atsižvelgti į informaciją apie ICO kriptovaliutą elektroninėje erdvėje – kriptovaliutų reitingų tinklalapius, kriptovaliutų ekspertų bendruomenes, kur kiti investuotojai dalinasi informacija apie *ICO* investavimo galimybes.

Europol kartu su Lietuvos policija išskiria šias „romantinio sukčiavimo“ aukų apsisaugojimo priemones[198]: būti atsargiam, dalinantis informacija socialiniuose tinkluose ir pažinčių svetainėse apie save; visada įvertinti galimą riziką registruojantis net ir į žinomiausius pažinčių portalus; išlikti ramiems ir klausinėti; atidžiai išsistudijuoti pašnekovo nuotrauką, kitą asmeninę informaciją, patikrinti, ar ji nėra atvaizduojama kitur; atkreipti dėmesį į asmens rašybos ir gramatines klaidas, jų atsiprašymus „neveikia vaizdo kamera“; nesidalinti jokia kompromituojančia informacija, kurią vėliau gali panaudoti sukčiai (angl. *sextortion*); vengti pervesti pinigų, atskleisti savo tapatybę identifikuojančią informaciją.

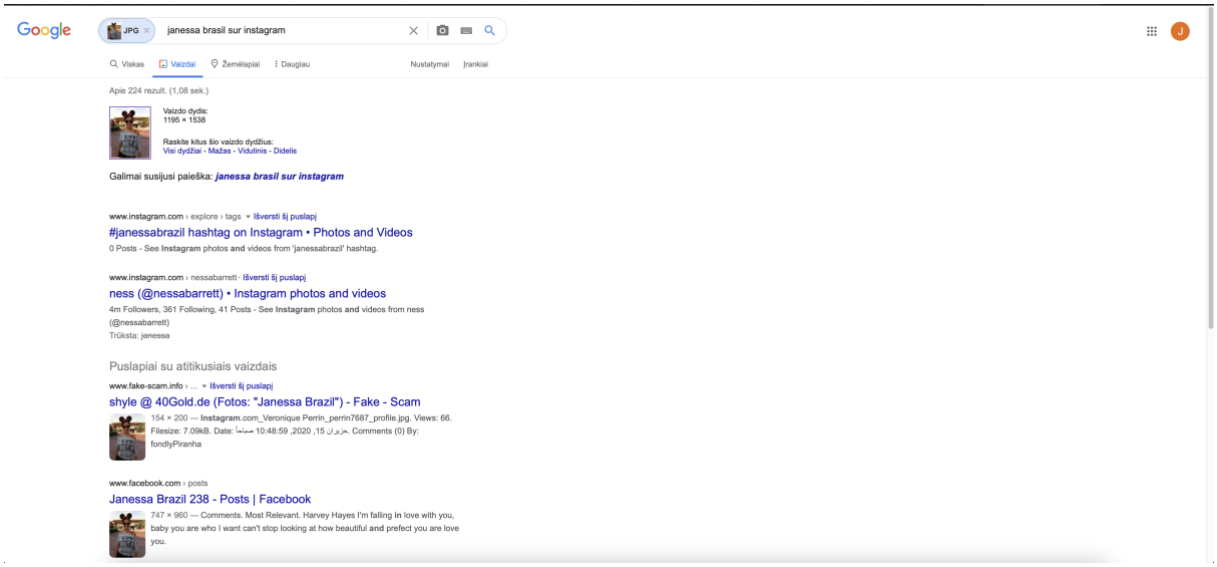
Nors ir šios priemonės atrodo galėtų asmenis apsaugoti nuo „romantinių sukčių“ tačiau anot K. D. Jong atsargumo kampanijos romantinio sukčiavimo atveju dažnai neveikia, todėl būtina apžvelgti kitus „romantinio sukčiavimo“ prevencijos būdus[199]. Vienas iš būdų yra atvirkštinė nuotraukos paieška (angl. *reverse image search*), kurios metu pažinčių svetainės vartotojas gali išsisaugoti kito asmens nuotrauką ir apsilankius tinklalapyje *images.google.com* šią nuotrauką pateikti bei patikrinti, ar ji nėra atvaizduojama kituose elektroninėje erdvėje veikiančiuose tinklalapiuose. Tokiu būdu vartotojas gali įsitikinti, ar iš tikrųjų bendrauja su tuo asmeniu, kuo jis skelbia esąs. Tačiau šis būdas ne visada gali padėti vartotojui apsisaugoti nuo sukčių elektroninėje erdvėje. Sukčiai gali panaudoti nuotraukas asmens, kuris nėra labai populiarus ir tokiu būdu vartotojas gali nerasti sukčiaus pateiktų nuotraukų per *Google* atvirkštinės nuotraukos paieškos platformą.

Elektroninėje erdvėje pastebėtinas tinklalapis *romancescamsnow.com,* kuriame aukos patyrusios viktimizaciją prevenciškai dalinasi informaciją apie „romantinius sukčius“. Baigiamojo darbo autorius apžvelgė vieną iš sukčių profilių[200] - šiame profilyje matyti sukčiaus naudojamas vardas „Becky Page“, elektroninio pašto adresas, taip pat paminėtina, jog šio asmens nuotraukos

[198] Europol, *supra note*, 192.
[199] Koen de Jong, „Detecting the online romance scam: Recognising images used in fraudulent dating profiles“ *Department of EEMCS,* University of Twente (November 2019): 3 http://essay.utwente.nl/80084/1/Jong_de_MA_EEMCS.pdf.
[200] „Yet Another Ghana Scammer“, Romancescamnow.com, žiūrėta 2020 m. lapkričio 14 d., https://romancescamsnow.com/dating-scams/scammer-becky-page/.

jau anksčiau buvo naudojamos pasisavinant kito asmens tapatybę „Beck Ellis“ bei „Yusifyn Destiny“, sukčiaus sukurta charakteristika, pažinčių svetainėje esantis anketos aprašymas, naudojama pirma žinutė, galimos užuominos, išduodančios sukčių bei sukčiaus patalpintos, neva „Becky Page“ nuotraukos. Pasirinkus pirmąją nuotrauką ir pasinaudojus atvirkštinės nuotraukos paieška matyti, jog „Becky Page“ iš tiesų yra „Janessa Brazil“ (žr. 36 pav.)

36 paveikslas. Google atvirkštinė nuotraukos paieškos sistema[201]



Fišingą, višingą ir smišingą skiria nusikalstamos veikos atlikimo būdas, todėl prevencinės priemonės bus nagrinėjamos kartu. *Europol* kartu su Lietuvos policija išskiria šias prevencinio pobūdžio priemones[202]: reguliariai atnaujinti savo programinę įrangą; būti budriems, jei „bankas“ el. paštu, trumpąja SMS žinute ar skambučiu prašo tapatybę identifikuojančių duomenų; atidžiai peržiūrėti el. laišką, trumpąją SMS žinutę ir palyginti su jau prieš tai siųstais banko. Patartina patikrinti, ar nėra rašybos ir gramatikos klaidų; nespausti ant pateiktų nuorodų ir neatsisiųsti laiške esančių priedų; niekada neatsakyti į tekstinę žinutę, kurioje reikalaujam nurodyti PIN kodą, internetinės bankininkystės slaptažodį ar bet kuriuos kitus saugos duomenis; užfiksuoti skambinančiojo numerį ir informuoti, jog jam perskambinsite; kilus įtarimui susisiekti su banku ar policija.

