MYKOLO ROMERIO UNIVERSITETO
TEISĖS MOKYKLOS
BAUDŽIAMOSIOS TEISĖS IR PROCESO INSTITUTAS

VLADIMIR GOLOVKO
BAUDŽIAMOJI TEISĖ IR KRIMINOLOGIJA

SUKČIAVIMO KRIMINALISTINĖS CHARAKTERISTIKOS POKYČIAI TECHNOLOGIJŲ ĮTAKOJE

Magistro baigiamasis darbas

Vadovas: prof. dr. Vidmantas Egidijus Kurapka
… … … … … …
… … … …
(parašas)

Vilnius, 2025

TURINYS

SANTRUMPŲ SĄRAŠAS

Lietuvos Respublikos baudžiamasis kodeksas – BK;

Lietuvos Respublikos baudžiamojo proceso kodeksas – BPK;

Lietuvos Aukščiausiasis Teismas – LAT;

Lietuvos Respublikos civilinis kodeksas – CK;

Integruota baudžiamojo proceso sistema – IBPS;

Internet Protocol – IP;

Inital Coin Offering – ICO;

Virtual private network – VPN;

Voice over Internet Protocol – VoIP.

ĮVADAS

Temos problema ir aktualumas:

1990 m. kovo 11 d. Lietuvos Respublikai atgavus nepriklausomybę, suvereni valstybė žengė rinkos ekonomikos keliu, kuris atvėrė plačias galimybes ekonominei plėtrai, verslumui ir naujų nuosavybės formų atsiradimui. Tačiau kartu šie pokyčiai sukūrė terpę nusikalstamoms veikoms, tarp jų ir sukčiavimui, kuris tapo viena pavojingiausių ir dažniausiai pasitaikančių nusikalstamų veikų. Per pastaruosius dešimtmečius sukčiavimo mastas ir padarymo būdai kardinaliai pasikeitė. Akivaizdu, jog šiandieniniame gyvenime informacinių technologijų ir interneto plėtra suteikė nusikaltėliams galimybę naudotis IT priemonėmis, leidžiančiomis jiems veikti vis sudėtingesniais būdais, o teisėsaugos institucijoms susidurti su iššūkiais, kurie apsunkina šios nusikalstamos veikos tyrimą. Šiuolaikinės sukčiavimo schemos daro didelę žalą ne tik nukentėjusiesiems, bet ir visuomenės pasitikėjimui teisėsaugos institucijomis. Šiandien sukčiavimas, pasitelkiantis informacinių technologijų ir interneto galimybes, yra viena sudėtingiausiai tiriamų nusikalstamų veikų. Be skaitmeninių technologijų problemos aktualumą dar labiau didina tarptautinis nusikaltimų pobūdis, nusikaltėlių tapatybės slėpimas ir dažnai pavėluota nukentėjusiųjų reakcija. Šie aspektai ne tik formuoja šiuolaikinės kriminogeninę problematiką, bet ir reikalauja naujų požiūrių bei efektyvių sprendimų[1].

Remiantis „Informatikos ir ryšių departamento“ duomenimis[2], Lietuvos Respublikoje 2020 metais užregistruota 2685 sukčiavimo atvejų (už kuriuos taikoma baudžiamoji atsakomybė), iš kurių 1656 bylos yra ištirtos. 2021 metų duomenimis užfiksuota 3169 veikų, susijusiu su sukčiavimu ir ištirta 1441 atvejis. 2022 metais užregistruota 3859 nusikalstamų veikų, iš kurių ištirta 1418 veikų. 2023 metais užfiksuota 4043 nusikalstamos veikos dėl sukčiavimo, iš kurių ištirta 1006 veikos. 2024 metais užregistruota 4800 sukčiavimo atvejų, ištirta – 1293 veikos.

[1] Ryšių reguliavimo tarnyba, Lietuvos kriminalinės policijos biuras, „Nusikaltėliai elektroninėje erdvėje: kaip sekasi juos stabdyti?“, *pristatymo skaidrės*, žiūrėta 2025 m. gruodžio 17 d., https://www.rrt.lt/wp-content/uploads/2024/10/4_NEE-kaip-sekasi-juos- stabdyti-2024-10-24-2.pdf

[2] Informatikos ir ryšių departamentas. „Sukčiavimai.“ *IRD.lt,* žiūrėta 2025 m. gruodžio 17 d. https://ird.lt/lt/atviri-duomenys/sukciavimai

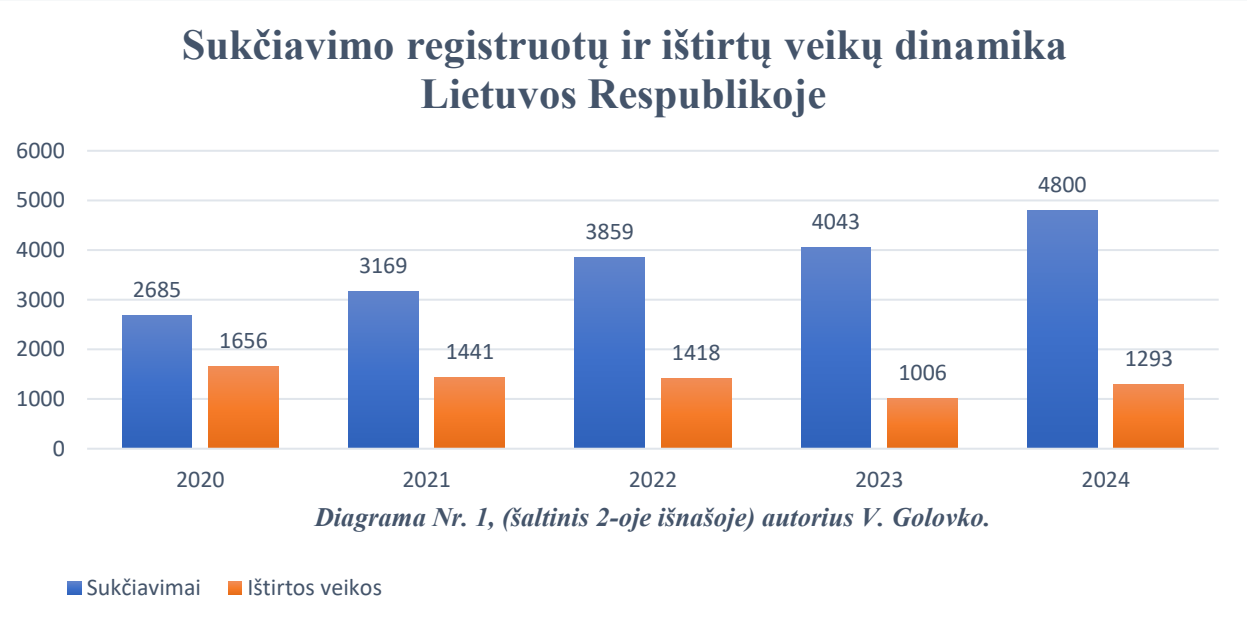


Diagrama Nr. 1, (šaltinis 2-oje išnašoje) autorius V. Golovko.

Iš pateiktų statistinių duomenų matyti, jog Lietuvos Respublikoje registruotų visų sukčiavimo atvejų skaičius kasmet sparčiai didėja, tuo tarpu nusikalstamų veikų ištyrimo rodikliai nuolat mažėja (2020 m. nuo 61,68 % – 2023 m. iki 24,88 %, 2024 m. 26,94 %). Tai rodo ne tik spartėjantį šios nusikalstamos veikos masto augimą, bet ir tai, jog sukčiavimai tampa sudėtingai tiriama nusikalstamos veikos rūšis.

Remiantis Pinigų plovimo prevencijos kompetencijų centro duomenimis[3], 2023 m. finansinių sukčių veikla ženkliai suintensyvėjo. Finansų įstaigos per šiuos metus užfiksavo daugiau nei 10 tūkst. sukčiavimo atvejų – 33 proc. daugiau nei 2022 m. Sukčių išviliotų lėšų suma, palyginti su ankstesniais metais, padidėjo 3,9 proc. ir siekė 12,3 mln. eurų. Nepaisant to, finansų institucijoms pavyko susigrąžinti beveik 900 tūkst. eurų, todėl realūs nuostoliai sudarė 11,4 mln. eurų. Analizė rodo, kad sukčiai vis dažniau naudojasi pandemijos laikotarpiu susiformavusiais gyventojų skaitmeniniais įpročiais. Jie taiko sudėtingesnes technologijas ir profesionaliai imituodami realiai atrodančias platformas, svetaines ar asmenis. 2023 m. labiausiai augo fišingo[4] (angl. phishing) ir investicinio sukčiavimo[5] atvejų skaičius. Fišingo atvejai per metus išaugo nuo 3,5 tūkst. iki 5 tūkst., tačiau dėl finansų įstaigų pastangų nuostoliai sumažėjo iki 1,6 mln. eurų. Tuo tarpu investicinis sukčiavimas, per metus padvigubėjęs iki 1,6 tūkst. atvejų, sukėlė žymiai didesnę finansinę žalą – nuostoliai siekė 4,8 mln. eurų. 2024 m. antrąjį

[3] „2023 m. finansinių sukčių aktyvumas augo trečdaliu: pasitelkė vartotojų pandeminius įpročius“, 2024 m. vasario 7 d., žiūrėta 2025 m. gruodžio 17 d., https://amlcenter.lt/2023-m-finansiniu-sukciu-aktyvumas-augo-trecdaliu-pasitelke-vartotoju-pandeminius-iprocius/

[4] „Fišingas“ *NKSC.lt*, žiūrėta 2025 m. gruodžio 17 d. https://www.nksc.lt/rekomendacijos/phishing.html

[5] Lietuvos bankų asociacija. „Investiciniai sukčiai siautėja toliau: pagrindiniai požymiai ir patarimai, kaip išvengti spąstų.“ *LBA.lt,* žiūrėta 2025 m. gruodžio 17 d. https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/investiciniai-sukciai-siauteja-toliau-pagrindiniai-pozymiai-ir-patarimai-kaip-isvengti-spastu#:~:text=%E2%80%9EInvesticinis%20suk%C4%8Diavimas%20%E2%80%93%20metodas%2C%20kuriam,pelno%20garantija%20ir%20minimalia%20rizika

ketvirtį investicinio sukčiavimo atvejų skaičius sumažėjo iki 378, palyginti su 551 užfiksuotu pirmąjį ketvirtį. Tačiau gyventojų patirti finansiniai nuostoliai dėl šio sukčiavimo metodo išaugo ir išliko didžiausi, lyginant su kitais sukčiavimo būdais. Per šį laikotarpį investiciniai sukčiai išviliojo 1,7 mln. eurų, o vidutinė vieno atvejo nuostolių suma siekė daugiau nei 4500 eurų. Šiuos duomenis papildo ir Lietuvos policijos 2024 m. stebėsenos rezultatai. Juose matyti, jog nors bendras elektroninėje erdvėje fiksuotų nusikalstamų veikų skaičius išliko stabilus, tačiau esminė ir sunkiausiai valdoma problema vis dar išlieka sukčiavimas. Net 53 % visų nusikalstamų veikų elektroninėje erdvėje sudarė sukčiavimo atvejai, o būtent – investicinis sukčiavimas, išankstinio mokėjimo (avansinis sukčiavimas) schemos, apgaulingi skambučiai, el. laiškai ir žinutės. Ypač nerimą keliantis apsektas yra ženklus apgaulingų telefoninių skambučių augimas. 2024 m., palyginti su 2023 m., tokių atvejų skaičius padidėjo net 64 %, o finansiniai nuostoliai, patirti dėl investicinio sukčiavimo didėjo toliau[6].

Šie rodikliai rodo, kad nepaisant prevencinių priemonių ir visuomenės švietimo, sukčiavimo atvejų skaičius ir jų daroma žala išlieka reikšminga problema. Tobulėjant informacinėms technologijoms ir skaitmenizuojantis visoms gyvenimo sritims, nusikalstamų veikų skaičius šioje srityje Lietuvoje, kaip ir visame pasaulyje, nuolat auga. Tikėtina, kad šis augimas tęsis ir ateityje.

Tokios tendencijos lemia tai, kad sukčiavimo mechanizmai tampa vis sudėtingesni, jų tyrimas ir atskleidimas vis labiau komplikuojasi dėl nusikaltėlių profesionalumo, maskavimosi elektroninėje erdvėje[7] ir veikimo skirtingose jurisdikcijose. Vis dažniau tokias veikas daro ne pavieniai asmenys, o organizuotos grupės (BK 25 str. 4 d.)[8], kuriose aiškiai pasiskirstę vaidmenys (aukų verbuotojai, techniniai maskuotojai, pinigų nešiotojai („kojos“) ir kt.). Tokios grupės kuria individualizuotas schemas, pritaikytas skirtingoms aukų kategorijoms pagal amžių, skaitmeninius įgūdžius, elgesio įpročius bei pasitelkia pažangias technologijas, tokias kaip dirbtinį intelektą, kriptovaliutas, suklastotas internetines svetaines ar net giliųjų klastočių technologijas (angl. Deepfakes), leidžiančias realistiškai sukurti išvaizdą ir / ar balsą, imituojant tikrus asmenis[9]. Be abejo, sukčiavimui būdingas itin aukštas latentiškumo lygis, kuris apsunkina tikrojo šio nusikaltimo masto įvertinimą. Latentiškumą lemia ne tik nukentėjusiųjų nenoras

[6] Nacionalinis kibernetinio saugumo centras. „Nacionalinė kibernetinio saugumo būklės ataskaita 2024.“ *VDAI.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d., https://vdai.lrv.lt/public/canonical/1748429329/942/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf

[7] Lietuvos Respublikos prokuratūra. „Nusikaltimai elektroninėje erdvėje.“ *Prokuraturos.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185

[8] Lietuvos policija. „Tarptautinis tyrimas atskleidė organizuotą sukčiavimo schemą.“ *Policija.lrv.lt,* žiūrėta 2025 m. gruodžio 17 d. https://policija.lrv.lt/lt/naujienos/tarptautinis-tyrimas-atskleide-organizuota-sukciavimo-schema/

[9] Nacionalinis kibernetinio saugumo centras. „Nacionalinė kibernetinio saugumo būklės ataskaita 2024.“ *VDAI.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d., 12 p.

kreiptis į teisėsaugą dėl socialinių ar psichologinių priežasčių, tokių kaip baimė, nepasitikėjimas teisėsaugos veiksmingumu ar gėdos jausmas dėl patirtos apgaulės, bet kartais ir jų nesuvokimas, jog jie tapo sukčiavimo aukomis. Be kita ko, latentiškumą didina ir teisiniai veiksniai. Dalis sukčiavimo atvejų priskiriami privačiai viešo kaltinimo byloms, todėl ikiteisminis tyrimas pradedamas tik esant nukentėjusiojo skundui ar jo teisėto atstovo pareiškimui. Pagal Lietuvos Respublikos baudžiamojo kodekso 182 straipsnio 1 ir 4 dalis, kai žala nėra itin didelė arba nėra kitų kvalifikuojančių požymių, nėra persekiojami teisėsaugos iniciatyva, o baudžiamasis procesas pradedamas tik nukentėjusiojo valia. Dėl tokios teisinės tvarkos nukentėjusieji gali nesikreipti į teisėsaugą ne tik dėl subjektyvių priežasčių, bet ir manydami, kad procesas bus pernelyg sudėtingas, ilgai trunkantis arba nepakankamai veiksmingas. Tai dar labiau apsunkina realaus sukčiavimo masto nustatymą ir jo kontrolę[10]. Prie latentiškumo prisideda ir tai, kad dėl vis inovatyvesnių sukčiavimo būdų elektroninėje erdvėje, praktikoje kartais objektyviai sunku aiškiai atriboti civilinį ginčą nuo veikos, turinčios sukčiavimo požymių. Tokiose situacijose pareiškimai gali būti vertinami kaip kylantys iš civilinių santykių arba siejami su paties nukentėjusiojo neapdairumu. Dėl šių priežasčių tikslių duomenų apie sukčiavimo mastą nustatyti nėra galimybės. Be to, apgauti asmenys kartais net nesuvokia nusikaltėlio tikrųjų ketinimų, ypač kai veika įvykdoma elektroninėje erdvėje. Tuo tarpu, dėl nukentėjusiųjų savalaikio nesikreipimo į teisėsaugą, ikiteisminio tyrimo institucijos praranda galimybę aptikti kaltininką „karštais pėdsakais“. Tai apsunkina ne tik ikiteisminio tyrimo organizavimą, bet ir veiksmingą jo atlikimą.

Tiriant tokio pobūdžio nusikalstamas veikas būtina taikyti nuoseklų metodinį pagrindą, tinkamas technines priemones, planavimą ir specialiuosius tyrimo metodus. Šiame kontekste kriminalistinė charakteristika veikia kaip pagalbinis instrumentas, leidžiantis struktūruotai nustatyti tipinius sukčiavimo požymius (būdus), numatyti tikėtinus duomenų (įrodymų) šaltinius ir formuoti tyrimo versijas. Ji ne tik sistemina duomenis apie veikos mechanizmą ir paliekamus pėdsakus, bet ir integruoja žinias iš baudžiamosios teisės, kriminalistikos, kriminologijos, psichologijos ir kitų mokslų. Toks kompleksinis požiūris užtikrina kokybiškesnį ir išsamesnį tyrimą, nes kiekviena mokslo sritis papildo bendrą nusikalstamos veikos analizę.

Nors nusikaltimų tyrimo metodika teoriniu požiūriu pradėta nagrinėti dar XIX a., kai dar austrų teisės teoretikas Hans Gross pirmą kartą pasiūlė sisteminti nusikaltimų tyrimo principus, pati sąvoka „kriminalistinė nusikaltimų charakteristika“ mokslinėje literatūroje atsirado tik XX a. šeštajame dešimtmetyje. Šis terminas įvestas Rusijos mokslininkų ir buvo

[10] Ancelis, Petras, Gediminas Bučiūnas, Marijus Šalčius, ir Rolandas Šlepetys. 2016. *Atskirų nusikalstamų veikų tyrimas: vadovėlis*. Vilnius: Registrų centras. 71 p. https://cris.mruni.eu/cris/entities/publication/30014ad7-db66-4490-ba70-082895b74b10

siekta sukurti universalią sistemą, leidžiančią struktūrizuotai tirti nusikalstamas veikas.[11] Šį universalumą lėmė to meto kontekstas, kai dauguma veikų vyko fizinėje erdvėje, o paliekami pėdsakai (įkalčiai) buvo materialūs.