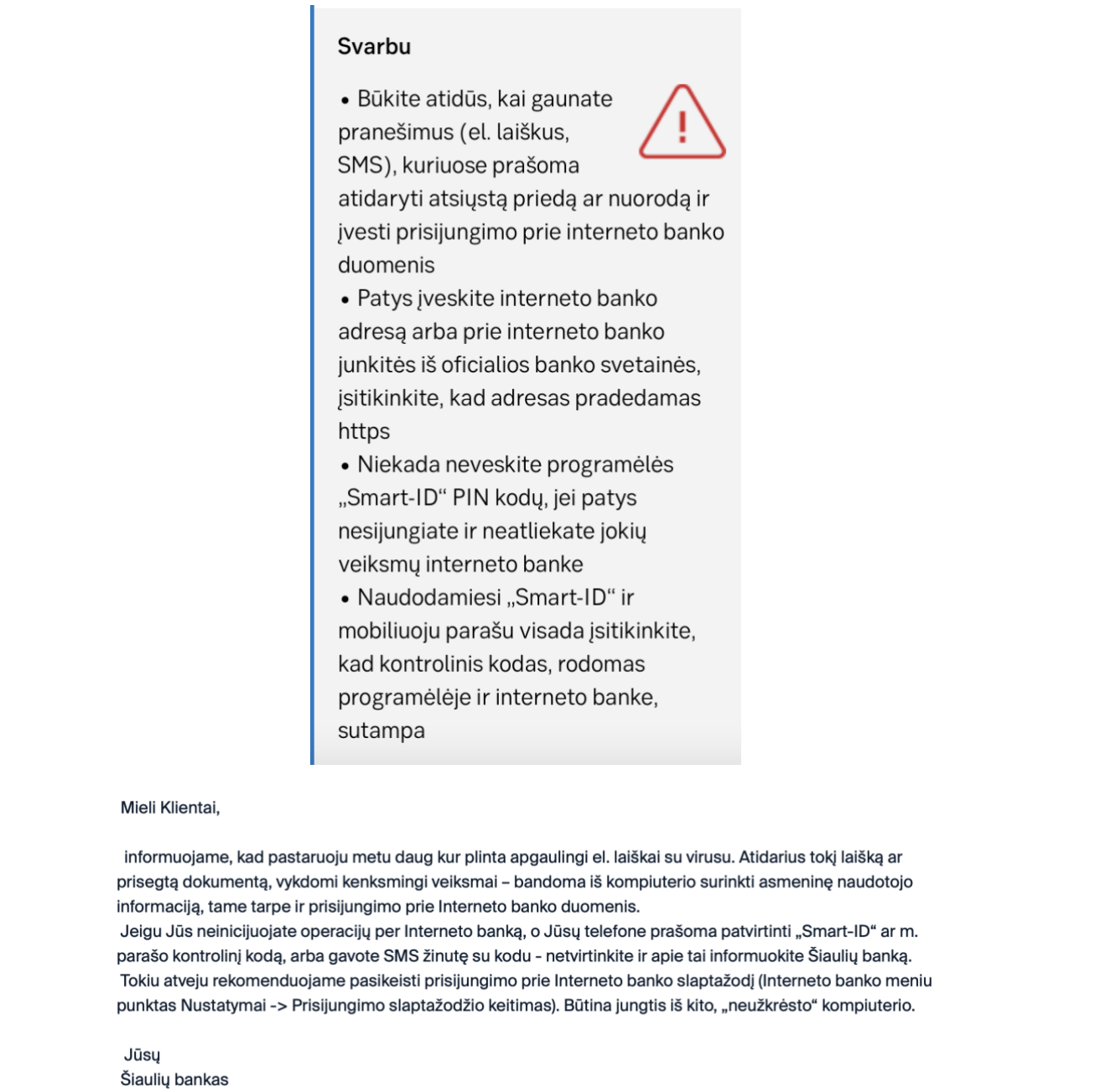
201 Šaltinis: https://www.google.com/search?tbs=sbi:AMhZZisZAc6uaAKWys05gbJsP1iG0YufxwJvlXz0k22p7Umg_1IEHFIj9yb1xTtHy5XMdk8IyqaWeBm_1OgOToFkxkCOkSlTJGCPpBY61Zh6Ns9mWM2zyhjzQ7WhE7Jp6J4Kvn156Ptnc7B-czcyWGGsOAR7b9KQlBATsHG2hwCCx3duBl5xqSrnLz413l_1hBUhfzBRWBVaIMCNLP7nX3Esj-dCmub03eLsq1is6sHCfaBjo4L8DaItI7WReX84R5yh5Hez63FvquJJEg8iCjZD_1ub5Ony6RYIaQNSiVdLUuEkyaTVHQ3YWyRyjmpSZmj-bMFwIAvLZr8g&hl=lt naudojant nuotrauką: https://i1.wp.com/romancescamsnow.com/wp-content/uploads/2013/10/IMG_1616.jpg?ssl=1.

202 Europol, *supra note*, 192.

Pastebėtina, jog keli didieji Lietuvoje veikiantys bankai įspėja vartotojus jungiantis prie elektroninės bankininkystės apie fišingo, višingo ir smišingo pavojų bei kaip netapti sukčių elektroninėje erdvėje auka (žr. 37 pav.) Šiuose pranešimuose finansinių paslaugų vartotojams rekomenduojama būti atidiems, kai gaunami el. laiškai ar pranešimai, kuriuose prašoma paspausti ant tame pranešime atvaizduojamos nuorodos ar paspausti jame esančią nuorodą.

37 paveikslas. Lietuvoje veikiančių bankų (SEB, Swedbank ir Šiaulių banko informaciniai pranešimai, kaip netapti fišingo, smišingo ar višingo auka)[203]

[203] AB SEB bankas, AB Šiaulių bankas ir AB Swedbank prisijungimo prie el. bankininkystės tinklalapis.



Svarbu

- Būkite atidūs, kai gaunate pranešimus (el. laiškus, SMS), kuriuose prašoma atidaryti atsiųstą priedą ar nuorodą ir įvesti prisijungimo prie interneto banko duomenis
- Patys įveskite interneto banko adresą arba prie interneto banko junkitės iš oficialios banko svetainės, įsitikinkite, kad adresas pradedamas https
- Niekada neveskite programėlės „Smart-ID“ PIN kodų, jei patys nesijungiate ir neatliekate jokių veiksmų interneto banke
- Naudodamiesi „Smart-ID“ ir mobiliuoju parašu visada įsitikinkite, kad kontrolinis kodas, rodomas programėlėje ir interneto banke, sutampa

Mieli Klientai,

informuojame, kad pastaruoju metu daug kur plinta apgaulingi el. laiškai su virusu. Atidarius tokį laišką ar prisegtą dokumentą, vykdomi kenksmingi veiksmai – bandoma iš kompiuterio surinkti asmeninę naudotojo informaciją, tame tarpe ir prisijungimo prie Interneto banko duomenis.
Jeigu Jūs neinicijuojate operacijų per Interneto banką, o Jūsų telefone prašoma patvirtinti „Smart-ID“ ar m. parašo kontrolinį kodą, arba gavote SMS žinutę su kodu - netvirtinkite ir apie tai informuokite Šiaulių banką.
Tokiu atveju rekomenduojame pasikeisti prisijungimo prie Interneto banko slaptažodį (Interneto banko meniu punktas Nustatymai -> Prisijungimo slaptažodžio keitimas). Būtina jungtis iš kito, „neužkrėsto“ kompiuterio.

Jūsų
Šiaulių bankas

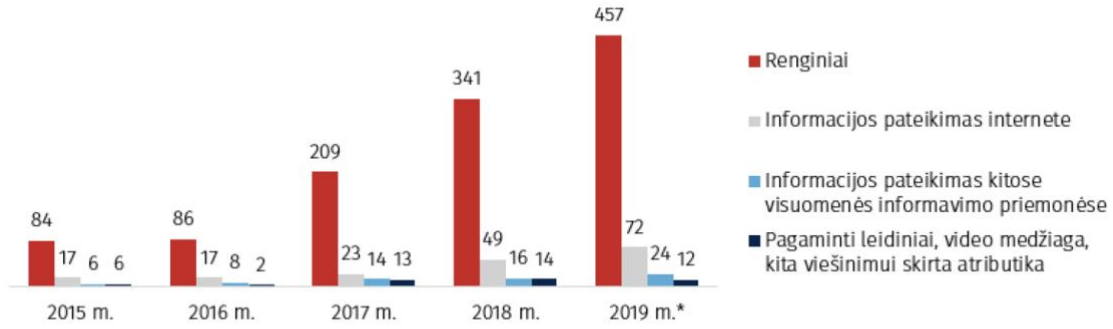
Būkite atsargūs! Sukčiai dažnai apsimeta banko ar „Smart-ID“ darbuotojais. Įsidėmėkite – niekada mes į Jus nesikreipiame, kad sužinotume Jūsų duomenis ar slaptažodžius! Net jei matote mūsų telefono numerį, į Jus kreipiasi vardu ar prašo suvesti duomenis, nedelsdami nutraukite bendravimą. Atminkite, kad sukčiai nuolat sugalvoja naujų būdų kaip išvilioti iš Jūsų lėšas.

S. H. Apandi ir kt. kaip *fišingo* prevencijos būdą išskiria dviejų lygių autentifikacijos procedūrą. Papildoma saugumo priemonė vartotojui jungiantis prie tinklalapio prašo papildomos autentifikacijos SMS žinute ar kitu vartotojui priimtinu būdu[204]. Manytina, jog ši procedūra gali padėti apsisaugoti nuo *fišingo* atakos. Sukčių sukurtas *fišingo* tinklalapis neturi prieigos prie banko vidinės duomenų bazės, todėl vartotojui paspaudus *fišingo* laiške, *smišingo* žinutėje ar *višingo* skambučio metu pateiktą sukčių sukurto tinklalapio nuorodą, šiame tinklalapyje įvedus naudotojo

[204] Apandi Hawa, J. Sallim, ir R. Mohd Sidek, „Types of anti-phishing solutions for phishing attack“, *IOP Conference Series: Materials Science and Engineering*, 2020, 769(1), 3, https://www.researchgate.net/publication/342050858_Types_of_anti-phishing_solutions_for_phishing_attack.

tapatybę patvirtinantį atpažinimo kodą įprasta autentifikavimo procedūra neįvyks. Sukčiai elektroninėje erdvėje įgys atpažinimo kodą bei slaptažodį. Tačiau finansų įstaigai naudojant dviejų lygių autentifikavimo procedūrą, sukčiai net ir žinodami naudotojo atpažinimo kodą bei slaptažodį prie elektroninės bankininkystės sistemos nepavyks prisijungti.