Lietuvos mokslinėje doktrinoje kriminalistinės nusikalstamų veikų charakteristikos klausimai taip pat buvo nuosekliai plėtoti. Pirmiausia paminėtina Snieguolės Matulienės 2004 m. disertacija „Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija“[12], taip pat Samuelio Kuklianskio ir S. Matulienės 2002 m. mokslinis straipsnis „Kriminalistinės nusikaltimų charakteristikos samprata“[13], Eglės Kažemikaitienės ir S. Matulienės 2005 m. mokslinis straipsnis „Kriminalistinė nusikaltimų charakteristika – vienas iš kriminalinės justicijos informacinės sistemos modelio kūrimo pagrindų Lietuvoje“[14] ir kt. Šie darbai suformavo tvirtą koncepcinį pagrindą, tačiau natūralu, jog atspindi laikotarpį iki šiandieninio informacinių technologijų proveržio ir yra orientuoti į universalius kriminalistinės charakteristikos principus.

Šiandien, daugeliui nusikalstamų veikų migruojant į skaitmeninę aplinką, tarp jų ir sukčiavimui, greta vis labiau patobulintų apgaulės schemų (būdai + įrankiai) atsiveria ir duomenų (įkalčių) gavimo bei jų aptikimo kliūtys, kylančios ne iš tyrimo subjektų veiksmų, kiek dėl tarpvalstybinio bendradarbiavimo barjerų, skirtingų jurisdikcijų reikalavimų, riboto paslaugų teikėjų (pvz. kriptoturto platformos) duomenų prieinamumo ir kt. Šiame kontekste aktuali Renatos Marcinauskaitės poziciją[15]: „nereikėtų stebėtis, kad nusikalstamos veikos, iki šiol egzistavusios tik fiziniame pasaulyje, perkeltos į elektroninę erdvę įgijo „tam tikrą specifiką, atsižvelgiant į jų elektroninę formą, komunikavimo internete būdus ir interneto globalumą bei kitus specifinius elektroninės komunikacinės erdvės požymius“[16].

Vertinant šiuos pokyčius, kriminalistinė charakteristika negali būti statiška – ją būtina nuolat atnaujinti ir pritaikyti aktualijoms, kad būtų išlaikytas praktinis veiksmingumas tiek požymių atpažinimo, tiek tyrimo planavimo lygmenyse, numatant galimus tyrimo krypčių

---

[11] Matulienė, Snieguolė. 2004. *Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija*. Daktaro disertacija, Mykolo Romerio universitetas. 4 p., https://cris.mruni.eu/cris/entities/etd/debef03a-a96a-4aad-b47c-6bf84efc5c12

[12] Ibid.

[13] Kuklianskis, Samuelis, ir Snieguolė Matulienė. 2002. „Kriminalistinės nusikaltimų charakteristikos samprata.“ *Jurisprudencija* 29(21). https://ojs.mruni.eu/ojs/jurisprudence/article/view/3581

[14] Kažemikaitienė, Eglė, ir Snieguolė Matulienė. 2005. „Kriminalistinė nusikaltimų charakteristika – vienas iš kriminalinės justicijos informacinės sistemos modelio kūrimo pagrindų Lietuvoje.“ *Jurisprudencija* 65(57). https://ojs.mruni.eu/ojs/jurisprudence/article/view/3108

[15] Marcinauskaitė, Renata. 2019. *Nusikalstamos veikos elektroninėje erdvėje: elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje: monografija*. Vilnius: Registrų centras. 37 p., https://cris.mruni.eu/cris/entities/publication/c9e5a17d-3878-4db2-ae66-89f31fb5bbc5

[16] Štitilis, Darius, *Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos:* daktaro disertacija: socialiniai mokslai, teisė (01 S), Vilnius, 2002, 19 p., cituota iš R. Marcinauskaitė *Nusikalstamos veikos elektroninėje erdvėje: elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje*. 37 p.,

scenarijus bei kliūtis. Todėl, nacionalinėje mokslinėje doktrinoje išryškėja poreikis atnaujintam požiūriui, pritaikytam šiuolaikiniams sukčiavimo elektroninėje erdvėje būdams.

Remiantis aukščiau išdėstytu, atnaujinta kriminalistinė charakteristika ne tik prisidės prie nusikaltimo tyrimo proceso efektyvumo, bet ir stiprins teisėsaugos institucijų gebėjimą reaguoti į kintančias nusikaltimų formas elektroninėje erdvėje, kur tradiciniai tyrimo metodai gali būti nepakankami. Teigtina, jog kriminalistinė charakteristika tampa svarbiu teoriniu ir praktiniu pagrindu, be kurio sudėtingi nusikaltimai, tokie kaip sukčiavimai elektroninėje erdvėje, negalėtų būti efektyviai tiriami.

Baigiamojo darbo mokslinis naujumas ir tiriamos problemos ištyrimo lygis:

Baigiamojo darbo mokslinis naujumas pasireiškia tuo, kad sukčiavimas elektroninėje erdvėje analizuojamas per kriminalistinės charakteristikos prizmę, atskleidžiant technologinių pokyčių įtaką veikos mechanizmui, pėdsakų šaltiniams, tipinėms tyrimo situacijoms ir tyrimo planavimui. Darbe analizuojami šiuolaikiniai sukčiavimo modeliai, jų realizavimo būdai ir su tuo susiję tyrimo sunkumai. Tiriamos problemos ištyrimo lygis yra visą laiką dinamikoje ir laikytinas aktualiu, nes dėl nuolat kintančių sukčiavimo schemų išlieka poreikis sistemiškai apibendrinti šiuos pokyčius ir jų reikšmę kriminalistinei analizei. Šio darbo autoriaus panaudoti viešai prieinami ir moksliniai šaltiniai (plačiau žr. tiriamąją darbo dalį), tame tarpe disertacinio lygmens, gali ne visuomet atspindėti sparčiai kintančius technologinius pokyčius, tačiau tai nereiškia, jog kriminalistikos mokslininkai pralaimi „lenktynėse“ su kriminaliniu pasauliu. Darbe remiamasi doktrina, teisės normomis, ikiteisminio tyrimo praktikos pavyzdžiais ir ekspertinių interviu įžvalgomis, kas leidžia pagrįsti praktinio taikymo išvadas.

Baigiamojo darbo reikšmė:

Šio baigiamojo darbo reikšmė pasireiškia tuo, kad jame sisteminami šiuolaikinio sukčiavimo (elektroninėje erdvėje) kriminalistinės charakteristikos pokyčiai technologijų įtakoje ir atskleidžiama jų reikšmė sukčiavimo kvalifikavimui bei ikiteisminio tyrimo organizavimui. Šios srities tyrimai yra būtini siekiant suprasti naujas nusikalstamo elgesio formas ir parengti kovos su jomis priemones. Darbą galima naudoti studijų procese bei keliant teisėsaugos pareigūnų kvalifikaciją.

Tikslas:

Šio baigiamojo darbo tikslas yra atskleisti sukčiavimo kriminalistinės charakteristikos pokyčius technologijų įtakoje, įvertinti šių pokyčių reikšmę sukčiavimo kvalifikavimui ir ikiteisminio

tyrimo organizavimui, bei pateikti kryptingas tyrimo tobulinimo ir prevencijos stiprinimo įžvalgas.

Uždaviniai:

1. Išnagrinėti kriminalistikos ir sukčiavimo tyrimo metodikų istorinę raidą, nustatyti pagrindinius jų raidos etapus bei jų reikšmę šiuolaikinėms sukčiavimo tyrimo metodikoms.
2. Įvertinti šiuolaikinio sukčiavimo elektroninėje erdvėje baudžiamąją teisinę ir kriminalistinę charakteristiką, atskleidžiant sukčiavimo sudėties ir kriminalistinės charakteristikos elementų tarpusavio ryšį bei jų reikšmę veikos kvalifikavimui ir tyrimui.
3. Ištirti naujausius sukčiavimo elektroninėje erdvėje metodus, atsirandančius dėl technologinės pažangos, socialinių tinklų populiarumo, dirbtinio intelekto ir kitų veiksnių.
4. Atskleisti sukčiavimo elektroninėje erdvėje tyrimų ypatumus, nustatyti tipines situacijas, būdingas tyrimo kryptis, dažniausiai pasitaikančias kliūtis bei pateikti kriminalistinius šių nusikalstamų veikų tyrimo tobulinimo pasiūlymus.
5. Įvertinti sukčiavimo elektroninėje erdvėje plėtros tendencijas ir nustatyti pagrindines prevencijos kryptis, analizuojant taikomų priemonių veiksmingumą bei jų sąveiką su kintančiais sukčiavimo modeliais, pateikti įžvalgas dėl šių problemų sprendimo būdus.

Tyrimo objektas:

Objektas yra sukčiavimo kriminalistinė elektroninėje erdvėje charakteristika jos kaita technologinių pokyčių kontekste. Tyrimas apima skirtingų sukčiavimo elektroninėje erdvėje formų analizę, siekiant išskirti joms būdingus bruožus ir atskleisti, kaip technologiniai veiksniai keičia kriminalistinės charakteristikos elementus bei jų pritaikomumą tiriant sukčiavimą.

Tyrimo metodai:

Darbe taikytas kompleksinis tyrimo metodų derinys. Naudotas istorinis metodas, leidęs aptarti kriminalistikos ir sukčiavimo tyrimo metodikų raidą. Taikytas teisės aktų sisteminės analizės metodas, vertinant sukčiavimo elektroninėje erdvėje kvalifikavimo ir susijusių nusikalstamų veikų reguliavimą, taip pat teismų praktikos analizės metodas, nustatant teismų formuojamus kvalifikavimo kriterijus. Šiuolaikinių sukčiavimo modelių mechanizmams ir technologiniams aspektams atskleisti taikyta mokslinės literatūros ir analitinių šaltinių analizė bei lyginamasis metodas, lyginant skirtingus sukčiavimo būdus. Praktiniams tyrimo ypatumams įvertinti naudota empirinių duomenų analizė ir ekspertų apklausos metodas. Išvadoms ir pasiūlymams

suformuluoti taikytas apibendrinimo metodas. Šis darbas taip pat rengtas remiantis autoriaus profesine patirtimi prokuratūroje. Profesinė veikla šioje institucijoje sudarė sąlygas gilinti nagrinėjamos problematikos supratimą per tikslinius mokymus, prieigą prie informacinių šaltinių ir praktinių įrankių (pvz., Infolex, IBPS), taip pat per profesinį bendravimą su prokurorais, aptariant aktualius su sukčiavimo elektroninėje erdvėje susijusius klausimus. Šios aplinkybės prisidėjo prie tyrimo analizės argumentacijos nuoseklumo bei suformuluotų išvadų ir pasiūlymų pagrįstumo.

Tyrimo struktūra:

Magistro baigiamasis darbas sudarytas iš santrumpų sąrašo, įvado, keturių skyrių, išvadų ir pasiūlymų, literatūros sąrašo, priedų, santraukos lietuvių ir anglų kalbomis. Pirmajame skyriuje nagrinėjama kriminalistikos ir sukčiavimo tyrimo metodikų istorinė raida, atskleidžiant pagrindinius kriminalistikos formavimosi etapus ir sukčiavimo tyrimo metodikų raidą nuo ankstyvųjų laikotarpių iki šiuolaikinio kriminalistikos mokslo susiformavimo. Antrajame skyriuje analizuojamos šiuolaikinės sukčiavimo baudžiamosios teisinės ir kriminalistinės charakteristikos. Pirmajame šio skyriaus poskyryje nagrinėjamas sukčiavimo teisinis 11 reguliavimas ir kvalifikavimo aspektai, o antrajame sukčiavimo kriminalistinė charakteristika, išskiriant nusikalstamos veikos dalyką, padarymo būdus, naudojamus įrankius ir priemones. Trečiajame skyriuje analizuojami sukčiavimo elektroninėje erdvėje tyrimo ypatumai. Jame nagrinėjama ikiteisminio tyrimo pradžia ir pagrindiniai duomenų šaltiniai, tipinės tyrimo situacijos, tyrimo kryptys ir dažniausiai pasitaikančios kliūtys, taip pat analizuojamas aukos ir kaltininko portretas kaip kriminalistinės charakteristikos elementų sudedamoji dalis. Ketvirtajame skyriuje aptariamos sukčiavimo elektroninėje erdvėje plėtros tendencijos ir pagrindinės prevencijos kryptys, vertinant taikomų priemonių veiksmingumą ir jų sąveiką su kintančiais sukčiavimo modeliais. Darbo pabaigoje pateikiamos išvados ir pasiūlymai, apibendrinantys atlikto tyrimo rezultatus ir suformuluojantys kriminalistinius sukčiavimo elektroninėje erdvėje tyrimo ir prevencijos tobulinimo aspektus.

Ginamieji teiginiai:

- Technologijos nuolat vystosi, todėl atsiranda naujos sukčiavimo elektroninėje erdvėje priemonės ir didėja padarymo būdų įvairovė, o tai turi lemiamos įtakos ikiteisminio tyrimo efektyvumui.
- Sukčiavimo kriminalistinės charakteristikos atspindi plačių technologinių pokyčių įtaką, o jų supratimas yra būtinas efektyvioms sukčiavimo prevencijos ir tyrimo priemonėms parinkti.

1. KRIMINALISTIKOS IR SUKČIAVIMO TYRIMO METODIKŲ ISTORINĖ RAIDA

Nusikalstamumas kaip socialinis reiškinys buvo paplitęs dar Senovės Romos laikais. Ši civilizacija garsėja ne tik savo išsivysčiusia teisės sistema, bet ir išradingais nusikaltimų tyrimo būdais. Tokios nusikalstamos veikos kaip vagystės, plėšimai, vynų, juvelyrinių dirbinių, monetų ir kvepalų padirbinėjimas buvo laikytina įprasta praktika. Veikos susijusios su apgaule, kaip būdas neteisėtai užvaldyti svetimą turtą buvo žinomas dar Senovės Romos įstatymų leidėjais, kurie net aiškiai apibrėžė sukčiavimo sąvoką ir išskyrė jo rūšis.[17] Pavyzdžiui, tiriant monetų padirbinėjimus, Romos imperatorius Aleksandras Severas įsteigė specialią tarnybą klastotėms aptikti, o pastarieji atlikdavo pilnavertes ekspertizes, kuriu metu nustatydavo priemaišų kiekį aukse. Tiriant nužudymus, gydytojai apsiribodavo lavonų apžiūra ir pateikdavo išvadas, kadangi Senovės Romoje, kaip ir daugelyje kitų senovės civilizacijų autopsija buvo vertinama kaip nepagarba mirusiajam ir už ją galėjo būti taikomos griežtos bausmės. Apklausos, kratos ir nusikaltėlių atpažinimas buvo minimi jau tokiuose ankstyvuosiuose religiniuose tekstuose kaip Senasis ir Naujasis Testamentas, Avesta, Koranas bei Senovės Romos, Kinijos, Graikijos, Vokietijos, Prancūzijos ir kitų šalių teisiniuose paminkluose. Žinoma, šios priemonės buvo grindžiamos gyvenimiška patirtimi ir taikytos pagal tuo metu galiojusias teisines procedūras.[18] Vis dėlto iki XIX a. pradžios techniniai klausimai, kylantys tyrimo metu, dažniausiai buvo sprendžiami remiantis praktine patirtimi ir elementaria logika. Be abejo, senoviniais laikais tyrė nusikalstamas veikas, tačiau tuo metu nebuvo koncepcijų, rekomendacijų ir apskritai mokslo, kaip pagalbinės metodikos nusikaltimams atskleisti ir jų išaiškinti.

Tik XIX a., sparčiai augant nusikalstamumui, kuris vis dažniau pasinaudodavo naujausiais technikos išradimais, buvo imtasi priemonių, siekiant pagerinti nusikaltimų tyrimo metodus. Tam reikėjo nuodugniai analizuoti nusikaltimų padarymo būdus, įtraukti įvairių sričių specialistus ir ekspertus bei taikyti mokslinį požiūrį į tyrimo procesą[19]. Šios pastangos labiausiai išsivysčiusiose kapitalistinėse valstybėse padėjo pagrindus naujam mokslui – kriminalistikai. Kriminalistikos kaip mokslo pradininku laikomas austrų kriminalistas Hans Gustav Adolf Gross, kuris vienas pirmųjų atkreipė dėmesį į daiktinius įrodymus atskleidžiant nusikaltimus, į

[17]Международный журнал *Молодой ученый*. Часть 3, Казань 2017 m. 210 p. https://moluch.ru/archive/153/43409/

[18]Ищенко, Е. П., и А. А. Топорков. 2006. *Криминалистика: учебник*. 2-е изд. Москва: Юнити-Дана. 3, https://ru.scribd.com/document/486830669/%D0%98%D1%89%D0%B5%D0%BD%D0%BA%D0%BE-%D0%95-%D0%9F-%D0%A2%D0%BE%D0%BF%D0%BE%D1%80%D0%BA%D0%BE%D0%B2-%D0%90-%D0%90-%D0%9A%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0-pdf

[19] Яблоков, Н. П., ред. 2005. *Криминалистика: учебник*. 3-е изд., перераб. и доп. Москва: Юристъ. 39 p., http://koldin-msu.ru/wp-content/uploads/2015/03/Учебник-классический-2005.pdf

mokslinių ir techninių priemonių bei gamtos mokslų metodų naudojimą jiems atskleisti ir tirti. H. Gross 1892 m. parašė veikalą „Teismo tardytojų vadovas kaip kriminalistikos sistema“. Remdamasis moksline analize ir iki tol sukauptos kriminalistiškai svarbios informacijos apibendrinimu, jis paskelbė, kad gimsta naujas savarankiškas mokslas, kurį jis pavadino kriminalistika. Pasak žymaus vokiečių publicisto Jurgen Torwald, kriminalistika kaip mokslas galutinai susiformavo XIX a. antrojoje pusėje, nors pirmieji kriminalistiniai tyrimai buvo atliekami gerokai ankščiau[20]. Pavyzdžiui, dar 1838-1841 m. Frankfurte, Vokietijoje, vokiečių procesualistas Ludwigas von Jagemann išleido dviejų tomų veikalą „Teisminio tyrimo vadovas“, kuriame, remdamasis to meto tyrimo praktikos analize, išdėstė idėjas, kaip tobulinti nusikaltimų tyrimą. Visų pirma jis pagrindė būtinybę užtikrinti, kad tyrimas būtų griežtai sistemingas ir aiškiai metodologiškai suprantamas ir pateikė atitinkamus pasiūlymus. Nors L. Jagemannui nepavyko įgyvendinti savo idėjų dėl tyrimo tobulinimo, tačiau neabejotina, jog šis darbas buvo svarbus kriminalistikos priešistorės etapas, kadangi šios publikacijos padėjo pagrindus mokslui apie tyrimo veiksmų taktiką, apimančią apžiūrą, kratą ir apklausą. Taigi būtent Hans Gross pripažįstamas neginčijamu kriminalistikos kaip savarankiško mokslo pradininku, nors ir iki jo veikalo pasirodymo buvo atlikta nemažai tyrimų ir paskelbta darbų, turėjusių esminę kriminalistinę reikšmę[21]. Vakarų Europos šalyse kriminalistikos mokslas atsirado ir tobulėjo pirmiausia kaip taikomoji, techninė disciplina (techninio tyrimo aspektas), apibendrinanti teisės aktais nereglamentuotą policijos veiklą, kuri atsispindėjo A. Bertillono, E. Locardo, R. A. Reisso ir F. Galtono darbuose.[22] Plėtojant kriminalistikos mokslo raidą XX a., kriminalistikos metodikos buvo ne tik stiprinamos ir tobulinamos, bet ir tapo itin svarbios tarptautiniame kontekste, kai Vakarų Europos šalys pradėjo aktyviai bendradarbiauti nusikaltimų tyrimo srityje.

Tarpukario laikotarpis Lietuvoje buvo vienas iš kertinių šalies istorijos etapų, sutapęs su nepriklausomybės atkūrimu ir valstybinės institucijų sistemos kūrimu. Tuo metu vyko intensyvus socialinis ir ekonominis modernizavimas, kurio tikslas buvo įveikti Pirmojo pasaulinio karo ir Nepriklausomybės kovų padarinius. Tačiau kartu šis laikotarpis išryškino ir nemažai socialinių bei ekonominių problemų, kurios sudarė palankias sąlygas kai kuriems visuomenės sluoksniams įsitraukti į neteisėtą veiklą. Kadangi tuo laikotarpiu net 80-90 % Lietuvos gyventojų gyveno kaimuose, būtent kaimo gyventojų nusikalstamumas formavo bendrą nusikalstamumo lygį visoje

[20]Torvaldas, J. *Kriminalistikos keliai ir klystkeliai*. Vilnius: Mintis, 1981. cituota iš: Kurapka, Vidmantas Egidijus, ir Snieguolė Matulienė, red. 2012. *Kriminalistika: teorija ir technika: vadovėlis*. Vilnius: Mykolo Romerio universitetas. 10 p., https://cris.mruni.eu/cris/entities/publication/bf3791d3-497c-465a-8665-db859f50ed8d

[21]11. Г. Гросс. 2002. *Руководство для судебных следователей как система криминалистики*. Москва: Юридическая литература.

[22] Ищенко, Е. П., и А. А. Топорков. 2006. Криминалистика: учебник. 2-е изд. Москва: Юнити-Дана. 14 p.

valstybėje. Kaimuose vyravę nusikaltimai dažniausiai kilo iš vietos gyventojų kasdienybės realijų, todėl šiuo laikotarpiu dominavo vadinamasis „kaimiško tipo“ nusikalstamumas.[23].

Metai	Vagystės	Kūno sužalojimai	Slapti degtinės varymai	Gyvybės atėmimo atvejai	Plėšimai	Iššaginimai
1931	10 609	2657	1562	389	131	65
1932	14 378	3225	1255	400	184	60
1933	17 926	3709	1092	498	294	86
1934	20 315	4307	1054	472	284	85
1935	17 054	4742	1848	453	167	91
1936	19 390	5467	2425	549	243	99
1937	19 663	5104	1437	437	285	101
1938	18 849	5557	1598	418	262	79

Lentelė Nr. 1, Nusikalstamumo rodikliai Lietuvoje 1931-1938 m., autoriai G. Babachinaitė, V. Paulikas (Nedarbas ir nusikalstamumas Lietuvos kaime 1918-1990 m., Jurisprudencija, 2002 m., 111 p.)

Nagrinėjant mokslinę literatūrą[24], ir statistinius duomenis apie tarpukario nusikalstamumą Lietuvoje, matyti, jog išskiriamos tokios veikos kaip vagystės, plėšimai, žmogžudystės, seksualiniai nusikaltimai ir kt. Kalbant apie sukčiavimus tarpukario Lietuvoje, jie buvo mažiau pastebimi. Tuo metu visuomenės ir spaudos dėmesys daugiausia krypo į labiau matomas nelegalios ekonomikos formas, kaip spekuliacija, kontrabanda ar nelegali degtindarystė. Šie reiškiniai buvo laikomi tiesiogine grėsme visuomenės interesams. Pavyzdžiui, sprendžiant slaptos degtindarystės problemą, siekta ne tik užkirsti kelią alkoholizmo plitimui[25], kuris buvo siejamas su išaugusiu nusikalstamumu, bet ir sumažinti šio reiškinio neigiamą poveikį šalies ekonomikai. Dėl to kovai su šiomis problemomis buvo skiriamas didesnis dėmesys, naudojant propagandines kampanijas ir baudžiamąsias priemones[26].

Nors sukčiavimui tarpukario Lietuvoje buvo skiriama mažiau dėmesio, tai nereiškia, kad tokio pobūdžio nusikaltimų nebuvo. Sukčiavimas buvo paplitęs prekybos ir paslaugų

[23] Kiškis, Alfredas. 2017. *Lietuvos kriminologijos raida, 1918–2017 m.: šimtmečio patirtis. Monografija.* Vilnius: Mykolo Romerio universitetas. 11 p., https://cris.mruni.eu/cris/entities/publication/8ea3640d-4ae4-4843-b84d-7c3cb9a7b104

[24] Babachinaitė, Genovaitė, ir Vygandas Paulikas. 2002. „Nedarbas ir nusikalstamumas Lietuvos kaime 1918–1990 m.“ *Jurisprudencija* 26(18): 111 p. https://ojs.mruni.eu/ojs/jurisprudence/article/view/3632

[25] „Tinklalaidė „Ko tyli istorikai?“: nusikaltimai tarpukariu.“ *Bernardinai.lt*, žiūrėta 2025 m. gruodžio 17 d. https://www.bernardinai.lt/tinklalaide-ko-tyli-istorikai-nusikaltimai-tarpukariu/

[26] Indrišionis, Darius. 2020. „Nelegalių ekonominių veiklų ir kovos su jomis vaizdiniai lietuviškoje spaudoje 1938–1940 metais.“ *Lietuvos istorijos studijos* 46: https://www.zurnalai.vu.lt/lietuvos-istorijos-studijos/article/view/22254

sektoriuose, o viena iš sričių, kur jis pasireikšdavo dažniau yra fotografijos verslas[27]. Viena iš dažniausių to meto sukčiavimo formų buvo fiktyvių adresų naudojimas registruojant veiklą, siekiant išvengti atsakomybės už mokesčių nemokėjimą. Tokį metodą dažniausiai taikė klajojantys arba neturintys nuolatinės darbo vietos fotografai. Kita paplitusi sukčiavimo forma buvo nelegalus darbas. Tokie asmenys vykdė veiklą be reikiamų leidimų ir apgaulingai nemokėjo pajamų mokesčių. Šių pažeidimų nustatymą apsunkindavo ne tik pačių fotografų slapstymasis, bet ir nepakankamai efektyvi to meto mokesčių kontrolės sistema bei retai atliekami inspekcijų patikrinimai. Nepaisant žinomų sukčiavimo praktikų, mokesčių inspekcija retai imdavosi efektyvių priemonių, o nesumokėti mokesčiai dažnai būdavo nurašomi kaip beviltiški.

Tarpukariu Lietuvos kriminalistika buvo ankstyvojoje raidos stadijoje ir kaip mokslas nacionaliniame lygyje dar nebuvo pakankamai išvystytas. Mokslinių darbų beveik nebuvo, o visas dėmesys buvo koncentruotas į sparčiai augančio nusikalstamumo kontrolę ir prevenciją. Pirmieji kriminalistikos raidos žingsniai Lietuvoje tiesiogiai susiję su policijos sistemos kūrimu, atskirų jos tarnybų veikla ir šios veiklos tobulinimu. Kriminalistikos institucijų užuomazgos siejamos su 1918-10-27, kai pradėti organizuoti pirmieji kriminalinės policijos, tuo metu vadintos milicija, padaliniai. Kadangi kriminalinės policijos darbuotojai buvo įvairių tautybių ir nė vienas nemokėjo lietuvių kalbos, pradžioje visi kriminalinio skyriaus dokumentai ir įsakymai buvo rašomi rusų kalba. Tik nuo 1919 m. vidurio jie pradėti rengti lietuviškai, taip atspindint naujai kuriamos valstybės kalbos politikos kaitą. Šiuo laikotarpiu kriminalinės policijos darbo sąlygos buvo itin sudėtingos. Karas smarkiai nualino šalį, demoralizavo visuomenę, o nusikalstamumas augo – daugėjo vagysčių, plėšimų ir žmogžudysčių. Vagys drąsiai veikė net atvirai, dažnai savininkų akivaizdoje ir be jokios baimės pardavinėjo pagrobtus daiktus. Nusikaltėliai dažnai veikė organizuotai, didelėmis gaujomis, o žmonės taip bijojo, kad vengdavo pranešti milicijai. Kriminalinė milicija neturėjo nei pakankamų priemonių, nei parengtų specialistų, nebuvo sudarytų nusikaltėlių sąrašų, albumų, registracijos sistemų, nebuvo aišku, kiek ir kokių recidyvistų veikia šalyje. Trūko fotoaparatų, specialiai apmokytų pėdsekių šunų, agentūros – viskam trūko lėšų. Finansavimas, kurį policijai teikė savivaldybės, buvo menkas, nes ir jos pačios dar tik kūrėsi ir negalėjo suteikti reikalingos paramos pagal to meto situacijos poreikius[28]. Iki 1920-02-07 kriminalinė milicija veikė kaip Piliečių apsaugos departamento padalinys. Ši data laikoma kriminalinės policijos reorganizavimo pradžia – tuomet įkurtas

[27] Kaminskas, Mindaugas. 2006. Kauno komercinė fotografija 1918–1940. *Panevėžio praeities: fotografijos kontekstas ir paveldas*. Panevėžys: Panevėžio kraštotyros muziejus. 66-67 p., http://www.paneveziomuziejus.lt/files/krasto_istorija/Kaminskas_Kauno_komercin_fotografija_1918_1940.pdf

[28] Palskys, Eugenijus. 1995. Lietuvos kriminalistikos istorijos apybraižos (1918–1940): monografinė studija. Vilnius: Lietuvos policijos akademija. 9 p., https://cris.mruni.eu/cris/entities/publication/c965eb93-d112-4c4a-972e-44b1d71a65ab

savarankiškas Milicijos departamentas, kuriam vadovavo P. Sližys. Tais pačiais metais, rugsėjo 1 d., įsteigtas Lietuvos kriminalinės milicijos centro biuras, tapęs svarbia kriminalinės policijos institucija[29].

Palaipsniui, siekiant gerinti būsimų policijos pareigūnų ir teisininkų rengimą, praėjus daugiau kaip dešimtmečiui, t. y. 1931 m., Kauno universitete pradėtas dėstyti kriminalistikos kursas. Be to, kriminalistikos, fotografijos, ginklų ir šaudymo mokymai buvo organizuojami ir Kauno policijos mokykloje. 1935 m. Valstybės saugumo departamentas inicijavo žurnalo „Kriminalistikos žinynas“ [30] leidybą. Šiame leidinyje buvo nagrinėjamos nusikalstamumo problemos, pristatomi naujausi kriminalinės technikos sprendimai ir nusikaltimų tyrimo metodai. Prie žurnalo turinio kūrimo prisidėjo tokie mokslininkai kaip prof. J. Vabalas-Gudaitis, kuris, analizavo kriminalinės psichologijos klausimus, prof. K. Oželis, kuris tyrinėjo teismo medicinos problemas, ir kiti. Žurnale taip pat buvo sprendžiamos praktinės kriminalistikos problemos, tokios kaip suklastotų dokumentų, šaunamųjų ginklų, kraujo pėdsakų, plaukų tyrimai. Vis dėlto kartu su pažangiomis idėjomis buvo pateikiama ir moksliškai, nors ir nepagrįstų teorijų. Kai kurie autoriai bandė įrodyti, kad žmogaus charakterį galima nuspėti pagal kūno sudėjimą, svarstė hipnozės vaidmenį nusikalstamumo kontekste, rėmėsi įgimto nusikaltėlio teorija. Buvo propaguojamos ir sterilizacijos bei kastracijos idėjos kaip nusikalstamumo prevencijos priemonės. Be to, atskiri straipsniai kriminalistikos temomis buvo publikuojami ir Kauno universiteto Teisės fakulteto moksliniuose darbuose.

Taigi atsižvelgiant į ribotus istorinius ir mokslinius šaltinius, nagrinėjančius sukčiavimo formas tarpukario Lietuvoje, galima daryti prielaidą, jog šie reiškiniai turėjo panašumų su tuo metu kitose valstybėse fiksuotais sukčiavimo modeliais. Kadangi šiuolaikinės sukčiavimo tendencijos Lietuvoje dažnai atitinka globalius metodus ir mechanizmus, tikėtina, kad panaši tarptautinė tendencija egzistavo ir tarpukariu. Nepaisant informacijos stokos, galima manyti, jog tarpukario Lietuvoje taikyti sukčiavimo būdai buvo artimi tiems, kurie buvo paplitę kitose valstybėse, išsivadavusiose iš Rusijos imperijos, vėliau įtrauktose į SSRS sudėtį arba artimoje geopolitinėje aplinkoje. Vis dėlto darant tokią prielaidą būtina atsižvelgti į tuo metu egzistavusius kriminalistikos išsivystymo skirtumus tarp valstybių. Pavyzdžiui, Sovietų Sąjungoje kriminalistikos mokslas buvo labiau išvystytas – plačiau taikytos ekspertizės, efektyviau veikė nusikaltėlių registracija, aktyviau dirbo specializuoti kriminalistai ir teismo ekspertai. Tuo tarpu tarpukario Lietuvoje šių priemonių plėtra dar tik prasidėjo, atitinkamai, tyrimų kokybė ir galimybės buvo ribotos dėl menkų institucinių resursų ir technologinių

[29] Lietuvos kriminalinės policijos biuras. „Kriminalinės policijos istorija.“ *LKPB.policija.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d. https://lkpb.policija.lrv.lt/lt/apie-mus/kriminalines-policijos-istorija/

[30] *Kriminalistikos žinynas* / redaktorius A. Povilaitis. - 1935-1940 - 1940-Nr.31, https://www.epaveldas.lt/preview?id=C10000221382-1940-Nr.31

pajėgumų. Todėl galima teigti, kad nors sukčiavimo būdai galėjo būti panašūs, jų tyrimo efektyvumas bei taikytos metodikos ženkliai skyrėsi. Vis dėlto, nepaisant dažnai kritikuotos tarpukario Lietuvos teisėsaugos veiklos, pastarųjų metų moksliniai tyrimai rodo, kad kriminalistikos mokslas tuo laikotarpiu buvo vystomas kryptingai, atsižvelgiant į konkrečius vietos poreikius ir galimybes[31].

Šiuolaikinio sukčiavimo kontekste akcentuotina, kad, pavyzdžiui, 2001 m. vadovėlyje „Kriminalistika“[32] sukčiavimas kaip nusikalstama veika metodologiškai pirmiausia buvo priskiriamas nusikaltimams nuosavybei ir analizuojamas atitinkamame skyriuje „Nusikaltimų nuosavybei tyrimas“. Kiti vadovėlio skyriai, tokie kaip „Organizuotų nusikalstamų bendruomenių padarytų nusikaltimų tyrimo ypatumai“, „Nusikaltimų kompiuterinės informacijos srityje tyrimo ypatumai“ bei „Užsieniečių padarytų nusikaltimų ir nusikaltimų prieš užsieniečius tyrimo ypatumai“, buvo skirti savarankiškoms nusikalstamų veikų kategorijoms. Toks metodinis skirstymas atspindėjo to laikotarpio nusikalstamumo specifiką ir technologinį kontekstą, kai sukčiavimas iš esmės buvo vykdomas tradicinėje, fizinėje erdvėje, neturėjo ryškaus tarptautinio elemento, o informacinės technologijos dar nebuvo tapusios pagrindine šios veikos terpe. Todėl tuo metu sukčiavimo kriminalistinė charakteristika, palyginus su šiandienėmis realijomis, buvo vertinama siauriau, t. y. orientuojantis į nuosavybinio kėsinimosi esmę ir apgaulės mechanizmą. Panašus metodikų atskyrimas išlieka ir vėlesnėje kriminalistikos doktrinoje. Pavyzdžiui, 2013 m. Mykolo Romerio universiteto vadovėlyje „Kriminalistika: taktika ir metodika“[33] sukčiavimas nagrinėjamas kaip atskira nusikalstamų veikų tyrimo metodika, o greta pateikiamos ir kitos savarankiškos metodikos, susijusios su kompiuterinių nusikaltimų tyrimu bei organizuotų grupuočių padarytų nusikalstamų veikų tyrimu. Tačiau šiuolaikinių technologijų plėtra iš esmės pakeitė sukčiavimo pobūdį. Šiandien sukčiavimas dažnai vykdomas elektroninėje erdvėje, pasižymi organizuotumu, tarptautiniu elementu, virtualiais pėdsakais bei sudėtingais informacinių ir finansinių technologijų naudojimo mechanizmais. Dėl šių pokyčių sukčiavimas šiandien nebeapsiriboja vien nusikaltimų nuosavybei tyrimo metodika, bet apima ir tuos kriminalistinius aspektus, kurie anksčiau buvo nagrinėjami atskiruose, savarankiškuose tyrimų skyriuose. Atsižvelgiant į tokius pokyčius, darytina prielaida, jog šiuolaikinės technologijos sukūrė naują sukčiavimo fenomeną, kurio

[31] Palskys, Eugenijus. 1995. Lietuvos kriminalistikos istorijos apybraižos (1918–1940): monografinė studija. Vilnius: Lietuvos policijos akademija. 4, 5, p., https://cris.mruni.eu/cris/entities/publication/c965eb93-d112-4c4a-972e-44b1d71a65ab.

[32] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Российская Е. Р. *Криминалистика: учебник для вузов* / под ред. Р. С. Белкина. Москва: Издательство, 2001. 1-8 p.