38 paveikslas. 2015–2019 m. Policijos Lietuvoje įgyvendintų nusikaltimų elektroninėje erdvėje prevencinių priemonių skaičius, vnt.[205]

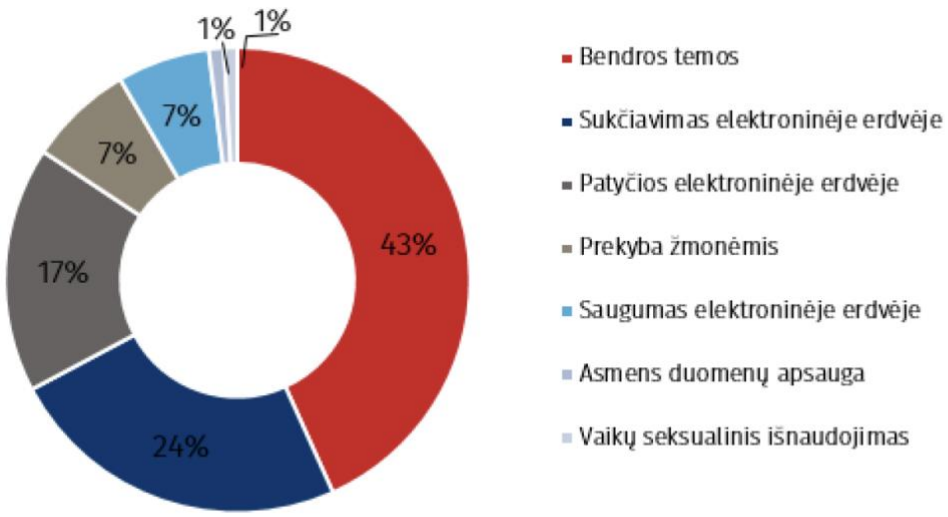


* 2019 m. sausio–spalio mėn. duomenys

Kaip matyti paveiksle nr. 38, 2019 m. lyginant su 2015 m. policijos įgyvendintų renginių, nukreiptų į nusikaltimų elektroninėje erdvėje prevenciją padaugėjo daugiau nei 500 proc., informacijos pateikimo internete lyginant su tiriamojo laikotarpio pabaiga daugėjo daugiau nei 400 proc., informacijos pateikimas kitose visuomenės informavimo priemonėse daugėjo 400 proc., pagamintų leidinių, vaizdo medžiagos, kitos viešinimui skirtos atributikos daugėjo 200 proc. Taigi, policija Lietuvoje siekdama įgyvendinti gyventojų švietėjišką veiklą daugiausia tą darė rengdami renginius. Manytina, jog toks švietėjiškos veiklos pobūdis, nors ir reikalauja daugiau resursų, nei, pavyzdžiui, informacijos pateikimas internete, gali pasiekti didesnę dalį visuomenės. Darbo autoriaus nuomone, didžioji dalis visuomenės *Europol* tinklalapyje nesilanko ir informacijos, kaip apsisaugoti nuo sukčių elektroninėje erdvėje neįsisavina. Todėl renginių metų atskleisti nusikaltimų elektroninėje erdvėje būdai (tarp jų ir sukčiavimo) gali padėti visuomenei suprasti, kas yra sukčiavimas elektroninėje erdvėje bei kaip sumažinti riziką tapti sukčiaus elektroninėje erdvėje auka.

39 paveikslas. 2015–2019 m. Policijos Lietuvoje įgyvendintos nusikaltimų elektroninėje erdvėje prevencinės priemonės pagal temas.[206]

[205] Valstybinio audito ataskaita, *supra note*, 13: 19.
[206] *Ibid*, 19.



Šaltinis – Valstybės kontrolė pagal AVPK pateiktą informaciją

Kaip matyti paveiksle nr. 39, didžiausia dalis policijos tiriamuoju laikotarpiu įgyvendintų priemonių pagal temas buvo bendros temos (43 proc.), greta to sekė sukčiavimas elektroninėje erdvėje (24 proc.). Manytina, jog visuomenės švietėjišką veiklą sukčiavimo elektroninėje erdvėje srityje galima laikyti prioritetine dalimi.

Greta visuomenės švietimo išskirtinas privačių ir valstybinių įstaigų bendradarbiavimas. Kai kurios finansų įstaigos turi įsteigusios globalius sukčiavimo ir ekonominių nusikaltimų prevencijos skyrius. Šių skyrių tikslas – padėti nuo sukčių elektroninėje erdvėje nukentėjusiems klientams. SEB banko Prevencijos departamento vadovas A. Šapola teigia, jog: „labai svarbu greitai reaguoti ir apie tai pranešti bankui“[207]. C. Soviany pažymi, jog aptikti sukčiavimo būdu padarytus mokėjimus naudojamas dirbtinis intelektas[208]. Dirbtinio intelekto pagalba pagal sukurtas taisykles yra tikrinami mokėjimai. Jeigu padarytas mokėjimas neatitinka dirbtinio intelekto nustatytų taisyklių, jo vykdymas yra sustabdomas rankiniam finansų įstaigos specialisto patikrinimui. Taisyklės yra sukuriamos ir nuolat tobulinamos atsižvelgiant į naujus sukčiavimo modelius, jų įvykdymo būdus. Kaip pažymi A. Šapola: „SEB bankas sustabdė daugiau negu 76 tūkst. eurų vertės mokėjimų, kuriuos per tris mėnesius mėgino atlikti sukčiai, siuntę apgaulingas SMS žinutes neva banko vardu banko klientams ir taip iš jų išvilioję prisijungimo prie interneto banko duomenis ir pavogę jų lėšas. Be to, SEB bankas padėjo savo klientams sugrąžinti per 40,5 tūkst. eurų sumą, kurią sukčiai jau buvo pervedę į kitų užsienyje ir Lietuvoje esančių bankų

[207] „Apgaulingas SMS žinutes siunčiantiems sukčiams SEB bankas užkirto kelią pavogti daugiau negu 116 tūkst. eurų“, SEB bankas, žiūrėta 2020 m. lapkričio 17 d., https://www.seb.lt/naujienos/2019-09-26/apgaulingas-sms-zinutes-siunciantiems-sukciams-seb-bankas-uzkirto-kelia-pavogti.

[208] Cristina Soviany, „The Benefits of Using Artificial Intelligence in Payment Fraud Detection: A Case Study.“ *Journal of Payments Strategy & Systems* 12, no. 2 (Summer 2018): 102. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=bth&AN=132033184&site=ehost-live.

sąskaitas.“[209]. Danske bank specialistė A. Krikščiūnė teigia, jog: „Būna, kad reaguoti į tam tikrus atvejus, stabdyti pinigines transakcijas ir perspėti kitus bankus turime ir vidury nakties. Taikome pažangias technologijas, matematinius modelius, kurie padeda atpažinti neteisėtas transakcijas ir jas sustabdyti. Be to, bendradarbiaujame su tokiomis tarptautinėmis teisėsaugos institucijomis kaip Interpolas ar Europolas, atskirų šalių teisėsauga ir bankais visuose žemynuose. Turime kolegų, kurie moka ne tik anglų, danų ar ispanų, bet ir, pavyzdžiui, kinų kalbą. Visa tai neretai leidžia neteisėtas transakcijas atsekti ir ant sukčių kabliuko užkibusių klientų pinigus grąžinti.“[210]. Net ir neteisėtai pateikus mokėjimo nurodymą tampa svarbus finansų įstaigos ir teisėsaugos institucijų bendradarbiavimas. Lėšos į sukčiaus sąskaitą, pavyzdžiui, Europos Sąjungoje yra įskaitomos pagal vieningos mokėjimo eurais erdvės *(angl. Single Euro Payments Area*) nustatytus laikus. Neteisėtai inicijavus mokėjimą iki 16 val., jis sukčiaus Europos Sąjungos finansų įstaigos sąskaitoje bus pervestos dar tą pačią dieną iki 18 val. Todėl finansų įstaigos turi skubiai kontaktuoti su sukčiaus banko atstovais, tam, kad užtikrinti sukčiaus valdomos banko sąskaitos užšaldymą bei su Europol, tam, kad sukčius būtų sulaikytas bei patrauktas atsakomybėn.