[33] Kurapka, Vidmantas Egidijus (atsak. red.), Matulienė, Snieguolė (atsak. red.) ir kt. *Kriminalistika: taktika ir metodika: vadovėlis*. Vilnius: Mykolo Romerio universitetas, 2013. 3-9 p., https://cris.mruni.eu/cris/entities/publication/e00c162c-8f82-41d5-8ffa-4f3a67742a39

tyrimas nebegali būti efektyviai atliekamas vien „nusikaltimų nuosavybei“ metodikos rėmuose, todėl reikalauja naujo, kruopštaus, vieningo kriminalistinio vertinimo.

2. ŠIUOLAIKINIO SUKČIAVIMO BAUDŽIAMOJI TEISINĖ IR KRIMINALISTINĖ CHARAKTERISTIKA

Tarpukario Lietuvoje sukčiavimo nusikaltimai, kaip aptarta ankstesniame skyriuje, nebuvo vyraujanti nusikalstamumo forma, lyginant su tokiais nusikaltimais kaip vagystės, plėšimai ar degtindarystė. Dėl tuo laikotarpiu vyravusio ekonominio ir socialinio konteksto nusikalstamumas dažnai buvo susijęs su tiesioginiais išgyvenimo poreikiais, o sukčiavimo atvejai daugiausia apsiribodavo prekybos ir paslaugų sektoriumi. Todėl tokio pobūdžio nusikaltimai buvo nedidelio masto ir nesudarė pastebimos įtakos nei visuomenei, nei valstybės funkcionavimui. Šiandien situacija atrodo visiškai kitaip. Sukčiavimas tapo ne tik dažnas, bet ir viena sudėtingiausių tiriamų ekonominių nusikaltimų formų. Informacinių technologijų pažanga, finansinės rinkos globalizacija sudarė palankias sąlygas naujų sukčiavimo formų atsiradimui. Tokios naujovės ne tik išplėtė sukčiavimo mastą, bet ir, atitinkamai, sukūrė naujas problemas teisėsaugai, reikalaujančias nuolat modernizuoti tiek teisines, tiek kriminalistines priemones.

Esant tokioms tendencijoms, teigtina, jog, vienas svarbiausių šiuolaikinės baudžiamosios teisės ir kriminalistikos uždavinių yra užtikrinti, jog sukčiavimų tyrimas būtų sistemingas, paremtas naujausiomis technologijomis ir atitiktų galiojančias teisės normas. Ne mažiau svarbu, kad šios priemonės ne tik prisitaikytų prie sparčiai kintančių sukčiavimo modelių, bet ir gebėtų juos aplenkti, pasinaudojant technologinės pažangos teikiamomis galimybėmis.

2.1 Sukčiavimo teisinis reguliavimas ir kvalifikavimo aspektai. (Baudžiamoji teisinė charakteristika)

Statistinių duomenų analizė rodo, jog kasmet Vilniaus apygardos prokuratūros ir Vilniaus apylinkės prokuratūros veiklos teritorijoje pagal Lietuvos Respublikos baudžiamojo kodekso (toliau – ir BK) 182 straipsnyje numatytos nusikalstamos veikos požymius pradedami tūkstančiai ikiteisminių tyrimų. Tarp jų reikšmingą dalį sudaro sukčiavimas elektroninėje erdvėje. Integruotos baudžiamojo proceso informacinės sistemos (toliau – ir IBPS) duomenimis, Vilniaus apygardos prokuratūros ir Vilniaus apylinkės prokuratūros veiklos teritorijoje, 2023 m. dėl sukčiavimo elektroninėje erdvėje pradėti 640 ikiteisminių tyrimų, o 2024 m. – 579 ikiteisminiai tyrimai, kurie apytiksliai sudaro apie ¼ visų pagal BK 182 straipsnį (ir jų idealiosios sutapties atvejus) pradedamų tyrimų.

Tačiau nemaža dalis su galimu sukčiavimu elektroninėje erdvėje susijusių pranešimų ikiteisminiai tyrimai taip ir neperauga, nes ikiteisminio tyrimo įstaigų pareigūnai konstatuoja, kad nėra nusikalstamos veikos požymių, kaip tai numatyta Lietuvos Respublikos baudžiamojo

proceso kodekso (toliau – ir BPK) 3 straipsnio 1 dalies 1 punkte. IBPS duomenimis, 2023 m. buvo priimti 565, o 2024 m. 307 nutarimai atsisakyti pradėti ikiteisminį tyrimą dėl galimo sukčiavimo elektroninėje erdvėje.

Vis dėlto prokurorai, vykdydami tyrimų kontrolę ir atsižvelgdami į tiriamas aplinkybes, tam tikrais atvejais panaikina policijos pareigūnų priimtus nutarimus atsisakyti pradėti ikiteisminį tyrimą dėl sukčiavimo elektroninėje erdvėje, motyvuodami tuo, kad egzistuoja nusikalstamos veikos požymiai, arba nurodo atlikti papildomus patikslinamuosius veiksmus prieš priimant galutinį procesinį sprendimą. IBPS duomenimis, Vilniaus apygardos prokuratūros ir Vilniaus apylinkės prokuratūros veiklos teritorijoje 2023 m. buvo panaikinti 71 nutarimas atsisakyti pradėti ikiteisminį tyrimą, o 2024 m. 92 nutarimai.

Be to, atlikus būtinus procesinius veiksmus, dalis pradėtų ikiteisminių tyrimų dėl sukčiavimo elektroninėje erdvėje yra perkvalifikuojami į kitų nusikalstamų veikų požymius arba yra nutraukiami prokurorų sprendimu. IBPS duomenimis 2023 m. buvo nutraukti 67 ikiteisminiai tyrimai, 2024 m. – 46 ikiteisminiai tyrimai.

Tuo tarpu aukštesnieji prokurorai bei teismai, nagrinėdami proceso dalyvių skundus dėl nutrauktų ikiteisminių tyrimų, tam tikrais atvejais panaikina šiuos prokurorų sprendimus nutraukti ikiteisminį tyrimą bei jį grąžina tolesniam procesui. IBPS duomenimis, 2023 m. aukštesnieji prokurorai panaikino 4, o 2024 m. 3 nutarimus nutraukti ikiteisminį tyrimą. Teismų praktikoje, Vilniaus apygardos prokuratūros ir Vilniaus apylinkės prokuratūros veiklos teritorijoje 2023 m. panaikintas 1 nutarimas nutraukti ikiteisminį tyrimą, 2024 m. tokių atvejų nefiksuota.

IBPS duomenimis, Vilniaus apygardos prokuratūros ir Vilniaus apylinkės prokuratūros veiklos teritorijoje 2023 m. buvo sustabdyti 394 ikiteisminiai tyrimai, 2024 m. sustabdyti 251 ikiteisminis tyrimas dėl sukčiavimo elektroninėje erdvėje. Šiais, visais atvejais buvo atlikti visi būtini veiksmai, siekiant nustatyti nusikalstamas veikas padariusius asmenis, tačiau tokie asmenys nustatyti nebuvo.

Apibendrinant IBPS duomenis, matomas aiškus 2023-2024 m. pokytis. Pavyzdžiui palyginti 2023 m ir 2024 m. Vilniaus apygardos ir Vilniaus apylinkės prokuratūrų veiklos teritorijoje sumažėjo tiek pradėtų ikiteisminių tyrimų dėl sukčiavimo elektroninėje erdvėje, tiek ir priimtų nutarimų atsisakyti pradėti ikiteisminį tyrimą. Tai gali būti aiškinama įvairiomis priežastimis, pavyzdžiui galima sieti ir su prevencinių priemonių stiprinimu finansų sektoriuje, tiek ir didėjančiu visuomenės švietimu apie dažniausiai pasitaikančius sukčiavimo modelius. Tačiau vertinant pradėtų ir sustabdytų ikiteisminių tyrimų santykį matyti, kad pastarieji sudaro beveik pusę pradėtų tyrimų, todėl sustabdytų ikiteisminių tyrimų rodikliai vis vien išlieka probleminiu indikatoriumi sukčiavimo elektroninėje erdvėje tyrimo praktikoje. Siekiant išsamiai

įvertinti šiuolaikinio sukčiavimo pobūdį ir jo teisinio reguliavimo ypatumus, būtina išanalizuoti, kaip ši nusikalstama veika apibrėžiama ir reglamentuojama Lietuvos Respublikos baudžiamajame kodekse[34], įvertinti baudžiamąją teisinę sukčiavimo charakteristiką, kuri apima šios nusikalstamos veikos sudėties požymius bei kvalifikavimo aspektus.

Visų pirma, baudžiamojoje teisėje sąvoka „baudžiamoji teisinė nusikaltimų charakteristika“ pagrinde minima tik moksliniuose tyrimuose. Ji apima įstatyme nustatytų požymių visumą, leidžiančią atskirti, ar konkretus visuomenei galimai pavojingas veiksmas laikytinas nusikaltimu, t. y. ar už jį numatyta baudžiamoji atsakomybė, taip pat padeda atriboti vieno nusikaltimo sudėtį nuo kito. Kitaip tariant, ši charakteristika nustato pagrindinius nusikaltimo elementus, jų teisinį vertinimą ir įrodinėjimo dalyką.[35] Baudžiamoji teisinė ir kriminalistinė nusikaltimų charakteristikos yra glaudžiai tarpusavyje susijusios. Kriminalistinė charakteristika, analizuodama nusikalstamos veikos požymius ir jų raišką praktikoje, remiasi baudžiamosios teisės kategorijomis, tokiomis kaip nusikalstama veika ir jos sudėtis, bei formuojama pagal nusikaltimų klasifikaciją, nustatytą BK specialiojoje dalyje. Tarp įvairių nusikalstamų veikų viena dažniausiai kriminalistinėje praktikoje analizuojamų yra sukčiavimas, kurio baudžiamoji teisinė charakteristika išsamiai atskleidžia šios nusikalstamos veikos sudėties požymius, kvalifikavimo ypatumus ir kitus baudžiamosios teisės aspektus.

Vienas svarbiausių baudžiamosios teisinės charakteristikos elementų yra nusikalstamos veikos sudėtis ir ją sudarantys požymiai. Kartu pažymėtina, kad baudžiamasis įstatymas tiesiogiai neapibrėžia nusikaltimo sudėties sąvokos, todėl jos turinys ir sudėties požymių atribojimas atskleidžiami baudžiamosios teisės doktrinoje. Teorijoje nusikalstamos veikos sudėtis suprantama kaip universalus modelis, kuriuo remiamasi siekiant pagrįsti nusikalstamos veikos buvimą bei užtikrinti kaltininko patraukimą baudžiamojon atsakomybėn. Tai taip pat leidžia kryptingai nustatyti ir įrodinėti būtent tuos aspektus, kurių reikalauja baudžiamasis įstatymas. Be to, nusikalstamos veikos sudėtis atlieka skiriamąją funkciją, nes leidžia atriboti asmenį, kurio veikoje yra nusikalstamos veikos požymių ir kuris turi būti traukiamas baudžiamojon atsakomybėn, nuo asmens, kurio veikoje tokių požymių nėra. Tiriant nusikalstamą veiką, svarbu neapsiriboti vien tik išorinių požymių nustatymu, kadangi tai sudaro tik dalį baudžiamosios atsakomybės taikymo pagrindų.[36] Kadangi nusikalstamos veikos sudėtis yra

[34] „Lietuvos Respublikos baudžiamasis kodeksas“, 2000-09-26, Nr. 1001010ISTAIII-1968. TAR. Žiūrėta 2025 m. sausio 31 d., https://www.infolex.lt/ta/66150

[35] *Соотношение уголовно-правовой и криминалистической характеристик умышленных убийств* https://studopedia.ru/28_48021_sootnoshenie-ugolovno-pravovoy-i-kriminalisticheskoy-harakteristik-umishlennih-ubiystv.html

[36] Pakštaitis, Laurynas. *Nusikalstamų veikų kvalifikavimas: baudžiamojo įstatymo taikymo teorija ir praktinės gairės: vadovėlis*. Vilnius: Mykolo Romerio universitetas, 2024. 156 p. https://cris.mruni.eu/cris/entities/publication/3b7a4d5c-b3c7-4918-9025-9de31db53c7e

pagrindinis teisinio vertinimo instrumentas, būtina išskirti jos sudedamąsias dalis, kurios leidžia tiksliai kvalifikuoti nusikalstamą veiką. Nusikaltimo sudėties požymiai sudaro tarpusavyje susijusią grupę, kuri apima tokius pagrindinius elementus kaip *objektas, objektyvioji pusė, subjektas ir subjektyvioji pusė*. Šie elementai kartu sudaro vientisą sistemą, kurioje bent vieno iš jų nebuvimas reiškia, kad nėra ir paties nusikaltimo. Per šiuos sudėtį sudarančius elementus nustatomos individualios nusikaltimo savybės, išskiriančios jį iš kitų nusikalstamų veikų. Šiuo aspektu V. N. Kudriavcevas pažymi, kad „nusikaltimo sudėtis yra informacinis tam tikros rūšies nusikaltimo modelis, įtvirtintas baudžiamajame įstatyme. Šis modelis formuojamas apibendrinant visų šios kategorijos nusikaltimų požymius. Taip sukuriamas ekonomiškas, glaustas ir pakankamai tikslus pagrindinių jų savybių aprašymas.“[37] Šis požiūris leidžia teigti, kad baudžiamoji teisinė nusikaltimo charakteristika doktrinoje siejama su sistemiškai apibendrinta informacija apie konkrečios nusikaltimo rūšies sudėties elementų požymius. Toks požymių sisteminimas sudaro teorinį pagrindą nusikalstamos veikos kvalifikavimui, padeda atriboti nusikalstamas veikas ir prisideda prie nuoseklaus baudžiamosios teisės normų taikymo.

Kadangi nusikalstamų veikų sudėtys ir jų požymių raiška praktikoje skiriasi, kvalifikavimui esminę reikšmę turi konkrečios veikos sudėties požymių analizė. Šiame darbe pagrindinis dėmesys skiriamas sukčiavimui kaip nusikalstamai veikai, susijusiai su neteisėtu svetimo turto ar turtinių teisių įgijimu. Sukčiavimas priskiriamas nusikaltimams ir baudžiamiesiems nusižengimams nuosavybei, turtinėms teisėms ir turtiniams interesams ir reglamentuojamas BK XXVIII skyriuje kartu su kitomis nusikalstamomis veikomis, nukreiptomis prieš šiuos objektus. Sukčiavimas yra viena iš turto pasisavinimo formų, ir pagal BK 182 straipsnį[38] suprantama kaip nusikalstama veika, kurios metu *apgaule savo ar kitų naudai įgyjamas svetimas turtas ar turtinė teisė, išvengiama turtinės prievolės arba ji panaikinama*.

Tačiau, prieš pradedant gilintis į sukčiavimo baudžiamąją teisinę charakteristiką, tikslinga išsiaiškinti įstatymo leidėjo vartojamų sąvokų turinį, tokių kaip: „įgijimas“, „svetimas turtas“, „turtinė teisė“, „turtinė prievolė“.

Analizuojant Lietuvos Respublikos baudžiamojo kodekso XXVIII skyriuje reglamentuojamas nusikalstamas veikas, pastebėtina, kad kai kurių veikų dispozicijose vartojama turto „*pagrobimo*“ terminas, pavyzdžiui, BK 178 straipsnyje (vagystė), BK 180 straipsnyje (plėšimas). Tuo tarpu sukčiavimo atveju BK 182 straipsnyje vartojamas terminas „*įgijimas*“. Šis terminų skirtumas leidžia kelti klausimą, kodėl sukčiavimas apibrėžiamas ne kaip svetimo turto pagrobimas apgaule, o kaip svetimo turto ar turtinės teisės įgijimas apgaule, ir kokią reikšmę

[37] Кудрявцев В. Н. *Общая теория квалификации преступлений*. Москва: Юридическая литература, 1972., 352 p. https://www.studmed.ru/kudryavcev-vn-obschaya-teoriya-kvalifikacii-prestupleniy_f7451ec8c9d.html

[38] 2. Lietuvos Respublikos baudžiamasis kodeksas, 182 straipsnis, „Sukčiavimas,“, Nr. 2023-08475. TAR. Žiūrėta 2025 m. sausio 31 d., https://www.infolex.lt/ta/66150:str182

toks pasirinkimas turi sukčiavimo sudėties atribojimui nuo kitų nusikalstamų veikų.

Atsakymą į šį klausimą padeda atskleisti Lietuvos Aukščiausiojo Teismo (toliau – ir LAT) senato 2005 m. birželio 23 d. nutarime pateiktas turto pagrobimo apibrėžimas, pagal kurį turto pagrobimu laikomas fizinis svetimo turto užvaldymas, atimantis iš asmens galimybę valdyti, naudotis ir disponuoti jam priklausančiu turtu.[39] Tame pačiame LAT senato nutarime pabrėžta, kad turto pagrobimas yra tyčinė nusikalstama veika, kuri padaroma tik tiesiogine tyčia, kai kaltininkas suvokia, kad veikia prieš turto savininko valią, numato nusikalstamos veikos padarinius ir jų nori.[40] Tuo tarpu sukčiavimo atveju veika grindžiama ne fiziniu turto atėmimu, o nukentėjusiojo valios klaidinimu. Kaip pažymima LAT parengtoje teismų praktikos AB 36-1 apžvalgoje, „svetimo turto įgijimas – tai kilnojamojo ar nekilnojamojo daikto, taip pat pinigų ar vertybinių popierių įgijimas panaudojant apgaulę. Iš esmės tai neteisėtas fiktyvaus teisinio santykio sukūrimas, pagal kurį kaltininkas ar tretieji asmenys gauna svetimą turtą ar materialių civilinės apyvartos objektų teikiamą naudą.“[41] Akcentuojama, kad toks įgijimas gali išoriškai atitikti turinio ir formos reikalavimus, nustatytus civilinės teisės sandoriams, nors jo tikrasis pobūdis yra baudžiamosios teisės reguliavimo sritis. Iš šių Lietuvos Aukščiausiojo Teismo sąvokų apibrėžimų matyti, kad pagrindinis sukčiavimo kaip nusikalstamos veikos požymis yra ne fizinis poveikis turtui, o nukentėjusiojo valios iškraipymas apgaulės būdu. Dėl to įstatymų leidėjas sukčiavimo kontekste pagrįstai vartoja terminą „įgijo“, o ne „pagrobė“. Šia prasme svetimo turto įgijimas sukčiaujant gali būti vertinamas kaip pagrobimo forma, besiskirianti nuo vagystės vien tuo, kad turto užvaldymas įvykdomas apgaule, o ne tiesioginiu fiziniu veiksmu.