Taigi, manytina, jog vartotojams pateikus finansų įstaigai mokėjimo vykdymą, jiems netapti sukčių auka gali padėti finansų įstaigų sukčiavimo prevencijos skyriaus specialistai. Šie specialistai gerai išmano visus sukčiavimo modelius, jų veikimo principus, kontaktuodami su gyventojais ir išgirdę jų istorijas, kokiu tikslu jie perveda pinigus, gali neteisėtą lėšų pervedimą sustabdyti bei grąžinti lėšas atgal į mokėtojo sąskaitą.

Apibendrinant, prevencinio pobūdžio veiklą Lietuvoje įgyvendina *Europol* pasitelkiant Lietuvos policiją, pastaroji rengia viešojo pobūdžio renginius, informacijos sklaidą elektroninėje erdvėje, kur visuomenei atskleidžiama aktualiausia informacija, kaip apsisaugoti nuo sukčių elektroninėje erdvėje. Taip pat pačios finansų įstaigos sukuria specialius padalinius, skirtus kovai su sukčiavimu elektroninėje erdvėje.

[209] *Supra note,* 207.
[210] „Profesionalių sukčių taktikos: pinigai nepastebimai gali keliauti metų metus“, Danske bank, žiūrėta 2020 m. lapkričio 18 d., https://danskebank.lt/apie-banka/naujienos/2020/profesionaliu-sukciu-taktikos.

IŠVADOS

1. Sukčiavimas elektroninėje erdvėje yra kompleksinis socialinis-teisinis reiškinys, susijęs su visuomenės privatumo, saugumo, turtinių interesų pažeidimais. Kai kurios valstybės pasirinko tradicinį sukčiavimą traktuoti siauriau, t.y. išskiriant romantinį sukčiavimą, sukčiavimą, susijusį su sąskaitomis-faktūromis į atskirus nusikaltimus.

2. Sukčiavimas elektroninėje erdvėje gali būti atliekamas pačiais įvairiausiais metodais, kurie kinta atsižvelgiant į socialinėje aplinkoje vyraujančius pokyčius. Dažniausiai naudojami šie sukčiavimo elektroninėje erdvėje modeliai – sukčiavimas, susijęs su investicijomis (angl. *investment scam*), romantinis sukčiavimas (angl. *romance scam*), fišingas (angl. *phishing*), smišingas (angl. *smishing*), višingas (angl. *vishing*), verslo partnerio banko sąskaitos keitimas (angl. *beneficiary account change fraud*), apsimetinas įmonės vadovu (angl. *CEO fraud*).

3. Lietuvoje užregistruotų sukčiavimų elektroninėje erdvėje statistiniai duomenys rodo, kad nuo 2014 metų iki 2019 metų sukčiavimų elektroninėje erdvėje nusikalstamų veikų sumažėjo daugiau nei dvigubai.

4. Jungtinėje Karalystėje užregistruotų sukčiavimų elektroninėje erdvėje statistiniai duomenys rodo, kad nuo 2014 metų iki 2019 metų sukčiavimų elektroninėje erdvėje skaičius išliko stabilus. Viktimologinių tyrimų rezultatų duomenys parodo, jog užregistruoti sukčiavimai elektroninėje erdvėje Jungtinėje Karalystėje atsispindi tik labai maža dalimi – apie 14 proc.

5. Remiantis Lietuvoje registruoto sukčiavimo elektroninėje erdvėje 2014-2019 m, statistiniais duomenimis vidutiniškai 80 proc. visų sukčiavimų elektroninėje erdvėje padarė vyrai. Moterys įvykdė 20 proc, visų sukčiavimų elektroninėje erdvėje. Vidutiniškai dirbantys asmenys padarė apie 41 proc. visų sukčiavimų elektroninėje erdvėje. Vidutiniškai apie 94 proc. visų kaltinamųjų (įtariamųjų) neturėjo aukštojo išsilavinimo. Sukčių elektroninėje erdvėje Lietuvoje 2014-2019 m. vidutinis amžius siekė 26 metus. Remiantis 2010-2015 m. Jungtinėje Karalystėje atlikto tyrimo duomenimis didesnis vyrų sukčiavimo elektroninėje erdvėje aktyvumas sietinas su ankstyvesniu domėjimuosi informacinėmis technologijomis.

6. Remiantis Lietuvoje registruoto sukčiavimo elektroninėje erdvėje 2014-2019 m. statistiniais duomenimis nuo sukčiavimo elektroninėje erdvėje dažniau nukenčia vyrai – apie 56 proc., moterys – apie 41 proc., juridiniai asmenys sudaro mažiausią nukentėjusiųjų dalį – apie 3 proc. Vidutiniškai 62 proc. aukų neturėjo aukštojo išsilavinimo. Aukų elektroninėje erdvėje Lietuvoje 2014-2019 m. siekė 37 metus. Aukos sukčiavimo elektroninėje erdvėje metu, priklausomai nuo sukčiavimo modelio patiria tiek turtinę, tiek psichologinę žalą.

7. Tyrimo metu išsiaiškinta, jog sukčiai elektroninėje erdvėje į savo schemą gali įtraukti asmenius, nieko neįtariančius apie vykstančią nusikalstamą veiką – pinigų mulus.

8. Svarbiausi specifiniai sukčiavimo elektroninėje erdvėje veiksniai yra techninio pobūdžio veiksniai, kadangi elektroninėje erdvėje nusikaltėliams lengviau paslėpti savo identitetą naudojant programinę įrangą ir taip išvengti baudžiamosios atsakomybės bei visuomenės nežinojimas.

9. Sukčiavimo elektroninėje erdvėje prevencija Lietuvoje yra orientuota į švietėjišką visuomenės veiklą policijai organizuojant renginius, informacijos sklaidą internete. Europol kartu su Lietuvos policija šviečia visuomenę, kaip netapti sukčių elektroninėje erdvėje auka. Greta to į „pagalbą“ įsitraukia ir finansinių įstaigų įkurti sukčiavimo prevencijos skyriai.

PASIŪLYMAI

Pasiūlymas finansų įstaigoms:

Kiekvienam finansinių paslaugų vartotojui, atsižvelgiant į jo tipą (fizinis ar juridinis asmuo) el. paštu išsiųsti informacinį pranešimą, kuriame būtų pateikiami sukčiavimo modelio *modus operandi* bei kaip nuo jų apsisaugoti.

Pasiūlymas juridiniams asmenims:

Rengti reguliarius darbuotojų mokymus, tam, kad šiems asmenims būtų žinomas sukčiavimų, nukreiptų į juridinius asmenis *modus operandi*.

Pasiūlymas žiniasklaidos priemonių atstovams:

Reguliariai skleisti informaciją, nukreiptą į sukčiavimo elektroninėje erdvėje prevenciją.

LITERATŪRA

Teisės aktai

1. „Lietuvos Respublikos Baudžiamasis kodeksas.“ *Valstybės žinios*. 2000, Nr. 89- 2741.
2. „Lietuvos Respublikos Seimo 2015 m. gegužės 7 d. nutarimas Nr. XII-1682 „Dėl Viešojo saugumo plėtros 2015–2025 metų programos patvirtinimo.“ (*TAR*, 2015-05-13, Nr. 2015-07293).
3. „Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo.“ (*TAR*, 2018-08-21, Nr. 2018-13252).
4. „2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų.“ (*Žin*., 2004, Nr. 36-1188).
5. „The Swedish Criminal Code.“ (*brottsbalken, SFS* 1962:700)
6. „Fraud act 2006.“
7. „Nigerian minimum wage act, 2019.“

Teismų praktika

Lietuvos Respublikos teismų praktika:

8. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2001 m. spalio 9 d. nutartis baudžiamojoje byloje Nr. 2K-682. *Teismų praktika*. 2001, 16.

Lietuvos banko praktika:

9. 2020 m. sausio 15 d. Lietuvos banko priežiūros tarnybos finansinių paslaugų ir rinkų priežiūros departamento direktoriaus sprendimas *dėl X.X. ir banko AB „SEB bankas“, ginčo nagrinėjimo* Nr. 242-22.
10. 2020 m. vasario 12 d. Lietuvos banko priežiūros tarnybos finansinių paslaugų ir rinkų priežiūros departamento direktoriaus sprendimas *dėl Y.Y. ir UAB „General Financing“, ginčo nagrinėjimo* Nr. 242-65.

Specialioji literatūra

11. Akdemir, Naci, ir Christopher James Lawless. „Exploring the Human Factor in Cyber-Enabled and Cyber-Dependent Crime Victimisation: A Lifestyle Routine Activities Approach“. *Internet Research* 30, no. 6 (November 2020): 1665–87. doi:10.1108/INTR-10-2019-0400. https://www.emerald.com/insight/content/doi/10.1108/INTR-10-2019-0400/full/pdf?title=exploring-the-human-factor-in-cyber-enabled-and-cyber-dependent-crime-victimisation-a-lifestyle-routine-activities-approach.
12. Archer, Aaron K. „I Made a Choice: Exploring the Persuasion Tactics Used by Online Romance Scammers in Light of Cialdini's Compliance Principles“. (2017) *All Regis University Theses*. 823. https://epublications.regis.edu/theses/823.
13. Archie, Jennifer C., Serrin Turner, ir Tim Wybitul. „The Pervasive Threat of Business Email Compromise Fraud - and How to Prevent It“. *Intellectual Property & Technology Law Journal* 32, no. 7 (July 2020): 13–15. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=144723570&site=ehost-live.
14. Árpád, Incze. „A Greater Involvement of Education in Fight Against Cybercrime“. Procedia - *Social and Behavioral Sciences Volume* 83, 4 July 2013, Pages 371-377 https://doi.org/10.1016/j.sbspro.2013.06.073.
15. Aston, Manuel, Stephen McCombie, Ben Reardon, ir Paul Watters. „A Preliminary Profiling of Internet Money Mules: An Australian Perspective. In Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing“. *IEEE Computer Society, USA* (July 2009): 482-487. doi:10.1109/UIC-ATC.2009.63 https://research-management.mq.edu.au/ws/portalfiles/portal/62417793/Publisher+version+%28open+access%29.pdf.
16. Babachinaitė, Genovaitė, ir kt. *Latentinio nusikalstamumo kriminologinio tyrimo metodikos [elektroninis išteklius]: metodinis leidinys*. Vilnius: Mykolo Romerio universitetas, 2009. http://www3.mruni.eu/~akiskis/alfredo-str-latent_nus_tyrimo_metodikos2009.pdf.
17. Babachinaitė, Genovaitė, ir kt. *Kriminologija*. Vilnius: Mykolo Romerio Universiteto leidybos centras, 2010.
18. Brennan, Margaret, ir Kris Van Cleave. „High-Profile Twitter Accounts Hacked in Cryptocurrency Scam“. *CBS Evening News with Katie Couric*. Accessed September 28, 2020.

http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=32U2663153790CB3&site=ehost-live.

19. Brown David, Steven. „Cryptocurrency and Criminality: The Bitcoin Opportunity“. *Police Journal* 89, no. 4 (December 2016): 327-339. https://heinonline-org.skaitykla.mruni.eu/HOL/Page?collection=journals&handle=hein.journals/policejl89&id=323&men_tab=srchresults.
20. Copes, Heith, ir Lynne M. Vieraitis. „Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes“. *Criminal Justice Review (Sage Publications)* 34, no. 3 (September 2009): 329–49. doi:10.1177/0734016808330589. http://cjr.sagepub.com/cgi/content/abstract/34/3/329.
21. Cross, Cassandra, Russell G. Smith, ir Kelly Richards. „Challenges of Responding to Online Fraud Victimisation in Australia“. *Trends & Issues in Crime & Criminal Justice*, no. 474 (May 2014): 1–6. https://www.aic.gov.au/publications/tandi/tandi474.
22. Cross, Cassandra. „'Oh We Can't Actually Do Anything about That': The Problematic Nature of Jurisdiction for Online Fraud Victims“. *Criminology & Criminal Justice: An International Journal* 20, no. 3 (July 2020): 358–75. doi:10.1177/1748895819835910. https://journals.sagepub.com/doi/pdf/10.1177/1748895819835910.
23. Cross, Cassandra, Kelly Richards, ir Russell G. Smith. „The Reporting Experiences and Support Needs of Victims of Online Fraud“. *Trends & Issues in Crime & Criminal Justice*, no. 518 (August 2016): 1–14. doi:10.1177/1748895815603773, https://www.aic.gov.au/sites/default/files/2020-05/tandi518.pdf.
24. Cross, Cassandra, ir Rosalie Gillett. „Exploiting Trust for Financial Gain: An Overview of Business Email Compromise (BEC) Fraud“. *Journal of Financial Crime* 27, no. 3 (July 2020): 871–84. doi:10.1108/JFC-02-2020-0026, https://eprints.qut.edu.au/200621/1/BEC_fraud_CROSS_GILLETT_submit.pdf.
25. Custers, Bart HM, Ronald LD Pool, ir Remon Cornelisse. „Banking Malware and the Laundering of Its Profits“. *European Journal of Criminology* 16, no. 6 (November 2019): 728–45. doi:10.1177/1477370818788007. https://journals.sagepub.com/doi/pdf/10.1177/1477370818788007.
26. Deliema, Marguerite, Doug Shadel, ir Karla Pak. „Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors“. *Journal of Consumer Research* 46, no. 5 (February 2020): 904–14. doi:10.1093/jcr/ucz020. http://web.a.ebscohost.com/ehost/detail/detail?vid=11&sid=b72d32f9-9e28-4188-be85-98f36cce2937%40sdc-v-sessmgr02&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=141139652&db=bth.

27. Driscoll, Kara. „Crime and Cryptocurrency: How Local Criminals Use Bitcoin Illegally“. *Dayton Daily News (OH)*, December 22, 2017. http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=2W617034305 49&site=ehost-live.
28. Gordon, G. R ir kt. *Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement*. Utica: NY Center for Identity Management and Information Protection, 2007. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.216.6696&rep=rep1&type=pdf.
29. Grincevičius, Rokas. „Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose“. Daktaro disertacija, Mykolo Romerio Universitetas, 2019. https://www.lvb.lt/permalink/f/16nmo04/ELABAETD36356059.
30. Gross, Grant. „First Phishing, Now Vishing“. *CIO* 19, no. 22 (September 2006): 16. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=22322570&site=ehost-live.
31. Hale, Chris ir kt. *Criminology.* Oxford: Oxford University Press, 2005.
32. Hawa Apandi, S., Sallim, J., ir Mohd Sidek, R. „Types of anti-phishing solutions for phishing attack“. *IOP Conference Series: Materials Science and Engineering*, 2020, 769(1), 8, https://www.researchgate.net/publication/342050858_Types_of_anti-phishing_solutions_for_phishing_attack.
33. Higgins E. George. *Cybercrime: an introduction to an emerging phenomenon*. Boston: McGraw-Hill Higer Education, 2010.
34. Holt J., Thomas. *Cybercrime Through an Interdisciplinary Lens*. London: Routledge, 2017. https://doi-org.skaitykla.mruni.eu/10.4324/9781315618456.
35. Jong, de Koen. „Detecting the online romance scam: Recognising images used in fraudulent dating profiles“. *Department of EEMCS, University of Twente* (November 2019): http://essay.utwente.nl/80084/1/Jong_de_MA_EEMCS.pdf.
36. Kakati, Shivam, ir Chandana Goswami. „Factors and Motivation of Fraud in the Corporate Sector: A Literature Review“. *Journal of Commerce & Accounting Research* 8, no. 3 (July 2019): 86–96. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=bth&AN=138408217&site=ehost-live.
37. Kary, Tiffany, ir Anne Riley Moffat. „Jeans Brand Diesel USA Files for Bankruptcy as Turnaround Lags“. *Bloomberg.Com*, March 5, 2019, N.PAG.

http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=140631142&site=ehost-live.

38. Kassem, Rasha, ir Higson, Andrew. „The New Fraud Triangle Model (June 1, 2012)“. *Journal of Emerging Trends in Economics and Management Sciences* (JETEMS), Vol. 3, No. 3, pp.191-195, (ISSN: 2141-7024), 2012, https://www.researchgate.net/publication/256029158_The_New_Fraud_Triangle_Model.
39. Kiškis, Alfredas. „Registruoto nusikalstamumo statistikos ir viktimologinių tyrimų duomenų kompleksinio panaudojimo problemos“. *Socialinių Mokslų Studijos: Mokslo Darbai = Social Sciences Studies: Research Papers* 4, no. 2 (2012): 700.
40. Lazarus, Suleman, ir Geoffrey U. Okolorie. „The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents“. *Telematics & Informatics* 40 (July 2019): 14–26. doi:10.1016/j.tele.2019.04.009, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331970.
41. Li, Xingan. „A Review of Motivations of Illegal Cyber Activities“. *Criminology & Social Integration: journal for criminology, penology and behaviour problems*, Vol. 25 No. 1, 2017: 110-126. https://doi.org/10.31299/ksi.25.1.4 https://hrcak.srce.hr/file/266976.
42. Marcinauskaitė, Renata. *Nusikalstamos veikos elektroninėje erdvėje :elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje: monografija.* Vilnius: Registrų centras, 2019.
43. Ogunleye, Yetunde O., U. Ojedokun, ir A. A. Aderinto. „Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria“. (2020). https://www.researchgate.net/publication/339941723_Pathways_and_Motivations_for_Cyber_Fraud_Involvement_among_Female_Undergraduates_of_Selected_Universities_in_South-West_Nigeria.
44. Patrick, Robert. „Florissant Man Linked to Romance Scam That Bilked Elderly Men, Women of Nearly $1 Million, Feds Say“. *St. Louis Post-Dispatch (MO)*, November 26, 2019. http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=2W64180382453&site=ehost-live.
45. Payne, Brian, Lora Hadzhidimova, ir David C. May. „America’s Most Wanted Criminals: Comparing Cybercriminals and Traditional Criminals“. *Criminal Justice Studies* 32, no. 1 (March 2019): 1–15. doi:10.1080/1478601X.2018.1532420. https://doi.org/10.1080/1478601X.2018.1532420.