Atrodytų, kad sukčiavimo atveju svetimo turto apibrėžimą būtų galima vertinti panašiai kaip ir vagystės atveju, t. y. kaip svetimą, materialų, kilnojamąjį objektą, turintį piniginę vertę. Vis dėlto įvertinus įstatymų leidėjo pasirinktų sąvokų – „įgijimas“ ir „pagrobimas“ skirtumus, tampa akivaizdu, kad teismų praktikoje sukčiavimo svetimo turto sąvoka aiškinama plačiau, apimant ir nekilnojamąjį turtą. LAT parengtoje teismų praktikos AB 36-1 apžvalgoje nurodoma, kad svetimu turtu laikomi tie kilnojamieji ar nekilnojamieji daiktai, taip pat pinigai, vertybiniai popieriai ir kiti panašūs objektai, kurie kaltinamajam nepriklauso nuosavybės teise[42]. Akivaizdu, jog plati svetimo turto samprata, apimanti ir nekilnojamuosius objektus, sukčiavimo veikose suponuoja teorinius sunkumus atribojant *turto* ir *turtinės teisės* sąvokas. Tokiais atvejais, kai apgaule įgyjamas nekilnojamasis turtas, tradicinė pagrobimo samprata tampa netinkama. Šios sampratos neatitinka ir turtinės teisės įgijimas, turtinės prievolės panaikinimas ar išvengimas

[39] Lietuvos Aukščiausiojo Teismo senato 2005 m. birželio 23 d. nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“. Teismų praktika, 2005, Nr. 23.

[40] Ibid.

[41] Lietuvos Aukščiausiasis Teismas. *Teismų praktikos sukčiavimo baudžiamosiose bylose (Baudžiamojo kodekso 182 straipsnis) apžvalga*. https://www.lat.lt/data/public/uploads/2018/06/ab-36-1.docx

[42] Ibid.

apgaule. Nusikaltimo mechanizmas šiais atvejais kitoks. Tokiu atveju susiduriama ne su fiziniu, bet juridiniu (dokumentiniu) turto įgijimu[43].

Turtinė teisė – tai kaltininko sau ar kito asmens naudai neteisėtai įgyta daiktinė ar prievolinė teisė arba teisė, atsirandanti iš intelektinės veiklos rezultatų (Lietuvos Respublikos civilinio kodekso (toliau – ir CK) 1.112 straipsnio 1 dalis). O. Fedosiuk, aiškindamas šios sąvokos reikšmę baudžiamosios teisės kontekste, pažymi, kad turtinė teisė sukčiavimo atveju suprantama analogiškai kaip ir turto prievartavimo sudėtyje. Įgyti turtinę teisę apgaule reiškia paveikti kito asmens valią taip, kad šis dėl suklydimo teisiškai patvirtina juridinį faktą, suteikiantį kaltininkui reikalaujamą teisę. Tokiais atvejais padariniai pasireiškia kaip nukentėjusiojo turtinės teisės netekimas, jos apimties sumažėjimas arba turtinės prievolės atsiradimas. Šis aiškinimas leidžia daryti išvadą, kad turtinė teisė sukčiavime nėra tik abstrakti teisinė galimybė, bet konkreti, apgaule įgyta turtinio pobūdžio nauda, kurios pagrindas yra ne teisėtas susitarimas, o klaidingai suformuota nukentėjusiojo valia.

CK 6.1. straipsnyje nurodoma, kad prievolė – tai teisinis santykis, kurio viena šalis (skolininkas) privalo atlikti kitos šalies (kreditoriaus) naudai tam tikrą veiksmą arba susilaikyti nuo tam tikro veiksmo, o kreditorius turi teisę reikalauti iš skolininko, kad šis įvykdytų savo pareigą. Atsižvelgiant į šią Civilinio kodekso normą, turtinė prievolė suprantama kaip pareiga, kylanti iš teisinių santykių, kurių pagrindu viena šalis turi teisę reikalauti atlyginti nuostolius ar sumokėti netesybas, o kita – atitinkamai įvykdyti šią pareigą. Baudžiamosios teisės požiūriu, LAT parengtoje teismų praktikos AB 36-1 apžvalgoje pažymima, kad sukčiavimo atveju turtinės prievolės gali būti panaikinamos ar jų vengiama apgaulės būdu, dėl ko faktiškai pažeidžiama nukentėjusiojo teisė į reikalavimą:

- Turtinės prievolės panaikinimas – tai nukentėjusiojo turtinės teisės, atitinkančios kaltininko ar trečiojo asmens turtinę prievolę, netekimas remiantis fiktyviu juridiniu faktu (pvz., fiktyviais atskaitos ir įskaitos būdais likviduojamas ar sumažinamas į biudžetą mokėtinas PVM).
- Turtinės prievolės išvengimas – tai kaltininko ar kito asmens pareigos, kilusios iš delikto, sandorio ar kitu teisėtu pagrindu, nevykdymas ar tik dalinis vykdymas panaudojant apgaulę (pvz., kaltininkas neteisėtai atsisako vykdyti savo pareigą kreditoriui, sudarydamas situaciją, kai kreditorius negali civilinėmis teisinėmis priemonėmis atkurti savo pažeistos teisės).

Pasak A. Abramavičių: „Baudžiamosios teisės teorijoje priimta nusikaltimo dalyku laikyti konkrečius materialaus pasaulio daiktus, kuriuos veikiant daroma žala teisiniams gėriams

[43] Gruodytė, Edita, Olegas Fedosiukas, Albertas Milinis, Aurelijus Gutauskas, Neringa Palionienė, Marius Kuzminovas, Marijus Šalčius ir Simona Žižienė. 2021. *Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga*. 2-asis leidimas. Kaunas: Vytauto Didžiojo universitetas. 392 p., https://ebooks.vdu.lt/einfo/3021/lietuvos-baudziamoji-teise-specialioji-dalis-pirmoji-knyga/

ar keliama tokios žalos atsiradimo grėsmė“[44]. Kaip jau buvo pažymėta aiškinant įstatymo leidėjo vartojamas sąvokas, sukčiavimo dalyku gali būti ne tik materialus turtas (kilnojamieji ir nekilnojamieji daiktai), bet ir nematerialūs daiktai, tokie kaip akcijos ar vertybiniai popieriai, taip pat turtinės prievolės. Šis aspektas išskiria sukčiavimą iš kitų turtinių nusikaltimų, kuriuose paprastai pasikėsinama tik į fizinį turtą. Sukčiavimo dalyko specifika lemia problemines situacijas, susijusias su turto ir turtinės teisės sąvokų atribojimu. Pavyzdžiui, nekilnojamojo turto įgijimas apgaule nebeatitinka tradicinės pagrobimo sampratos, nes, kaip jau buvo minėta, šiuo atveju nusikalstamos veikos mechanizmas yra ne fizinis, o juridinis – įgyjamos ne materialios gėrybės, o teisės į jas. Panaši situacija kyla ir sukčiaujant dėl turtinių prievolių – kai apgaule panaikinama arba sumažinama skola, dėl ko nukentėjusysis netenka turtinės teisės arba jos apimties. Tradiciškai sukčiavimo baigtumas siejamas su momentu, kai nukentėjusysis, būdamas suklaidintas, savanoriškai perduoda turtą kaltininkui, manydamas, kad šis turi teisę jį gauti. Tokiu būdu kaltininkas įgyja galimybę turtą valdyti, naudoti ar juo disponuoti savo nuožiūra. Vis dėlto tam tikrais atvejais svetimo turto ir turtinės teisės įgijimo požymiai gali sutapti – pavyzdžiui, įgyjant nekilnojamąjį turtą kartu su nuosavybės teise į jį arba perimant banko sąskaitoje esančias lėšas kartu su teise jomis disponuoti[45].

Minėtas požiūris į sukčiavimo dalyką atsispindi ir mokslinėje doktrinoje. Olego Fedosiuk teigimu, Lietuvos Respublikos baudžiamajame kodekse sukčiavimo dalykas iš esmės siejamas su terminu „nauda“, kuri įgyjama BK normoje nurodytais būdais: įgyjant turtą ar turtinę teisę, arba išvengiant ar panaikinant turtinę prievolę[46]. Panašią poziciją išreiškia ir T. Girdenis, A. Gutauskas bei P. Kujalis, pažymėdami, kad sukčiavimo dalyku laikytini tiek turtas, tiek turtinės teisės ar prievolės, tačiau visą tai galima apibendrinti kaip turtinę naudą, kurią, pasak autorių, kaltininkas realizuoja apgaulės būdu užvaldydamas svetimą turtą, pažeisdamas turtinę teisę ar prievolinį interesą[47]. Taigi, būtinu šios veikos požymiu laikomas ir turto įgijimas bei jo pavertimas kaltininko ar trečiųjų asmenų naudai, dėl ko savininkui ar kitam teisėtam valdytojui padaroma turtinė žala.

Pažymėtina, kad kaltininko veikos kvalifikavimas tiesiogiai priklauso nuo sukčiavimo

---

[44] Antanas Abramavičius, *Baudžiamoji teisė: Bendroji dalis* (Vilnius: Eugrimas, 2003), p. 166, cituojama pagal: Tomas Dargis, *Sukčiavimo (BK 182 straipsnis) atskyrimas nuo nusikalstamų veikų finansų sistemai*, magistro darbas, Vilniaus universitetas, Teisės fakultetas, 2016, 16 p.

[45] Gruodytė, Edita, Olegas Fedosiukas, Albertas Milinis, Aurelijus Gutauskas, Neringa Palionienė, Marius Kuzminovas, Marijus Šalčius ir Simona Žižienė. 2021. *Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga.* 2-asis leidimas. Kaunas: Vytauto Didžiojo universitetas. 392 p., https://ebooks.vdu.lt/einfo/3021/lietuvos-baudziamoji-teise-specialioji-dalis-pirmoji-knyga/

[46] Fedosiuk, Oleg. 2003. „Sukčiavimo normos koncepcija naujame Lietuvos Respublikos baudžiamajame kodekse ir jos įgyvendinimo problemos“. *Teisė 48*: 79 p. https://www.lituanistika.lt/content/45733

[47] Girdenis, Tomas, Aurelijus Gutauskas, ir Pavelas Kujalis. *Baudžiamoji teisė: metodinė priemonė*. Vilnius: Mykolo Romerio universitetas, 2014. 228 p. https://cris.mruni.eu/cris/entities/publication/5bafeae8-80c5-414f-9586-1cb4dedb229b

dalyko pobūdžio ir vertės. Lietuvos Respublikos baudžiamojo kodekso 182 straipsnio 2 ir 3 dalyse nustatyti kvalifikuojantys požymiai, susiję su didelės ar labai didelės vertės svetimo turto, turtinės teisės ar turtinės prievolės įgijimu apgaule. Kvalifikavimą taip pat gali lemti ir ypatingas dalyko pobūdis – pavyzdžiui, kai įgyjamos didelės mokslinės, istorinės ar kultūrinės reikšmės vertybės, arba kai sukčiavimas vykdomas organizuotoje grupėje (BK 182 straipsnio 3 dalyje). Tais atvejais, kai kyla klausimas, ar sukčiavimo būdu įgytas turtas pasižymi minėta specifine verte, dažniausiai būtina remtis atitinkamos srities specialisto ar eksperto išvada, leidžiančia objektyviai įvertinti vertybės reikšmę[48]. Tuo tarpu 4 dalyje numatyta veika, kai įgyjamas nedidelės vertės turtas ar turtinė teisė, arba išvengiama atitinkamos vertės prievolės, kvalifikuojama kaip baudžiamasis nusižengimas. Nustatant, ar turtas atitinka BK 182 straipsnyje numatytas vertės ribas, vadovaujamasi BK 190 straipsnyje pateiktu turto vertės išaiškinimu. Turto vertė gali būti grindžiama pirkimo-pardavimo sandorio kaina, įsigijimo ar atkūrimo išlaidomis. Tais atvejais, kai turtas įgytas pirkimo-pardavimo būdu ir byloje yra duomenų apie šio sandorio kainą, tačiau nuo įsigijimo iki nusikalstamos veikos padarymo momento praėjo tam tikras laiko tarpas, turto vertė nustatoma pagal jo faktinę rinkos (didmeninę ar komiso) vertę nusikaltimo padarymo metu. Tai leidžia objektyviai įvertinti kaltininko įgytos turtinės naudos dydį ir tinkamai kvalifikuoti veiką pagal atitinkamą BK straipsnio dalį[49].

Lietuvos baudžiamosios teisės doktrinoje turtinių nusikaltimų objektu laikomi teisiniai gėriai, kuriuos saugo XXVIII BK skyrius – nuosavybė, turtinės teisės ir turtiniai interesai. Šios nusikalstamos veikos objektyviąją pusę apibūdina veika, jos padarymo būdas, tam tikrais atvejais padariniai ir priežastinis ryšys. Sukčiavimas pasireiškia tam tikromis alternatyviomis veikomis: 1) svetimo turto įgijimu; 2) svetimos turtinės teisės įgijimu; 3) turtinės prievolės išvengimu; 4) turtinės prievolės panaikinimu. Šie sukčiavimo objektyvieji požymiai BK 182 straipsnio dispozicijoje suformuluoti kaip alternatyvūs, todėl baudžiamajai atsakomybei kilti pakanka, kad būtų padaryta bent viena nurodytų veikų. Akivaizdu, kad sukčiavimo, kaip baudžiamosios teisės kategorijos, specifika atsiskleidžia per šio nusikaltimo padarymo būdą – apgaulės mechanizmą, kuris laikytinas būtinu šios nusikalstamos veikos sudėties požymiu. Tai reiškia, jog kaltininkas vieną iš alternatyvių veikų turi būti įvykdęs panaudodamas apgaulę. Dabartinės lietuvių kalbos žodyne[50] *apgaulė* apibūdinama kaip „veiksmai, elgesys ar žodžiai, kuriais sąmoningai norima apgauti, suklaidinti“.

Civilinėje teisėje apgaulės samprata pasireiškia situacijomis, kai viena šalis sąmoningai

[48] Girdenis, Tomas, Aurelijus Gutauskas, ir Pavelas Kujalis. *Baudžiamoji teisė: metodinė priemonė*. Vilnius: Mykolo Romerio universitetas, 2014. 232 p. https://cris.mruni.eu/cris/entities/publication/5bafeae8-80c5-414f-9586-1cb4dedb229b

[49] Ibid. 230 p.

[50] Stasys Keinys, vyriaus. red., *Dabartinės lietuvių kalbos žodynas*, 8-as patais. ir papild. leid. (Vilnius: Lietuvių kalbos institutas, 2021), XXVI, 973, https://ekalba.lt

pasinaudoja jai žinoma informacija, kuri kitai šaliai yra nežinoma arba dėl kurios ji klysta. Tokiu atveju, kai asmuo, veikdamas remdamasis klaidingu situacijos suvokimu, sudaro nenaudingą sandorį ar netinkamai disponuoja turtu, laikoma, kad jo valia nėra laisva. Dėl to sandoris gali būti pripažintas negaliojančiu nukentėjusiojo ieškiniu[51].

Tiesioginis apgaulės apibrėžimas nėra įtvirtintas galiojančiame Lietuvos Respublikos baudžiamajame kodekse, tačiau šios sąvokos turinys formuojamas remiantis teismų praktika, analizuojant sukčiavimo sudėtį. Teismų praktikos sukčiavimo baudžiamosiose bylose apžvalgoje, AB-36-1, pažymima, kad apgaulė pasireiškia siekiu suklaidinti turto savininką, valdytoją ar kitą asmenį, turintį teisę disponuoti turtu (įskaitant bankus, teismus, antstolius, notarus). Suklaidintas asmuo savanoriškai perleidžia turtą ar turtinę teisę kaltininkui, manydamas, kad šis turi teisę juos gauti, arba priima sprendimą, kurio pasekmė – kaltininko naudai perleidžiamos turtinės teisės ar panaikinama turtinė prievolė.

Pasak O. Fedosiuk[52], Lietuvos Respublikos baudžiamojoje teisėje apgaulė paprastai suprantama kaip sąmoningas kito asmens suklaidinimas, pateikiant melagingą informaciją (aktyvioji apgaulė) arba nuslepiant svarbius faktus, kuriuos buvo būtina atskleisti (pasyvioji apgaulė). Dėl kaltininko iškraipytos objektyviosios tiesos nukentėjusiojo sąmonėje susiformuoja klaidingas įsivaizdavimas apie esamus ar buvusius faktus, kas jį paskatina priimti ekonomiškai nenaudingus sprendimus. Tai gali reikštis turto perdavimu, turtinės teisės perleidimu, atsisakymu pasinaudoti savo turtine teise, turtinių įsipareigojimų prisiėmimu ir pan. Kasacinės instancijos teismo praktikoje išaiškinta, kad apgaulė, be kita ko, reiškiasi asmenų suklaidinimu, pranešant neteisingus duomenis arba nutylint esmines jų apsisprendimui dėl turto, turtinės teisės perleidimo ar turtinės prievolės panaikinimo aplinkybes, turint teisinę pareigą apie jas pranešti. Asmuo gali būti suklaidinamas dėl bet kokių aplinkybių ar faktų, susijusių su turto, turtinės teisės perleidimu kaltininkui arba jo turtinės prievolės panaikinimu (dėl turto vertės, jo savybių, kaltininko asmenybės, jo įgaliojimų ar ketinimų ir pan.), tačiau kaltininko panaudota apgaulė turi būti esminė, t. y. turėti lemiamą įtaką asmens apsisprendimui atlikti minėtus veiksmus (kasacinės nutartys baudžiamosiose bylose Nr. 2K-108-788/2018[53], 2K-71-976/2022[54], 2K-43-495/2024[55]).

---

[51] Sinkevičius, Edvardas. 2002. *Neteisėtas banko kredito gavimas arba panaudojimas ir jų kvalifikavimas.* Vilnius: Lietuvos teisės universiteto leidybos centras. 49 p.

[52] Gruodytė, Edita, Olegas Fedosiukas, Albertas Milinis, Aurelijus Gutauskas, Neringa Palionienė, Marius Kuzminovas, Marijus Šalčius ir Simona Žižienė. 2021. *Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga.* 2-asis leidimas. Kaunas: Vytauto Didžiojo universitetas. 394 p., https://ebooks.vdu.lt/einfo/3021/lietuvos-baudziamoji-teise-specialioji-dalis-pirmoji-knyga/

[53] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 20 d. nutartis baudžiamojoje byloje Nr. 2K-108-788/2018“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/1576411

[54] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. kovo 16 d. nutartis baudžiamojoje byloje Nr. 2K-71-976/2022“ . Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2068440

[55] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2024 m. kovo 6 d. nutartis baudžiamojoje byloje Nr. 2K-43-495/2024“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2230506

Jei asmens suklaidinimas neturėjo lemiamos įtakos asmens apsisprendimui perduoti turtą, ar turtinę teisę, tokia apgaulė nedaro veikos sukčiavimo nusikaltimu. Be kita ko, civilinių teisinių santykių nereikia painioti su jų imitavimu, kai civilinė sutartis yra tik priemonė kito asmens turtui užvaldyti ir atitinkamai turtinei žalai jam padaryti (kasacinės nutartys baudžiamosiose bylose Nr. 2K-76-788/2020[56], 2K-27-788/2021[57], 2K-215-697/2023[58]).