46. Pinnington, Dan. „Financial Fraudsters Want You: Avoiding Scams Targeting Lawyer Trust Accounts“. *Law Practice: The Business of Practicing Law* 46, no. 5 (September 2020): 1–15. http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=145417888&site=ehost-live.
47. Popper, Nathaniel, The New York Times. „When Good Crypto Investment Goes Bad“. *Toronto Star (Canada)*, June 2, 2018. http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=6FPTS201806024609 1442&site=ehost-live.
48. Rabkin, Jeff ir kt. „Phishing for Corporate Dollars: The Emerging Global Threat Posed by Spear Phishing and Business Email Compromise“. *Venulex Legal Summaries*, July 2015, 1–6. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=110358898&site=ehost-live.
49. Rash, Wayne. „FBI Crime Report Lists Business Email Compromise as Top Scam“. *EWeek*, April 24, 2019, N.PAG. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=136100388&site=ehost-live.
50. Rash, Wayne. „Advanced Phishing Scam Targets CEOs, CFOs for Phony Cash Transfers“. *EWeek*, July 2015, 1. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=109363463&site=ehost-live.
51. Sakalauskas, Gintautas ir kt. *Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai. Teisės instituto mokslo tyrimai, 7 tomas*. Vilnius: Eugrimas, 2011.
52. Shields, Alan. „Jailed, ‘Vishing’ Fraud Pair Who Stole £360,000“. *Daily Mail*, March 9, 2019. http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=135150998&site=ehost-live.
53. Simpson, Alan. „How Scammers Track down Their Victims... Use ‘the Suckers List.’“. Daily Mail, September 6, 2014. http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=97929064&site=ehost-live.

54. Smith, Russell. „Coordinating Individual and Organisational Responses to Fraud“. *Crime, Law & Social Change* 49, no. 5 (June 2008): 379–96. doi:10.1007/s10611-008-9112-x, https://link.springer.com/article/10.1007/s10611-008-9112-x.
55. Soviany, Cristina. „The Benefits of Using Artificial Intelligence in Payment Fraud Detection: A Case Study“. *Journal of Payments Strategy & Systems* 12, no. 2 (Summer 2018): 102–10. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=bth&AN=132033184&site=ehost-live.
56. Štitilis, Darius ir kt. *Tapatybės Vagystė Elektroninėje Erdvėje: Socialiniai, Elektroninio Verslo Ir Teisinio Reguliavimo Aspektai: Kolektyvinė Mokslo Monografija*. Vilnius: Mykolo Romerio Universitetas, 2011.
57. Štitilis, Darius. *Elektroniniai nusikaltimai: metodinė priemonė*. Vilnius: Mykolo Romerio universitetas, 2011.
58. Tiwari, Milind, Adrian Gepp, ir Kuldeep Kumar. „The Future of Raising Finance - a New Opportunity to Commit Fraud: A Review of Initial Coin Offering (ICOs) Scams“. Crime, Law & Social Change 73, no. 4 (May 2020): 417–41. doi:10.1007/s10611-019-09873-2. https://www.deepdyve.com/lp/springer-journals/the-future-of-raising-finance-a-new-opportunity-to-commit-fraud-a-QCSgDt0asJ?key=springer.
59. Turton, William. „Twitter Cryptocurrency Scam Echoes Previous Schemes on YouTube“. *Bloomberg.Com*, July 23, 2020, N.PAG. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=144732153&site=ehost-live.
60. Uscila, Rokas. *Viktimologijos pagrindai*. Vilnius: Nusikalstamumo prevencijos Lietuvoje centras, 2005.
61. Vilic, Vida M. „Phishing and Pharming as Forms of Identity Theft and Identity Abuse“. *Balkan Social Science Review* 13, no. 13 (June 2019): 43–55. http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=140388562&site=ehost-live.
62. Waddell, Melanie. „Cryptocurrencies Are the ‘Mother of All Scams’: Testifying before the Senate Banking Committee, a Popular Academic Also Lays into Blockchain and Argues the ‘Real Revolution’ Is in Fintech“. *Investment Advisor*, November 2018, 1. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=132741339&site=ehost-live.
63. Weinstein, Michael. „Business Email Compromise and Wire Fraud: How to Protect Your Clients and Firm in the Year Ahead“. *National Real Estate Investor*, January 2017, 14.

http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=f5h&AN=121064686&site=ehost-live.

64. Wentz, Jennifer. „SCAMMED: As Hackers Get Smarter, Even Educated Professionals Can Fall Victim to Fraud“. *Central Penn Business Journal* 33, no. 20 (May 12, 2017): 15-22. http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=123070717&site=ehost-live.
65. Whitty, Monica T., ir Tom Buchanan. „The online dating romance scam: The psychological impact on victims - both financial and non-financial“. *Criminology & Criminal Justice* 16, no. 2 (2016): 176-194. https://heinonline-org.skaitykla.mruni.eu/HOL/Page?public=true&handle=hein.journals/crmcj16&div=13&start_page=176&collection=journals&set_as_cursor=0&men_tab=srchresults.
66. Whitty, Monica T. „The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam“. *The British Journal of Criminology*, Volume 53, Issue 4, July 2013, Pages 665–684, https://doi-org.skaitykla.mruni.eu/10.1093/bjc/azt009.
67. Whitty, Monica T, ir Tom Buchanan. „The Online Romance Scam: A Serious Cybercrime“. *Cyberpsychology, Behavior and Social Networking* 15, no. 3 (March 2012): 181–83. doi:10.1089/cyber.2011.0352. https://www.researchgate.net/publication/221805037_The_Online_Romance_Scam_A_Serious_Cybercrimehttp://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=123070717&site=ehost-live.
68. Whitty, Monica Therese. „Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims“. *European Journal on Criminal Policy & Research* 26, no. 3 (September 2020): 399–409. doi:10.1007/s10610-020-09458-z. https://www.deepdyve.com/lp/springer-journal/is-there-a-scam-for-everyone-psychologically-profiling-cyberscam-SfX3P9WJTi?key=springer.
69. Wolfe, D., ir D. Hermanson. „The Fraud Diamond: Considering the Four Elements of Fraud“. (2004). https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=2546&context=facpubs.
70. Zuhru, Fadi Abu. „The profile of a Cybercriminal“. (2016). https://www.semanticscholar.org/paper/THE-PROFILE-OF-A-CYBERCRIMINAL-ZUHRI/90a64adad75163d030214a18e9dd7897fae75101.
71. Zweighaft, David. „Business Email Compromise and Executive Impersonation: Are Financial Institutions Exposed?“. *Journal of Investment Compliance (Emerald Group)* 18,

no. 1 (January 2017): 1–7. doi:10.1108/JOIC-02-2017-0001, https://www.batesgroup.com/publications/joic-02-2017-0001.pdf.

Statistiniai duomenys

72. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, *Nusikalstamumo ir ikiteisminių tyrimų statistinės ataskaitos* (statistinės kortelės nr. 10, 20, 30, 50).
73. Jungtinės Karalystės nacionalinės statistikos biuras, *Nusikalstamumo Anglijoje ir Velse statistinės ataskaitos*: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables.
74. The world bank, *Total population data*: http://data.worldbank.org/indicator/SP.POP.TOTL/ countries/LT?display=graph.
75. Swedish National Council for Crime Prevention (Brå), *Total number of reported offences* 2019: https://www.bra.se/download/18.7d27ebd916ea64de5304e143/1585655101251/Total_number_of_reported_offences_2019.xls.
76. Survey on "Scams and fraud experienced by consumers", Contract n° 2018 85 04 under FWC CHAFEA/2017/CP/03 *Lot 1 Written by: Ipsos*, Date: January 2020: https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf.
77. Darbo užmokestis šalyje. *Oficialiosios statistikos portalas*: https://osp.stat.gov.lt/informaciniai-pranesimai?articleId=7938671.
78. Lietuvos bankas, statistinė informacija apie sukčiavimą, susijusį su investicijomis.

Kiti šaltiniai

79. „Skaitmeninės ekonomikos ir visuomenės indeksas (DESI) 2020 m. Lietuvos ataskaita". DESI. Žiūrėta 2020 m. rugsėjo 8 d. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66948.
80. „Ar veiksmingai kovojama su elektroniniais nusikaltimais?". Valstybinio audito ataskaita. Žiūrėta 2020 rugsėjo 10 d. https://www.vkontrole.lt/failas.aspx?id=4101.

81. „How criminals profit from the COVID-19 pandemic“. Europol. Žiūrėta 2020 m. rugsėjo 8 d. https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic.
82. „FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic“. FBI. Žiūrėta 2020 m. rugsėjo 19 d. https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic.
83. „2019 Internet Crime Report“. IC3. Žiūrėta 2020 m. rugsėjo 17 d. https://pdf.ic3.gov/2019_IC3Report.pdf.
84. „Lithuanian Man Arrested For Theft Of Over $100 Million In Fraudulent Email Compromise Scheme Against Multinational Internet Companies“. United States Department of Justice. Žiūrėta 2020 m. rugsėjo 17 d. https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme.
85. „Business E-Mail compromise the 12 billion dollar scam“. IC3. Žiūrėta 2020 m. rugsėjo 17 d. https://www.ic3.gov/media/2018/180712.aspx.
86. „Bank branch staff and police team up to stop £19 million of fraud in first half of 2020“. Action Fraud UK. Žiūrėta 2020 m. rugsėjo 17 d. https://www.actionfraud.police.uk/news/bank-branch-staff-and-police-team-up-to-stop-19-million-of-fraud-in-first-half-of-2020.
87. „Over £27 million reported lost to crypto and forex investment scams“. Action Fraud UK. Žiūrėta 2020 m. rugsėjo 19 d. https://www.actionfraud.police.uk/news/over-27-million-reported-lost-to-crypto-and-forex-investment-scams.
88. „Senolė pardavė butą ir sukčiam pervedė 36 000 EUR“. Teismo Vikingas. Patalpinta 2019 m. gruodžio 4 d. YouTube klipas. https://youtu.be/OGpLei1heAU.
89. „Interaktyvus SEB banko žaidimas „Pinklės“, kuris padės, suprasti labiausiai paplitusius sukčių metodus ir patars, kaip elgtis konkrečiose situacijose“. Sukčių pinklės. Žiūrėta 2020 m. rugsėjo 12 d. https://sukciupinkles.lt.
90. „Sustiprink imunitetą“, kuris moko atpažinti ir atremti grėsmes internete. Sustiprink imunitetą. Žiūrėta 2020 m. rugsėjo 13 d. https://sustiprinkimuniteta.lt.
91. Silverman, Craig. „Facebook Removed Over 2 Billion Fake Accounts, But The Problem Is Getting Worse“. *Buzzfeed news*. 2019 m. gegužės 24 d. Žiūrėta 2020 m. spalio 1 d. https://www.buzzfeednews.com/article/craigsilverman/facebook-fake-accounts-afd.
92. „Coinlore.com, list of all cryptocurrency“. Coinlore. Žiūrėta 2020 m. rugsėjo 28 d. https://www.coinlore.com/all_coins.

93. „Kas tai, ICO?“. Kriptoinfo. Žiūrėta 2020 m. rugsėjo 28 d. https://www.kriptoinfo.lt/page/kas-tai-ico.
94. „AB SEB banko bendrosios paslaugų teikimo taisyklės“. SEB bankas. Žiūrėta 2020 m. rugsėjo 28 d. https://www.seb.lt/sites/default/files/web/pdf/Bendrosios_taisykles_2017_06_12.pdf.
95. „Key Payment and Service Information“. Paypal. Žiūrėta 2020 m. spalio 1 d. https://www.paypal.com/uk/webapps/mpp/ua/servicedescription-full#6.
96. „Netikri laiškai iš „Sodros“ ir VMI galėjo būti užsienio sukčių darbas“. LRT. Žiūrėta 2020 m. spalio 1 d. https://www.lrt.lt/naujienos/verslas/4/1051818/netikri-laiskai-is-sodros-ir-vmi-galejo-buti-uzsienio-sukciu-darbas.
97. „Hook, line and sinker: Cybercrime network phishing bank credentials arrested in Romania“. Europol. Žiūrėta 2020 m. spalio 2 d. https://www.europol.europa.eu/newsroom/news/hook-line-and-sinker-cybercrime-network-phishing-bank-credentials-arrested-in-romania.
98. „Informacija apie WWW ir IP adresus“. Serveriai.lt. Žiūrėta 2020 m. spalio 1 d. https://whois.serveriai.lt/vmiparama.com.
99. „Sukčių elektroninėje erdvėje sukurtas tinklalapis, tiesiogiai skirtas dayrti nusikalstamą veiką, numatytą LR BK 182 str.“. VMI parama. Žiūrėta 2020 m. spalio 1 d. www.vmiparama.com.
100. „Sukčių elektroninėje erdvėje sukurtas, sukčiavimo, susijusio su investicijomis tinklalapis“. Immediateedge. Žiūrėta 2020 m. spalio 1 d. www.immediateedgesystem.com.
101. „Envestio has vanished. This is why“. Explorep2p. Žiūrėta 2020 m. lapkričio 29 d. https://explorep2p.com/envestio/.
102. „Internetinė pažintis su vyru baigėsi liūdnai – iš moters išviliojo virš 55 tūkst. eurų“. *Lrytas*. 2019 m. liepos 17 d. https://www.lrytas.lt/lietuvosdiena/kriminalai/2019/07/17/news/internetine-pazintis-su-vyru-baigesi-liudnai-is-moters-isviliojo-virs-55-tukst-euru-11129419/.
103. „Emkei‘s mailer“. Emkei.cz. Žiūrėta 2020 m. spalio 11 d. https://emkei.cz.
104. „SEB banko bendrosios paslaugų teikimo taisyklės“. SEB bankas. Žiūrėta 2020 m. spalio 10 d. https://www.seb.lt/sites/default/files/web/pdf/Bendrosios_taisykles_2018_08_01.pdf.
105. „Contingent Reimbursement Model Code for Authorised Push Payment Scams“. Lending standards board. Žiūrėta 2020 m. spalio 11 d. https://www.lendingstandardsboard.org.uk/wp-content/uploads/2019/05/CRM-code.pdf.

106. „App Scams Voluntary Code: Seven launch signatories to the code continue ‘no-blame’ interim funding to 31 March 2020“. UK Finance. Žiūrėta 2020 m. spalio 11 d. https://www.ukfinance.org.uk/press/press-releases/app-scams-voluntary-code-seven-launch.

107. „Ar daugės moterų IT srityje?“. VDU. Žiūrėta 2020 m. spalio 17 d. https://www.vdu.lt/lt/ar-dauges-moteru-it-srityje/.

108. Fazinni, Kate. „CFTC Settlement Shows New Era of Third Party Cyberrisk.“ *Wsj.com*. October 4, 2017. https://www.wsj.com/articles/cftc-settlement-shows-new-era-of-third-party-cyberrisk-1507151448.

109. „The internet organised crime threat assesment (IOCTA) 2016“. IOCTA. Žiūrėta 2020 m. spalio 24 d. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

110. „Europol prevencijos būdai“. Europol. Žiūrėta 2020 m. lapkričio 14 d. https://www.europol.europa.eu/sites/default/files/documents/lt_0.pdf.

111. „Subjektų, neturinčių teisės verstis investicine veikla Lietuvos Respublikoje, sąrašas“. Lietuvos bankas. Žiūrėta 2020 m. lapkričio 14 d. https://www.lb.lt/lt/subjektu-sarasas.

112. „Yet Another Ghana Scammer“. Romancescamnow.com. Žiūrėta 2020 m. lapkričio 14 d. https://romancescamsnow.com/dating-scams/scammer-becky-page/.

113. „Apgaulingas SMS žinutes siunčiantiems sukčiams SEB bankas užkirto kelią pavogti daugiau negu 116 tūkst. eurų“. SEB bankas. Žiūrėta 2020 m. lapkričio 17 d. https://www.seb.lt/naujienos/2019-09-26/apgaulingas-sms-zinutes-siunciantiems-sukciams-seb-bankas-uzkirto-kelia-pavogti.

114. „Profesionalių sukčių taktikos: pinigai nepastebimai gali keliauti metų metus“. Danske bank. Žiūrėta 2020 m. lapkričio 18 d. https://danskebank.lt/apie-banka/naujienos/2020/profesionaliu-sukciu-taktikos.

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

Augulis, J. Sukčiavimai elektroninėje erdvėje: kriminologiniai aspektai / Baudžiamosios teisės ir kriminologijos magistro darbas. Vadovas doc. dr. Alfredas Kiškis. – Vilnius: Mykolo Romerio universitetas, Baudžiamosios teisės ir proceso institutas, 2020. – 108 p.

Reikšminiai žodžiai: sukčiavimas, sukčiautojai, elektroninė erdvė, prevencija.