Tačiau net ir turint aiškiai suformuluotą nusikaltimo teisinę charakteristiką, teismų praktikoje itin svarbus baudžiamosios atsakomybės atribojimo nuo kitų teisinių atsakomybės rūšių klausimas. Teismai ne kartą yra pažymėję, kad ne bet kokia neteisėta veika turi būti priskiriama baudžiamajai atsakomybei, nes ši teisės šaka demokratinėje visuomenėje veikia pagal principą *ultima ratio* (lot. paskutinis argumentas; paskutinė priemonė[59]) – kaip kraštutinė priemonė, taikytina tik tada, kai kitomis (civilinės ar administracinės teisės) priemonėmis negalima pasiekti teisinių gėrių apsaugos ir teisingumo atkūrimo[60]. Toks požiūris ypač svarbus sukčiavimo atvejais, kadangi ši veika neretai balansuoja ties riba tarp civilinių ir baudžiamųjų teisinės atsakomybės institutų. Nuosavybės teisė, kaip viena iš fundamentalių teisinių vertybių, pirmiausia turėtų būti ginama civilinės ar administracinės teisės priemonėmis, o baudžiamasis persekiojimas taikomas tik tais atvejais, kai kiti teisiniai mechanizmai pasirodo neefektyvūs.

Sukčiavimo, kaip nusikalstamos veikos, požymis, skiriantis jį nuo civilinio delikto ir darantis turto užvaldymą neteisėtą baudžiamąja prasme, yra apgaulės panaudojimas prieš turto savininkus, teisėtus valdytojus ar asmenis, kurių žinioje yra turtas, ir (arba) sąmoningas situacijos sudarymas, kad nukentėjusysis negalėtų civilinėmis teisinėmis priemonėmis atkurti savo pažeistos teisės arba toks pažeistų teisių gynimo būdas būtų esmingai pasunkintas. Aptariama apgaulė turi būti esminė, t. y. suklaidinimas turi turėti lemiamą įtaką asmens apsisprendimui dėl turto perdavimo kitam asmeniui (kasacinės nutartys baudžiamosiose bylose Nr. 2K-7-27-746/2015[61], 2K-7-47-895/2016[62], 2K-7-41-511/2017[63], 2K-7-136-489/2017[64], 2K-

[56] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2020 m. kovo 24 d. nutartis baudžiamojoje byloje Nr. 2K-76-788/2020“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. 53, p. 565-573, https://www.infolex.lt/tp/1869178

[57] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2021 m. kovo 9 d. nutartis baudžiamojoje byloje Nr. 2K-27-788/2021“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/1975659

[58] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. lapkričio 14 d. nutartis baudžiamojoje byloje Nr. 2K-215-697/2023“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2204286

[59] Lietuvių kalbos žodynas. „Ultima ratio.“ *Lietuviuzodynas.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.lietuviuzodynas.lt/terminai/Ultima_ratio

[60] Pavyzdžiui, LAT Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. gegužės 24 d. nutartis baudžiamojoje byloje Nr. 2K-262/2011; LAT Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. spalio 20 d. nutartis baudžiamojoje byloje Nr. 2K-P-267/2011; LAT Baudžiamųjų bylų skyriaus teisėjų kolegijos 2013 m. gegužės 14 d. nutartis baudžiamojoje byloje Nr. 2K-250/2013 ir kt.

[61] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. balandžio 23 d. nutartis baudžiamojoje byloje Nr. 2K-7-27-746/2015“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. 43, p. 358-368, https://www.infolex.lt/tp/1045319

17-976/2020[65] ir kt.). Kasacinės instancijos teismo praktikoje išskiriami šie apgaulės kriterijai: 1) objektyvios tiesos iškraipymas; 2) tikslas – suklaidinti nukentėjusįjį (lemti nukentėjusiojo klaidą); 3) tyčia – kaltininko suvokimas, kad jis sąmoningai pateikia objektyvios tikrovės neatitinkančią informaciją (kasacinės nutartys baudžiamosiose bylose Nr. 2K-158-303/2021[66], 2K-6-976/2023[67], 2K-91-891/2025[68] ir kt.). Atskiriant sukčiavimą nuo civilinės teisės pažeidimo, taip pat taikytinas pirmiau nurodytas kreditoriaus teisinės padėties pasunkinimo kriterijus (kai dėl skolininko veiksmų kreditoriaus galimybės atkurti pažeistas teises civilinėmis teisinėmis priemonėmis esmingai pasunkintos). Teismų praktikoje kartu yra pateikiami ir galimi teisių gynimo būdų civilinėmis teisinėmis priemonėmis apsunkinimo pavyzdžiai: be teisėsaugos pagalbos neįmanoma surasti ar identifikuoti prievolės vengiančio asmens arba asmenų, kuriems turtas buvo perleistas; kaltininkas tyčia tapo nemokus, aktyviais veiksmais vengė (pavyzdžiui, slapstėsi), trukdė atlyginti žalą arba kitaip teisės atkūrimą padarė neperspektyvų; sąmoningai nevykdė įpareigojimų, atsiradusių patikėjus ar perdavus jo žinion turtą; nuslėpė nuo nukentėjusiojo esminę informaciją apie turimas dideles skolas ar nemokumą; dėl dokumentų klastojimo, operacijų su turtu nefiksavimo ar kitų veikų apsunkino turto disponavimo proceso nustatymą; sudarė akivaizdžiai su turto savininko interesais nesutampančius, ekonomiškai nepagrįstus sandorius (kasacinės nutartys baudžiamosiose bylose Nr. 2K-46-699/2018[69], 2K-241-942/2022[70], 2K-138-1073/2023[71], 2K-261-489/2024[72])

---

[62] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. sausio 15 d. nutartis baudžiamojoje byloje Nr. 2K-7-47-895/2016“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/1173577

[63] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2017 m. vasario 7 d. nutartis baudžiamojoje byloje Nr. 2K-7-41-511/2017“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. 47, p. 457-475, https://www.infolex.lt/tp/1426475

[64] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2017 m. lapkričio 16 d. nutartis baudžiamojoje byloje Nr. 2K-7-136-489/2017“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. 48, p. 270-290, https://www.infolex.lt/tp/1538664

[65] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2020 m. vasario 11 d. nutartis baudžiamojoje byloje Nr. 2K-17-976/2020“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/1817721

[66] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2021 m. birželio 28 d. nutartis baudžiamojoje byloje Nr. 2K-158-303/2021“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2006460

[67] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. vasario 2 d. nutartis baudžiamojoje byloje Nr. 2K-6-976/2023“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2140988

[68] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2025 m. gegužės 28 d. nutartis baudžiamojoje byloje Nr. 2K-91-891/2025“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2317237

[69] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 26 d. nutartis baudžiamojoje byloje Nr. 2K-46-699/2018“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1584302

[70] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. lapkričio 22 d. nutartis baudžiamojoje byloje Nr. 2K-241-942/2022“. Teismų praktika, 2022, Nr. 58, p. 524–561. Infolex. Žiūrėta 2025 m. gruodžio 16 d , https://www.infolex.lt/tp/2123749

Sukčiavimo baigtumas priklauso nuo dalyko rūšies[73]:

- Sukčiavimas įgyjant svetimą turtą laikomas baigtu, kai turto savininkas ar valdytojas arba asmuo, kurio žinioje yra turtas, perleidžia jį kaltininkui ar kitam asmeniui, o šis įgyja galimybę turtą valdyti ir (ar) juo naudotis ir (ar) disponuoti savo nuožiūra.
- Sukčiavimas įgyjant turtinę teisę ar panaikinant turtinę prievolę laikomas baigtu, kai apgaule įtvirtinamas juridinis faktas, suteikiantis kaltininkui turtinę teisę nepriklausomai nuo to, ar šis ją įgyvendino, arba panaikinantis jo turtinę prievolę.
- Apie turtinės prievolės išvengimo baigtumo momentą teismas sprendžia atsižvelgdamas į konkrečias bylos aplinkybes.

Baudžiamosios teisės doktrinoje nėra vieningos nuomonės, ar apgaulė gali būti siejama su ateityje įvyksiančiomis aplinkybėmis. Vieni teoretikai teigia, kad apgaulė gali būti grindžiama tik esamuoju ar praeities faktų iškraipymu, nes ateities įvykiai yra tik tikėtini, todėl pažadai ar įtikinėjimai dėl būsimos situacijos negali būti laikomi apgaule. Priešingai, kiti laikosi pozicijos, kad esminė apgaulės sąlyga yra nukentėjusiojo suklaidinimas, nepriklausomai nuo to, kokios laiko perspektyvos faktai yra iškraipomi. Lietuvos teismų praktikoje vyrauja pastarasis požiūris, ypač pabrėžiant piktnaudžiavimą pasitikėjimu kaip apgaulės formą. Tai apima sąmoningą klaidinimą, suteikiant neteisingą informaciją apie būsimus veiksmus, įtikinėjimą ar sutarčių sudarymą be realaus ketinimo jas vykdyti. Piktnaudžiavimas pasitikėjimu yra tada, kai kaltininkas BK 182 straipsnyje nurodytas veikas padaro piktnaudžiaudamas tarp jo ir turto savininko, valdytojo ar asmens, kurio žinioje yra turtas, susiklosčiusiais asmeniniais, tarnybiniais ar kitokiais tarpusavio ryšiais, sudarančiais tarpusavio pasitikėjimo pagrindą (kasacinės nutartys baudžiamosiose bylose Nr. 2K-507/2012[74], 2K-327/2014[75], 2K-188-719/2018[76]). Piktnaudžiavimas pasitikėjimu yra ir tada, kai viena šalis, įgijusi kitos šalies pasitikėjimą, įtikina ją suteikti atlygintiną materialinę pagalbą. Kita šalis, suklaidinta dėl kaltininko ketinimų, perduoda turtą, tikėdamasi, kad vėliau atgaus analogišką materialinį atlygį, tačiau kadangi kita

[71] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. gegužės 8 d. nutartis baudžiamojoje byloje Nr. 2K-138-1073/2023“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2162528

[72] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2024 m. gruodžio 12 d. nutartis baudžiamojoje byloje Nr. 2K-261-489/2024“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2284787

[73] Lietuvos Aukščiausiasis Teismas. *Teismų praktikos sukčiavimo baudžiamosiose bylose (Baudžiamojo kodekso 182 straipsnis) apžvalga*. https://www.lat.lt/data/public/uploads/2018/06/ab-36-1.docx

[74] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 30 d. nutartis baudžiamojoje byloje Nr. 2K-507/2012“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/478922

[75] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2014 m. birželio 19 d. nutartis baudžiamojoje byloje Nr. 2K-327/2014“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/831495

[76] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. birželio 6 d. nutartis baudžiamojoje byloje Nr. 2K-188-719/2018“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1603326

šalis to daryti nesiruošia, ji patiria materialų nuostolį, kurio atlyginimas civilinėje teisėje nustatytomis priemonėmis yra pasunkintas (kasacinės nutartys baudžiamosiose bylose Nr. 2K-264-895/2016[77], 2K-188-719/2018[78], 2K-71-976/2022[79], 2K-6-976/2023[80]). Vis dėlto teismų sprendimuose išskiriama aiški riba tarp sukčiavimo ir civilinių teisinių santykių – jei nėra objektyvių duomenų, kad asmuo jau sandorio sudarymo metu neketino vykdyti savo įsipareigojimų, situacija kvalifikuojama kaip civilinis ginčas, o ne baudžiamasis nusikaltimas[81].

Dar vienas būtinųjų nusikalstamos veikos sudėties elementų yra subjektas, kuris Lietuvos Respublikos baudžiamosios teisės teorijoje ir praktikoje tradiciškai siejamas su fiziniu, pakaltinamu asmeniu, sulaukusiu baudžiamosios atsakomybės amžiaus. Vadovaujantis BK 13 straipsniu, asmuo atsako pagal baudžiamuosius įstatymus, jeigu iki nusikalstamos veikos padarymo yra sulaukęs 16 metų, o už kai kurias išimtines veikas – nuo 14 metų. Kadangi sukčiavimas nėra priskiriamas prie šių išimčių, baudžiamoji atsakomybė už šią nusikalstamą veiką prasideda nuo 16 metų. Kita svarbi sąlyga – pakaltinamumas, kuris reiškia asmens gebėjimą suprasti savo veiksmų esmę ir juos valdyti. Pakaltinamumo klausimas reglamentuojamas BK 17 ir 18 straipsniuose. Asmuo yra nepakaltinamas, jei darydamas nusikalstamą veiką dėl psichikos sutrikimo negalėjo suvokti jos pavojingumo arba valdyti savo veiksmų (BK 17 straipsnis). Tokiu atveju baudžiamoji atsakomybė jam netaikoma, tačiau gali būti taikomos priverčiamosios medicinos priemonės. Tuo tarpu asmuo, kuris dėl psichikos sutrikimo negalėjo visiškai suvokti nusikalstamos veikos pavojingumo arba valdyti savo veiksmų, tačiau šis sutrikimas nėra pakankamas pripažinti jį nepakaltinamu, laikomas ribotai pakaltinamu (BK 18 straipsnis). Ribotai pakaltinamas asmuo atsako baudžiamąja tvarka, tačiau bausmė jam gali būti švelninama, o tam tikrais atvejais jis gali būti atleistas nuo baudžiamosios atsakomybės ir jam gali būti taikomos baudžiamojo poveikio arba priverčiamosios medicinos priemonės.

Svarbu pažymėti, kad nuo 2000 m. rugsėjo 26 d. įsigaliojus naujajam BK (Nr. VIII-

[77] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. birželio 17 d. nutartis baudžiamojoje byloje Nr. 2K-264-895/2016“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1288766

[78] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. birželio 6 d. nutartis baudžiamojoje byloje Nr. 2K-188-719/2018“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1603326

[79] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. kovo 16 d. nutartis baudžiamojoje byloje Nr. 2K-71-976/2022“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2068440

[80] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. vasario 2 d. nutartis baudžiamojoje byloje Nr. 2K-6-976/2023“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2140988

[81] Gruodytė, Edita, Olegas Fedosiukas, Albertas Milinis, Aurelijus Gutauskas, Neringa Palionienė, Marius Kuzminovas, Marijus Šalčius ir Simona Žižienė. 2021. Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga. 2-asis leidimas. Kaunas: Vytauto Didžiojo universitetas. 395 p., https://ebooks.vdu.lt/einfo/3021/lietuvos-baudziamoji-teise-specialioji-dalis-pirmoji-knyga/

1968), atsirado išimtis, kai baudžiamoji atsakomybė gali būti taikoma ne tik fiziniams, bet ir juridiniams asmenims. Vadovaujantis BK 182 straipsnio 6 dalimi, už šiame straipsnyje 1, 2 ir 3 dalyse numatytas nusikalstamas veikas baudžiamoji atsakomybė gali būti taikoma ir juridiniam asmeniui, jei tai numatyta įstatymuose. Tokiu būdu išplečiamos subjektų ribos sukčiavimo bylose, ypač tais atvejais, kai nusikalstama veika vykdoma organizacijos vardu ar jos naudai.

Kitas būtinas sudėties elementas – subjektyvioji pusė, kuri sukčiavimo atveju pasireiškia tiesiogine tyčia. Tai reiškia, kad kaltininkas suvokia, jog apgaule klaidina kitą asmenį, ir dėl to siekia turtinės naudos sau ar kitam asmeniui. Tiesioginė tyčia yra esminė kaltės forma šio tipo nusikalstamai veikai, todėl jos nebuvimas eliminuoja baudžiamosios atsakomybės taikymo pagrindus.

Bendrininkavimas yra laikytinas pavojingesne sukčiavimo ar bet kurios kitos nusikalstamos veikos padarymo forma. Kasacinės instancijos teismas yra išaiškinęs, kad objektyvieji bendrininkavimo požymiai yra kelių asmenų dalyvavimas padarant nusikalstamą veiką ir jų veikos bendrumas, subjektyvieji - tyčia (savo veiksmų bendrumo suvokimas) ir susitarimas daryti nusikalstamą veiką. Tai reiškia, jog bendrininkavimo atveju, kiekvienas bendrininkas taip pat veikia tiesiogine tyčia – jis suvokia, kad dalyvauja bendrame nusikalstamos veikos įgyvendinime, ir sąmoningai prisideda prie jos įvykdymo. Kiekvieno bendrininko kaltė vertinama individualiai, tačiau visais atvejais turi būti nustatyta, kad jis suvokė bendrą nusikalstamos veikos pobūdį, tikslą bei prisidėjo prie jos įvykdymo.

Bendrininkų grupė yra tada, kai bet kurioje nusikalstamos veikos stadijoje du ar daugiau asmenų susitaria nusikalstamą veiką daryti, tęsti ar užbaigti, jei bent du iš jų yra vykdytojai (BK 25 straipsnio 2 dalis). Tais atvejais, kai tik vienas bendrininkas atliko vykdytojo vaidmenį, o kiti atliko organizatoriaus, kurstytojo ar padėjėjo vaidmenis, bendrininkų grupės aplinkybė neinkriminuotina. Pagal BK 24 straipsnio 3 dalį, vykdytojas yra asmuo, nusikalstamą veiką padaręs pats arba pasitelkęs nepakaltinamus asmenis arba nesulaukusius šio kodekso 13 straipsnyje nustatyto amžiaus asmenis, arba kilus asmenis, kurie dėl tos veikos nėra kalti. Jeigu nusikalstamą veiką padarė keli asmenys kartu, tai kiekvienas iš jų laikomas vykdytoju (bendravykdžiu). Šiame kontekste pabrėžtina, kad bendravykdis yra ne tik tas asmuo, kuris pats realizuoja visus nusikalstamos veikos sudėties objektyviuosius požymius, bet ir tas, kuris realizuoja dalį jų (kasacinės nutartys baudžiamosiose bylose Nr. 2K-605/2007[82], 2K-211/2008[83],

[82] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2007 m. spalio 2 d. nutartis baudžiamojoje byloje Nr. 2K-605/2007“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/81406

[83] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2008 m. gegužės 6 d. nutartis baudžiamojoje byloje Nr. 2K-211/2008“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/86476

2K-197/2009[84], 2K-52-511/2019[85], 2K-278-303/2020[86], 2K-51-788/2022[87] ir kt.).

Tuo tarpu pagal BK 25 straipsnio 4 dalį (*2024 m. kovo 14 d. įstatymo Nr. XIУ-2488 redakcija, galiojusi nuo 2024 m. kovo 16 d., f. y. veikų padarymo melu galiojusi įstatymo redakcija*), organizuota grupė yra tada, kai bet kurioje nusikalstamos veikos stadijoje du ar daugiau asmenų susitaria daryti kelis nusikaltimus arba vieną apysunkį, sunkų ar labai sunkų nusikaltimą ir kiekvienas grupės narys, darydamas nusikaltimą, atlieka tam tikrą užduotį ar turi skirtingą vaidmenį. Pagal naujai įsigaliojusią BK redakciją *(2024 m. balandžio 25 d įstatymo redakcija, remiantis 2024 m. spalio 15 d. įstatymu Nr. XIУ-3033, įsigaliojusi nuo 2025 m. vasario 1 d.*) BK 25 straipsnio 4 dalį, organizuota grupė yra tada, kai du ar daugiau asmenų iš anksto susitaria daryti kelis nusikaltimus arba vieną apysunkį, sunkų ar labai sunkų nusikaltimą ir kiekvienas grupės narys, darydamas nusikaltimą, atlieka tam tikrą užduotį ai turi skirtingą vaidmenį. Pagrindinis skirtumas tarp nurodytų BK 25 straipsnio 4 dalies redakcijų yra tas, jog pagal šiuo metu galiojančią redakciją reikalaujamas išankstinis susitarimas, kai pagal nusikalstamos veikos padarymo metu galiojusią redakciją, susitarimą tarp asmenų taip pat nors ir buvo privalomas, tačiau buvo galimas bet kurioje nusikalstame veikos stadijoje (be kita ko, iki nusikalstamos veikos (-ų) darymo).

Nusikalstamos veikos padarymą organizuotoje grupėje apibūdina tokios aplinkybės kaip apgalvotos nusikalstamos veikos mechanizmo sudėtingumas, veikų padarymo intensyvumas, narių pasiskirstymas vaidmenimis, kiekvieno iš bendrininkų konkrečios užduoties atlikimas siekiant bendro tikslo. Organizuotos grupės nariai paprastai iš anksto aptaria, suderina svarbiausius bendros nusikalstamos veikos momentus, pavyzdžiui parengiamas nusikaltimo padarymo planas, numatomas nusikaltimo pėdsakų slėpimo mechanizmas, bendrininkams nurodomos užduotys, paskirstomi vaidmenys, susitariama dėl nusikaltimo padarymo būdo, vietos, laiko ir pan. (kasacinės nutartys baudžiamosiose bylose Nr. 2K-257/2011[88], 2K-275/2012[89], 2K-453/2012[90], 2K-35/2013[91], 2K-156-788/2016[92], 2K-103-976/2016[93], 2K-109-

[84] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2009 m. birželio 23 d. nutartis baudžiamojoje byloje Nr. 2K-197/2009“. Infolex. Žiūrėta 2025 m. gruodžio 16 d , https://www.infolex.lt/tp/128269

[85] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. kovo 5 d. nutartis baudžiamojoje byloje Nr. 2K-52-511/2019“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1705125

[86] Lietuvos Aukščiausiojo Teismo atrankos kolegijos 2020 m. gruodžio 22 d. nutartis Nr. 2K-278-303/2020, https://www.infolex.lt/tp/1954818

[87] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. kovo 1 d. nutartis baudžiamojoje byloje Nr. 2K-51-788/2022“. Teismų praktika, 2022, Nr. 57, p. 400–411. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2064210

[88] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2011 m. gegužės 31 d. nutartis baudžiamojoje byloje Nr. 2K-257/2011“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/211678

[89] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2012 m. gegužės 29 d. nutartis baudžiamojoje byloje Nr. 2K-275/2012“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/380545

[90] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 2 d. nutartis baudžiamojoje byloje Nr. 2K-453/2012“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/449713

746/2017[94], 2K-178-303/2019[95], 2K-1-719/2020[96], 2K-7-38-1073/2023[97]). Nebūtina, kad kiekvienas narys tiesiogiai realizuotų BK specialiosios dalies straipsnyje nurodytus objektyvius nusikaltimo sudėties požymius. Organizuota grupe veikiantys bendrininkai, nepriklausomai nuo jų vaidmens, laikomi nusikaltimo vykdytojais (Nr. 2K-149-648/2023[98] ir kt.). Svarbus aspektas sprendžiant klausimą dėl organizuotos grupės buvimo yra organizuotumo lygis ir asmens, dalyvaujančio darant nusikaltimą suvokimas priklausant grupei, turinčiai tikslą daryti nusikaltimus.

Taigi šie niuansai ypač svarbūs sukčiavimo kvalifikavime, kadangi tokios veikos dažnai pasižymi sudėtinga teisine sandara ir reikalauja išsamaus vertinimo tiek objektyviųjų, tiek subjektyviųjų požymių aspektu. Nors baudžiamoji teisė sukčiavimą apibrėžia kaip neteisėtą svetimo turto ar turtinės naudos įgijimą apgaule, praktikoje kvalifikavimui lemiančios aplinkybės dažnai paaiškėja tik vertinant konkrečios apgaulės mechanizmą, t. y. kaip ji buvo panaudota, ar ji buvo esminė nukentėjusiojo apsisprendimui, kada laikytina veika baigta ir kokia turtinė žala faktiškai atsirado. Dėl to kiekvienu atveju būtina nustatyti ne tik faktines aplinkybes, bet ir jų atitiktį BK 182 straipsnio sudėčiai, remiantis suformuota teismų praktika. Tai ypač aktualu sukčiavimo atveju, kai kyla klausimų dėl civilinės atsakomybės ribų ir kada tam tikri turtiniai ginčai peržengia civilinės teisės ribas ir patenka į baudžiamosios teisės sritį. Todėl tiriant ir kvalifikuojant sukčiavimą, būtina vadovautis ne tik normomis, bet ir baudžiamosios teisės doktrina, teismų praktika, siekiant teisingo ir pagrįsto atsakomybės taikymo.

---

[91] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2013 m. sausio 29 d. nutartis baudžiamojoje byloje Nr. 2K-35/2013“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/506623

[92] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. gegužės 17 d. nutartis baudžiamojoje byloje Nr. 2K-156-788/2016“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1269445

[93] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-103-976/2016“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1241430

[94] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2017 m. gegužės 16 d. nutartis baudžiamojoje byloje Nr. 2K-109-746/2017“. Teismų praktika, 2017, Nr. 47, p. 572–616. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1475216

[95] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. birželio 20 d. nutartis baudžiamojoje byloje Nr. 2K-178-303/2019“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1740432

[96] „Lietuvos Aukščiausiojo Teismo atrankos kolegijos 2020 m. vasario 27 d. nutartis Nr. 2K-1-719/2020“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1852510

[97] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. birželio 19 d. nutartis baudžiamojoje byloje Nr. 2K-7-38-1073/2023“. Infolex. Žiūrėta 2025 m. gruodžio 16 d ., https://www.infolex.lt/tp/2173033

[98] 46. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. gruodžio 6 d. nutartis baudžiamojoje byloje Nr. 2K-149-648/2023“. Infolex. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2210026

2.2 Sukčiavimo kriminalistinė charakteristika (dalykas, būdas, įrankiai ir priemonės)

Nusikalstamų veikų įrodinėjimas yra svarbiausias baudžiamojo proceso aspektas, kuris atlieka esminį vaidmenį analizuojant praeityje įvykusius nusikaltimus, apimdamas praktinį duomenų (įrodymų) rinkimą ir jų loginį išdėstymą. Kadangi kiekvienas nusikaltimas pasižymi savo unikalumu, kartais reikalaujantis specializuotų tyrimo metodų, dar austrų mokslininkas Hans Gross orientavosi į būtinybę, jog tyrėjai nuolat tobulintų savo žinias ir gebėjimus, įgytų kriminalistinių žinių apie nusikaltimus, siekiant efektyviai analizuoti skirtingas nusikalstamas veikas. Šių pastangų rezultatas atsispindi kriminalistikos mokslo raidoje, kurioje nusikalstamų veikų tyrimo metodikos vystėsi palaipsniui. Nors dar XIX a. kriminalistikos pradininkas H. Gross iškėlė idėją sisteminti nusikalstamų veikų tyrimo principus, tačiau kriminalistinės nusikaltimų charakteristikos sąvoka mokslinėje literatūroje įsitvirtino tik XX a. šeštajame dešimtmetyje. Ši koncepcija, suformuluota Rusijos mokslininkų, tapo svariu metodiniu pagrindu sisteminant nusikaltimų tyrimo procesą. Ji sudarė prielaidas tikslingai nustatyti konkrečių nusikalstamų veikų ypatumus, bei pritaikyti atitinkamus tyrimo veiksmus, paremtus praktiniais duomenimis ir analitiniais kriterijais[99].

Kriminalistinėje literatūroje yra daugybė požiūrių į kriminalistikos kaip mokslo esmę ir nusikaltimų kriminalistinių požymių turinį. Nepaisant ilgai trunkančių diskusijų šia tema, iki šiol nėra visuotinai priimto susitarimo dėl kriminalistinės nusikaltimų charakteristikos apibrėžimo, jo reikšmės bei turinio. S. V. Vinokurov kriminalistinę charakteristiką įvardija kaip moksliškai parengtą tipinių konkrečios nusikaltimų rūšies požymių sistemą, leidžiančią išsiaiškinti pėdsakų susidarymo mechanizmą ir nustatyti pirminius tyrimo uždavinius[100]. V. A. Obrazcov kriminalistinę nusikaltimų charakteristiką apibrėžia kaip nusikaltimo padarymo būdų, pėdsakų, bei kitų objektų santykių aprašymą, kurie turi reikšmės tiek tiriant nusikaltimus, tiek sprendžiant su jais susijusius mokslinius ir praktinius uždavinius. Ši apibrėžtis taip pat apima nusikaltėlių elgesį tiek iki nusikaltimo padarymo, tiek po jo.[101] N. A. Selivanov pastebi, kad kriminalistinė nusikaltimo charakteristika apima ir aplinkybes ar faktus, kurie nors tiesiogiai nepriklauso

[99] Matulienė, Snieguolė. 2004. *Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija.* Daktaro disertacija, Mykolo Romerio universitetas. 4 p., https://cris.mruni.eu/cris/entities/etd/debef03a-a96a-4aad-b47c-6bf84efc5c12

[100] Винокуров С. И. „*Криминалистическая характеристика преступления, ее содержание и роль в построении методики расследования*“. Методика расследования преступления (общие положения). М.: 1976 m., 101 p. cituota iš Гликерман Александр Петрович, Скобина Елена Александровна, „*Криминалистическая характеристика мошенничества на примере судебной практики Забайкальского края*“, Молодой ученый, 2020 m. 183 p., https://moluch.ru/archive/305/68634

[101] Образцов В. А. *Теоретические основы раскрытия преступлений, связанных с ненадлежащим исполнением профессиональных функций в сфере производства*. – Иркутск, 1985. С.8. cituota iš Snieguolė Matulienė, „*Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: Teorinių ir praktinių problemų šiuolaikinė interpretacija*“ daktaro disertacija, Vilnius 2004 m.

nusikalstamai veikai, turi įtakos jos tyrimui.[102] V. E. Kornouchov, kiekvienam nusikaltimui pritaiko specifinių požymių sistemą, kuri vienokiu ar kitokiu mastu apibūdina nusikalstamą veiką. Pavyzdžiui, kalbant apie sukčiavimą, V. E. Kornouchov išskiria tokius požymius: veikos padarymo būdą, kaltininko asmenybę, nusikaltimo motyvą ir tikslą, atlikimo vietą ir laiką, nusikaltimo priemones bei kėsinimosi objektą[103]. S. Kuklianskis ir S. Matulienė kriminalistinę nusikaltimų charakteristiką supranta kaip nusikaltimą apibūdinančių kriminalistiškai svarių (svarbių, turinčių išskirtinę reikšmę) savybių visumą[104]. A. A. Faizulina teigia, jog kriminalistinę charakteristika tikslinga suvokti kaip informacinį modelį, atspindinti esminius nusikalstamos veikos požymius, svarbius jos atskleidimui ir tyrimui[105]. Tuo tarpu V. Šepitko akcentuoja, kad atskiros kriminalistikos metodikos tikslas – sukurti standartizuotas tyrėjų ar prokurorų veiksmų gaires, leidžiančias optimizuoti veiksmų kryptį tiriant specifines nusikaltimų rūšis. Ši metodika pateikia tipiškų patarimų rinkinį, kuris padeda tyrėjams efektyviau tirti tam tikrų rūšių nusikaltimus, pavyzdžiui, vagystes, turto prievartavimus, sukčiavimo atvejus ar teroristinius nusikaltimus[106]. A. Kiseliovo vertinimu, kriminalistinė charakteristika nusikaltimų kompiuterinės informacijos srityje apima tokius elementus kaip kaltininko asmenybė ir jo motyvai, nusikaltimo vieta, laikas ir padarymo būdas bei pagrindinis – techninis komponentas[107]. Dabartinėje mokslinėje literatūroje ir toliau aktyviai analizuojama kriminalistinės nusikaltimų charakteristikos problematika[108]. Mokslininkai siekia naujai interpretuoti kriminalistinės nusikaltimų charakteristikos sąvoką, atsižvelgiant į vykstančius pokyčius technologijų, nusikaltimų tyrimo, teismų praktikos ir visuomenės raidos srityse. Pažymėtina, kad kriminalistinės nusikaltimų charakteristikos klausimą nagrinėja daug platesnis mokslininkų ratas, nei šioje analizėje aptarti autoriai. Tačiau iš analizuotų kriminalistų įžvalgų matyti, kad nepaisant skirtingų formuluočių, galima įžvelgti bendrumų dėl kriminalistinės nusikaltimų charakteristikos

---

[102] Kuklianskis, Samuelis, ir Snieguolė Matulienė. 2002. „Kriminalistinės nusikaltimų charakteristikos samprata.“ *Jurisprudencija* 29(21). 49-65 p., https://ojs.mruni.eu/ojs/jurisprudence/article/view/3581.

[103] В. Е. Корноухов „*Курс криминалистики. Методики расследования насильственных и корыстно- насильственных преступлений*“. 2001 m. 450 p.

[104] Kuklianskis, Samuelis, ir Snieguolė Matulienė. 2002. „Kriminalistinės nusikaltimų charakteristikos samprata.“ Jurisprudencija 29(21). 50 p., https://ojs.mruni.eu/ojs/jurisprudence/article/view/3581.

[105] Файзуллина, А. А. 2017. „К вопросу о соотношении понятий “криминалистическая характеристика преступлений” и “следственная ситуация”“. *Инновационная наука*, 140-142 p. cituota iš: Киселев, Александр Сергеевич, и Ксения Анатольевна Горбунова. 2023. „Особенности криминалистической характеристики преступлений в сфере компьютерной информации“. *Актуальные проблемы государства и права:* 373 p., https://cyberleninka.ru/article/n/osobennosti-kriminalisticheskoy-harakteristiki-prestupleniy-v-sfere-kompyuternoy-informatsii

[106] Shepitko, Valery. 2021. Introduction to Criminalistics. Kharkiv: Apostille Publishing House LLC.,54 p.

[107] Киселев, Александр Сергеевич, и Ксения Анатольевна Горбунова. 2023. „Особенности криминалистической характеристики преступлений в сфере компьютерной информации“. *Актуальные проблемы государства и права:* 373 p.

[108] Sup, Yevhen. 2025. “Forensic Characterization Elements of Criminal Offenses Committed by Professional Participants in Justice.” *Theory and Practice of Forensic Science and Criminalistics*. https://khrife-journal.org/index.php/journal/article/view/650

paskirties, ir pagrindinių jos elementų. Taigi, remdamasis aptartais požiūriais, darbo autorius kriminalistinę nusikaltimų charakteristiką supranta kaip pagalbinį tyrimo įrankį, apimantį tam tikrą informacijos sistemos rinkinį, atsispindinti tipiškus, tam tikro nusikaltimo ir su juo susijusių elementų bruožus. Toks informacijos rinkinys apima duomenis (elementus) apie nusikalstamos veikos padarymo:

- *dalyką (kėsinimosi objektą);*
- *būdą (mechanizmas, nusikaltimo padarymo aplinka, kaltininko palikti pėdsakai);*
- *įrankius ir priemones;*
- *nukentėjusiojo(-ųjų) portretą(-us);*
- *kaltininko(-ų) portretą(-us);*

Nepaisant plačiai pripažįstamos kriminalistinės nusikaltimų charakteristikos reikšmės, mokslinėje literatūroje egzistuoja ir alternatyvių nuomonių, kurios kelia abejonių dėl šios kategorijos savarankiškumo bei mokslinio pagrįstumo. Kai kurie autoriai[109] teigia, kad kriminalistinės charakteristikos samprata neatitinka griežtų mokslinių kategorijų reikalavimų, todėl siūlo atsisakyti šios sąvokos vartojimo. Vietoje to siūloma išskirti tik specifinius įrodinėjimo aspektus konkrečių nusikalstamų veikų rūšių tyrime, neskiriant kriminalistinei charakteristikai savarankiško statuso. Tokie autoriai argumentuoja, kad baudžiamajame procese įtvirtintas įrodinėjimo dalykas jau savaime apima pagrindines aplinkybes, būtinas kiekvienos bylos tyrimui, nepriklausomai nuo nusikalstamos veikos rūšies. Todėl, jų manymu, detali kriminalistinė veikų charakteristika tik dubliuotų jau egzistuojančius teisinius reikalavimus, o jos taikymas praktikoje sukurtų perteklinį informacinį sluoksnį, apsunkinantį tyrimo procesą.