Pagrindinis baigiamojo darbo tikslas, ištyrus sukčiavimo elektroninėje erdvėje kriminologinius aspektus, pateikti siūlymų jų prevencijai. Pirmajame darbo skyriuje atskleidžiami teoriniai sukčiavimo elektroninėje erdvėje aspektai. Antrajame skyriuje išanalizuoti 2014-2019 m. Lietuvoje registruotų sukčiavimų elektroninėje erdvėje duomenys, juos palyginant su to pačio laikotarpio Anglijos ir Velso registruotų ir viktimologinių apklausų statistiniais tyrimo duomenimis. Trečiajame skyriuje remiantis užregistruoto sukčiavimo elektroninėje erdvėje statistiniais duomenimis bei mokslinių tyrimų medžiaga atskleista nusikaltėlių charakteristika. Ketvirtajame skyriuje remiantis užregistruoto sukčiavimo elektroninėje erdvėje statistiniais duomenimis bei mokslinių tyrimų medžiaga atskleista aukų charakteristika. Penktajame skyriuje analizuojami sukčiavimo elektroninėje erdvėje veiksniai. Šeštajame skyriuje apžvelgiami sukčiavimo elektroninėje erdvėje Lietuvoje prevencijos būdai.

Augulis, J. Cyber Fraud: Criminological Aspects / Master's Work in Criminal Law and Criminology. Supervisor: assoc. dr. Alfredas Kiškis. – Vilnius: Mykolas Romeris universitety, Criminal Law and Procedure Institute, 2020. – 108 p.

ANNOTATION IN ENGLISH

Keywords: fraud, fraudster, cyberspace, prevention

The main goal of this paper is after studying the criminological aspects of cyber fraud, to provide suggestions for their prevention. The first chapter reveals the theoretical aspects of cyber fraud. The second chapter analyzes the statistical data for period from 2014 to through 2019. Cyber fraud registered offenses data in Lithuania, comparing them with the statistical survey data of registered and victimological surveys in England and Wales during the same period. The third chapter reveals the characteristics of criminals based on the statistics of registered cyber fraud and research material. The fourth chapter analyzes the characteristics of victims based on the statistics of registered cyber fraud and the research material. The fifth chapter analyzes the factors of cyber fraud. The sixth chapter reviews the methods of cyber fraud in Lithuania.

Augulis, J. Sukčiavimai elektroninėje erdvėje: kriminologiniai aspektai / Baudžiamosios teisės ir kriminologijos magistro darbas. Vadovas doc. dr. Alfredas Kiškis. – Vilnius: Mykolo Romerio universitetas, Baudžiamosios teisės ir proceso institutas, 2020. – 108 p.

SANTRAUKA LIETUVIŲ KALBA

Sukčiavimas elektroninėje erdvėje šiuolaikinėje socialinėje terpėje yra didesnė rizika, nei bet kada anksčiau. COVID-19 pandemijos metu vis daugiau visuomenės dirbant, mokantis nuotoliniu būdu tuo suskubo pasinaudoti ir sukčiai. Sukčiavimo elektroninėje erdvėje modelių analizė, kriminologiniai asmenų charakteristikos ir veiksnių tyrimai yra svarbūs, siekiant efektyviai kontroliuoti šią nusikalstamą veiką bei atsižvelgiant į tai parengti prevencinės priemones.

Tyrimo tikslas – ištirti sukčiavimo elektroninėje erdvėje aspektus ir pateikti siūlymų jų prevencijai. Pagrindiniai uždaviniai - atskleisti teorinius sukčiavimo elektroninėje erdvėje aspektus, išanalizuoti sukčiavimo elektroninėje erdvėje nusikalstamų veikų Lietuvoje raišką 2014–2019 m., pateikti asmenų, įtariamų įvykdžius sukčiavimą elektroninėje erdvėje charakteristiką, pateikti aukų, patyrusių sukčiavimą elektroninėje erdvėje, charakteristiką, atskleisti veiksnius, nuo kurių priklauso, kodėl žmonės daro sukčiavimą elektroninėje erdvėje, apžvelgti prevencijos nuo sukčiavimo elektroninėje erdvėje metodus ir pateikti siūlymų prevencijos gerinimui.

Atlikus 2014-2019 m. užregistruoto sukčiavimo elektroninėje erdvėje Lietuvos Respublikoje bei Anglijoje ir Velse statistinių duomenų analizę buvo nustatyta, kad sukčiavimo elektroninėje erdvėje registruoto nusikalstamumo rodikliai Lietuvoje mažėjo, kai tuo tarpu Anglijoje ir Velse išliko stabilūs viso tiriamojo laikotarpio metu. Anglijos ir Velso viktimologinių tyrimų duomenys parodo, jog tik apie 14 proc. veikų buvo užregistruota teisėsaugos institucijose.

Tyrimo metu nustatyta, jog dažniausiai sukčiavimus elektroninėje erdvėje įvykdo vyrai, nukenčia irgi vyrai. Pastebėta, jog tiek kaltinamieji, tiek aukos, kurios nukentėjo dažniausiai neturi aukštojo išsilavinimo. Tyrimo metu nustatyta, jog buvo keletas aukų ir iš teisėsaugos institucijų, kas parodo, jog nuo sukčių elektroninėje erdvėje nėra apsaugotas nei vienas.

Darbą sudaro įvadas, šeši skyriai bei išvados. Pirmajame darbo skyriuje atskleidžiami teoriniai sukčiavimo elektroninėje erdvėje aspektai. Antrajame skyriuje išanalizuoti 2014-2019 m. Lietuvoje registruotų sukčiavimų elektroninėje erdvėje duomenys, juos palyginant su to pačio laikotarpio Anglijos ir Velso registruotų sukčiavimų elektroninėje erdvėje ir viktimologinių apklausų statistiniais tyrimo duomenimis. Trečiajame skyriuje remiantis užregistruoto sukčiavimo elektroninėje erdvėje statistiniais duomenimis bei mokslinių tyrimų medžiaga atskleista nusikaltėlių charakteristika. Ketvirtajame skyriuje remiantis užregistruoto sukčiavimo elektroninėje erdvėje statistiniais duomenimis bei mokslinių tyrimų medžiaga atskleista aukų

charakteristika Penktajame skyriuje analizuojami sukčiavimo elektroninėje erdvėje veiksniai. Šeštajame skyriuje apžvelgiami sukčiavimo elektroninėje erdvėje Lietuvoje prevencijos būdai.

Augulis, J. Cyber Fraud: Criminological Aspects / Master's Work in Criminal Law and Criminology. Supervisor: assoc. dr. Alfredas Kiškis. – Vilnius: Mykolas Romeris universitety, Criminal Law and Procedure Institute, 2020. – 108 p.

SUMMARY

Cyber fraud is a greater risk than ever before in today's social environment. During the COVID-19 pandemic, more and more members of the public started working remotely. Analysis of cyber fraud models, criminological research of personal characteristics and factors are important in order to effectively control this criminal act and to develop preventive measures accordingly.

The aim of the study is to investigate the aspects of cyber fraud and make suggestions for their prevention. The main tasks are to reveal the theoretical aspects of cyber fraud, to analyze the expression of cyber fraud in Lithuania from 2014 to 2019, to present the characteristics of persons suspected of cyber fraud, to present the characteristics of victims of cyber fraud, to reveal the factors on which they depend. why people commit cyber fraud, review methods of cyber fraud prevention and make suggestions for improving prevention.

After analyzing the statistics on registered cyber fraud in the Republic of Lithuania and in England and Wales from 2014 to 2019 it was revealed that registered cybercrime crime rates in Lithuania decreased, while in England and Wales they remained stable throughout the research period. In the United Kingdom, data from victimology crime survey show that only about 14% of crimes were registered with the police.

The research revealed that fraud in cyberspace is most often committed by men, men also suffer the most from it. It has been observed that both the accused and the victims who are victims usually do not have higher education. The investigation revealed that there were several victims from law enforcement agencies as well, which means that none are protected from cyber fraud in the cyber space.

The work consists introduction, six chapters and conclusion. The first chapter reveals the theoretical aspects of cyber fraud. The second chapter analyzes the statistical data for 2014-2019. Fraud offenses registered in Lithuania, comparing them with the statistical survey data of registered and victimological surveys in England and Wales during the same period. The third chapter reveals the characteristics of criminals based on the statistics of registered cyber fraud and research material. The fourth chapter analyzes the characteristics of victims based on the statistics of registered cyber fraud and the research material. The fifth chapter analyzes the factors of cyber fraud. The sixth chapter reviews the methods of cyber fraud prevention in Lithuania.

Priedas Nr. 4

Forma patvirtinta Mykolo Romerio universiteto
Senato 2012 m. lapkričio 20 d. nutarimu Nr.1SN-10

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2020-12-14
Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),
Teisės mokyklos, Baudžiamosios teisės ir proceso instituto, Baudžiamosios teisės ir kriminologijos

(fakulteto / instituto, programos pavadinimas)

Studentas (-ė) Jonas Augulis
(vardas, pavardė)

patvirtinu, kad šis magistro baigiamasis darbas „Sukčiavimai elektroninėje erdvėje: kriminologiniai aspektai“:

1. Yra atliktas savarankiškai ir sąžiningai;

2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;

3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

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

(parašas) Jonas Augulis
(vardas, pavardė)