Vis dėlto ši pozicija mokslinėje bendruomenėje laikoma diskusine. Atidžiai analizuojant baudžiamojo proceso normas ir praktiką, akivaizdu, kad įrodinėjimo dalykas apibrėžia tik bendrąsias tyrimo kryptis. Pavyzdžiui, būtinybę nustatyti nusikalstamos veikos padarymo faktą, kaltininko tapatybę, kaltės formą, nusikaltimo padarymo aplinkybes ir kt. Šios aplinkybės, nors ir būtinos kiekvienai nusikalstamai veikai atskleisti, bet yra pernelyg bendro pobūdžio ir neatskleidžia specifinių ypatumų, būdingų skirtingoms nusikaltimų rūšims. Tuo tarpu kriminalistinės nusikaltimų charakteristikos paskirtis yra kitokia. Ji leidžia sistemingai rinkti ir analizuoti tipinius duomenis apie nusikaltimo atlikimo būdus, nusikaltėlių asmenybę, jų motyvus, aplinką, naudojamas priemones bei kitus specifinius faktorius, kurie tiesiogiai padeda tirti konkrečias nusikalstamas veikas[110]. Kaip pažymi S. Matulienė ir L. Novikovienė:

[109] Головин, А. Ю. 2012. *Криминалистическая характеристика преступлений как категория современной криминалистики*. Тула: ТулГУ. 43-46. p., https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-prestupleniy-kak-kategoriya-sovremennoy-kriminalistiki

[110] Ibid. 47-49 p.

„kriminalistinės charakteristikos duomenys konkretizuoja, papildo teisines charakteristikas ir interpretuoja svarbią nusikalstamų veikų tyrimui informaciją taip, kad ji tampa artima pažinimo procesui, turinčiam įrodomąją reikšmę“[111]. Kitaip tariant, kriminalistinė charakteristika veikia kaip metodinis ir informacinis įrankis, kuris, kaip jau buvo minėta, palengvina tyrėjų ar net prokurorų darbą ir leidžia greičiau atpažinti nusikalstamos veikos modelius, kurti pagrįstas versijas ir organizuoti kryptingus tyrimo veiksmus.

Nors Lietuvos Respublikos baudžiamajame kodekse sukčiavimo objektyvieji požymiai suformuluoti universaliai, šiandieninėje praktikoje ši veika vis dažniau įgyvendinama pasitelkiant informacines technologijas bei nuotolinio bendravimo priemones. Sukčiavimas telefonu, SMS žinutėmis, elektroniniais laiškais, pasitelkiant netikras interneto svetaines, socialinių tinklų platformas ar kriptovaliutų schemas, pastaruoju metu vis dažnėja, o tokių veikų tyrimas dažnai kelia praktinių sunkumų. Literatūroje ir praktikoje tokie sukčiavimai įvardijami kaip kibernetiniai[112], internetiniai[113], padaryti elektroninėje erdvėje. Šio pobūdžio sukčiavimas pasižymi įvairiomis atmainomis ir modifikacijomis, kurios nuolat kinta, prisitaikydami prie technologinių pokyčių, nukentėjusiųjų elgsenos ypatumų ir teisėsaugos taikomų priemonių. Skirtingai nei kai kuriose kitose valstybėse[114], Lietuvos Respublikos baudžiamasis kodeksas nenumato atskiros normos sukčiavimui, padarytam pasitelkiant informacines technologijas. Visos tokios nusikalstamos veikos kvalifikuojamos pagal bendrąją BK 182 straipsnio dispoziciją. Dėl šios priežasties šiuolaikinio sukčiavimo, kaip nusikalstamos veikos, teisinis vertinimas ir įrodinėjimas pagal nusikaltimo objektą, subjektą, objektyviąją ir subjektyviąją puses iš esmės išlieka analogiški tradiciniams sukčiavimo padarymo atvejams. Vis dėlto akivaizdu, kad sukčiavimo veikimo būdų kaita ir technologinis šių nusikalstamų veikų pobūdis lemia poreikį peržiūrėti ir adaptuoti kriminalistinę analizę. Šiuolaikinėje kriminalistinėje praktikoje nepakanka apsiriboti vien bendrųjų teisinių kriterijų taikymu. Būtina sistemiškai analizuoti specifinius veikos padarymo būdus, naudojamas technologines priemones, kaltininko elgsenos modelius, tipinius nukentėjusiųjų bruožus bei kitus dalykus.

---

[111] Matulienė, Snieguolė, ir Lina Novikovienė. 2022. „Kriminalistinės nusikalstamų veikų charakteristikos ir kriminalistinės profilaktikos vieta šiuolaikinės kriminalistikos koncepcijoje.“ *Kriminalistikos teorijos plėtra ir teismo ekspertologijos ateitis : kolektyvinė monografija. Liber Amicorum Profesoriui Vidmantui Egidijui Kurapkai*. Vilnius: Lietuvos kriminalistų draugija, Mykolo Romerio universitetas. 93, p. https://cris.mruni.eu/cris/entities/publication/1eab09d3-4b92-40e8-aa22-7729e800ab2e

[112] Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. 2022. "*Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*." Forensic Sciences 2, https://doi.org/10.3390/forensicsci2020028

[113] Fortinet. „Internet Fraud.“ *Fortinet CyberGlossary*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/resources/cyberglossary/internet-fraud

[114] Nikoloska, Svetlana, and Marija Gjosheva. 2021. “Criminal Law, Criminological and Criminalist Aspects of Computer Fraud in the Republic of North Macedonia.”*Security Concepts and Policies – New Generation of Risks and Threats: Proceedings of the International Scientific Conference.* Skopje: Faculty of Security – Skopje, University “St. Kliment Ohridski” – Bitola. 124-125 p. https://eprints.uklo.edu.mk/id/eprint/6808/

Iš baudžiamosios teisinės charakteristikos analizės matyti, jog sukčiavimo dalyku laikomas tiek materialus turtas (kilnojamieji ir nekilnojamieji daiktai), tiek nematerialūs daiktai (akcijos, vertybiniai popieriai, turtinės prievolės ir kt.). Samuelis Kuklianskis ir Snieguolė Matulienė 2002 m. moksliniame straipsnyje „Kriminalistinės nusikaltimų charakteristikos samprata“ pažymėjo: „pasikėsinimo dalykas lemia veiksmus, kuriuos reikia atlikti norint įgyvendinti nusikaltimo kėslus. Nuo pasikėsinimo dalyko daug priklauso nusikaltimo mechanizmas, jo pobūdis“[115]. Dalykas šiuo atveju suprantamas kaip konkreti objekto, į kurį kėsinamasi, apraiška. S. Matulienė savo 2004 m. disertacijoje „Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija“ iš esmės laikosi tos pačios pozicijos, pažymėdama, jog „<...> ne mažiau svarbus yra ir pasikėsinimo dalykas, nuo kurio priklauso nusikaltimo mechanizmas bei jo pobūdis.“[116].

Pažymėtina, kad minėtos nuostatos buvo suformuluotos daugiau nei prieš 20 metų ir pirmiausia buvo taikomos tradicinėje *nusikalstamos veikos padarymo aplinkoje*, siekiant paaiškinti ryšį tarp pasikėsinimo *dalyko* ir nusikalstamos veikos *mechanizmo*. Tuo laikotarpiu pasikėsinimo dalykas dažniausiai buvo suvokiamas kaip materialus objektas, o pats nusikaltimo įgyvendinimas buvo siejamas su tiesioginiu kontaktu tarp kaltininko ir nukentėjusiojo. Tačiau šiuolaikinio sukčiavimo kontekste, kuriame informacinės technologijos ir nuotolinė komunikacija tapo kasdienio gyvenimo dalimi, toks požiūris reikalauja tam tikro atnaujinimo. Šiandien sukčiavimo kėsinimosi dalykas, pavyzdžiui, pinigai, apgaulės būdu gali būti įgyjami tiek tradiciškai, t. y. tiesioginio kontakto metu, tiek nuotoliniu būdu, pasitelkiant informacines technologijas. Dėl to šiuolaikinio sukčiavimo mechanizmą iš esmės lemia ne vien tai, į ką kėsinamasi, bet ir tai, kokiu būdu bei kokioje aplinkoje veika įgyvendinama. Tokiais atvejais lemiamą reikšmę įgyja būtent *nusikaltimo padarymo aplinka*, kurią formuoja visų pirma skaitmenizacijos procesai ir su jais susiję visuomenės elgsenos, įpročių pokyčiai. Papildomai pažymėtina, jog lyginant tradicinę ir elektroninę aplinką, pastaroji sudaro palankesnes sąlygas sukčiavimui dėl galimybės veikti nuotoliniu būdu, pasinaudoti tapatybės slėpimo priemonėmis ir sumažinti tiesioginio identifikavimo riziką. Kartu sutiktina, kad pasikėsinimo dalykas ir šiandien išlieka svarbiu veiksniu, orientuojančiu nusikalstamos veikos mechanizmo kryptį. Pavyzdžiui, kai kėsinamasi į pinigus, kurie yra laikomi banko sąskaitose ar susieti su mokėjimo kortelėmis, apgaulė natūraliai gali būti realizuojama per nuotolinius kanalus, susijusius su prieigos suteikimu, tapatybės patvirtinimu ar mokėjimo inicijavimu. Tačiau vis dėlto esminė aplinkybė

[115] Kuklianskis, Samuelis, ir Snieguolė Matulienė. 2002. „Kriminalistinės nusikaltimų charakteristikos samprata.“ *Jurisprudencija* 29 (21):57 p. https://ojs.mruni.eu/ojs/jurisprudence/article/view/3581

[116] Matulienė, Snieguolė. 2004. *Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija*. Daktaro disertacija, Mykolo Romerio universitetas. 118 p., https://cris.mruni.eu/cris/entities/etd/debef03a-a96a-4aad-b47c-6bf84efc5c12

yra ta, kad toks pasikėsinimo dalyko „pavidalas“ pats savaime yra skaitmenizacijos (aplinkos) procesų rezultatas. Todėl, darbo autoriau vertinimu, sukčiavimo elektroninėje erdvėje mechanizmas priklauso nuo pasikėsinimo dalyko, tačiau pats pasikėsinimo dalykas šiuolaikinėmis sąlygomis yra nulemtas nusikaltimo padarymo aplinkos.

Pasak mokslininkės Jelenos Charinos[117], plačiąja prasme sukčiavimo padarymo aplinką (elektroninėje erdvėje), formuoja:

- dabartinis informacinių technologijų išsivystymo lygis, darantis įtaką nusikalstamų veikų padarymo būdams ir kovos su jomis metodams;
- informacijos prieinamumas ir plačios galimybės įgyti žinių IT srityje, net ir nusikalstamiems tikslams;
- programinės įrangos pažeidžiamumai bei jų užkrėtimas kenkėjiškomis programomis;
- reguliarūs asmens duomenų nutekėjimai, bei sąlyginai nesudėtingas prieinamumas prie jų naudojantis „Dark Web“

Siaurąja prasme nusikaltimo padarymo aplinka siejama su konkrečiomis faktinėmis aplinkybėmis, kurios tiesiogiai daro įtaką nusikalstamos veikos įgyvendinimui. Ji apima nusikaltimą darančio asmens naudojamus *įrankius ir priemones,* ypač tas priemones, kurios leidžia slėpti kriminalistikai svarbią informaciją, taip pat aukos elgesį iki sukčiavimo padarymo, jo metu ir po jo ir pan[118]. Remiantis išdėstytu, manytina, jog nusikaltimo padarymo aplinką tikslinga vertinti ne kaip savarankišką kriminalistinės charakteristikos elementą, o kaip sukčiavimo padarymo būdo sudedamąją dalį. Darbo autoriaus vertinimu, elektroninėje erdvėje technologinė ir socialinė aplinka iš esmės įsilieja į sukčiavimo įgyvendinimo mechanizmą ir lemia konkrečių veiksmų seką.

Atsižvelgiant į tai akcentuotina, jog šiandieninė skaitmenizuota visuomenė, kurioje vis plačiau taikomos nuotolinės komunikacijos formos, elektroniniai pirkimai ir pardavimai, natūraliai sudaro palankią terpę tokio pobūdžio sukčiavimui. Šios nusikalstamos veikos subjektai pasirenka virtualią veiklos erdvę, nes ji, viena vertus, aktuali, tendencinga, o kita vertus – suteikia galimybę išlaikyti anonimiškumą. Auka beveik visada nemato kaltininko, nežino jo

[117] Харина, Елена Алексеевна. 2024. *Особенности методики расследования мошенничества в сфере компьютерной информации.* Диссертация на соискание ученой степени кандидата юридических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования „Красноярский государственный аграрный университет“. 71, 72, p., https://kubsau.ru/upload/iblock/500/m0oh4gpjtj0xoc5qcwm213n43ghqy23d.pdf

[118] Смирнова, Вероника Сергеевна. 2025. „*Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий*“. Институт публичного права и управления, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА). 92 p., https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-moshennichestva-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy-1

tapatybės, kartais turi mažiau galimybių įvertinti situacijos riziką realiuoju laiku, o informacijos pertekliaus aplinkoje lengviau manipuliuoti jos sprendimais. Dėl šių priežasčių, darbo autoriaus vertinimu, būtent šios nusikalstamos veikos pobūdis šiuolaikiniame kontekste labiau priklauso ne tiek nuo dalyko, kiek nuo socialinių ir technologinių aplinkybių (nusikaltimo padarymo aplinkos), kuriose nusikaltimas įvykdomas. Taigi tai leidžia teigti, kad kiekvienos nusikalstamos veikos pobūdis reikalauja individualaus vertinimo, bei tai, jog kriminalistinė charakteristika negali būti taikoma universaliai.

Vienu svarbiausiu kriminalistinės charakteristikos elementu laikomas nusikalstamos veikos padarymo būdas. Kriminalistikoje nusikaltimo būdo sąvoka suprantama plačiau nei baudžiamojoje teisėje. Kaip pažymi Snieguolė Matulienė savo daktaro disertacijoje[119], baudžiamosios teisės doktrinoje nusikaltimo būdas dažnai turi ribotą reikšmę. Nusikalstamos veikos padarymo būdas gali būti tiek kvalifikuojanti, tiek sunkinanti aplinkybė, kadangi BK straipsnių dispozicijose nusikalstamos veikos dažnai pateikiamos apibendrintai, be detalesnių techninių ar praktinių aspektų. Ši mintis ypač aktuali analizuojant šiuolaikinio sukčiavimo sudėtį, kadangi Lietuvos Respublikos baudžiamajame kodekse kalbama tik apie apgaulės būdu įgyjamą turtą ar turtinę teisę, išvengtą ar panaikintą turtinę prievolę ir nenurodoma, kokiomis konkrečiomis priemonėmis ar būdu tai gali būti įgyvendinama. Tuo tarpu kriminalistikoje nusikaltimo būdas įgyja papildomą praktinę ir taktinę prasme. Anot S. Matulienės, jeigu baudžiamojoje teisėje nusikaltimo būdas padeda išryškinti pačią veiką, tai kriminalistikos kontekste jis tampa vienu pagrindinių įrankių įtariamojo ar galimų įtariamųjų rato nustatymui. Nusikaltimo būdas siejamas su pėdsakų susidarymo mechanizmu, kuris gali būti rekonstruojamas pagal loginę seką: būdas → sąveikos pobūdis → nusikaltimo pėdsakai. Ši schema leidžia kriminalistams ne tik įrodyti tam tikrą veikos padarymo būdą, bet ir remiantis aptiktais pėdsakais ieškoti kitų su veikos padarymų susijusių įkalčių. Be to, kaip nurodo mokslininkė, būdo pasikartojimų nustatymas gali turėti įrodomąją reikšmę, t. y. jei tyrimo metu paaiškėja, kad asmuo ir ankščiau yra veikęs tokiu pačiu būdu, tai leidžia susieti kelis epizodus ar nustatyti nusikalstamo elgesio modelį[120]. Tačiau prieš pradedant plačiau analizuoti sukčiavimo būdą kaip kriminalistinės charakteristikos elementą, tikslinga aptarti tokių vartojamų terminų įvairovę kaip: *„elektroninė erdvė“, „kibernetinė erdvė“, „internetas“* reikšmės bei jų tarpusavio santykį.

Anot daugelio mokslininkų ir praktikų, tokio pobūdžio veikos dažnai apibūdinamos įvairiais artimos reikšmės terminais, tokiais kaip – *„kibernetiniai nusikaltimai“, „elektroniniai*

[119] Matulienė, Snieguolė. 2004. *Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija*. Daktaro disertacija, Mykolo Romerio universitetas. 50 p.,

[120] Ibid. 50, 51 p.

nusikaltimai“, „kompiuteriniai nusikaltimai“, „nusikaltimai elektroninėje erdvėje“ ir t. t. Vertinant šių terminų vartoseną Lietuvos nacionalinėje teisės sistemoje, pažymėtina, kad tiriant sukčiavimo atvejus specifinėje terpėje, remiamasi Lietuvos Respublikos generalinio prokuroro patvirtintomis metodinėmis rekomendacijomis dėl sukčiavimo elektroninėje erdvėje nusikalstamų veikų kvalifikavimo ir tyrimo[121]. Jau iš pačių rekomendacijų pavadinimo matyti, kad Lietuvos baudžiamojoje teisėje prioritetiškai vartojamas terminas „elektroninė erdvė“. Tačiau atkreiptinas dėmesys, kad pačiose rekomendacijose šio termino apibrėžimas nėra pateikiamas. Terminų neapibrėžtumo problematika atsiskleidžia ir Europos Sąjungos lygmeniu. 2001 m. priėmus Europos Tarybos Budapešto konvenciją dėl elektroninių nusikaltimų[122], praktikoje pradėtas vartoti nusikaltimų elektroninėje erdvėje terminas, nors iki tol dažniau buvo vartojamas kompiuterinio nusikaltimo terminas. Pačioje konvencijoje minimos ir tokios sąvokos kaip: „*elektroniniai nusikaltimai“, „nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui“, „kompiuteriniai nusikaltimai“*. Tačiau ir šioje Konvencijoje nėra pateiktas aiškus termino „*elektroniniai nusikaltimai*“ apibrėžimas. Amerikiečių mokslininkas Lance Strate, apibūdinant šią specifinę erdvę pažymi, jog ši erdvė yra nuolat prieinama ir tarsi esanti šalia, tačiau jos buvimo vieta sunkiai apibrėžiama, kadangi ji nepavaldi fizinėms ar valstybių sienų riboms. Tokie įrenginiai kaip nešiojamieji kompiuteriai ar išmanieji telefonai atlieka tik tarpininko funkciją, užtikrinančią ryšį tarp asmenų, esančių skirtinguose pasaulio regionuose. L. Strate įvardina šią terpę *„kibernetinės erdvės“* terminu[123]. Pažymėtina, kad pats šio termino atsiradimas nėra susijęs su kriminalistika. Pirmą kartą žodžių junginį „kibernetinė erdvė“ 1982 m. pavartojo rašytojas William Gibson savo mokslinės-fantastikos kūrinyje, šią erdvę apibūdindamas kaip virtualią aplinką kompiuterinių tinklų viduje, su kuria žmogus gali sąveikauti[124]. Remdamasis L. Strate požiūriu, lietuvių mokslininkas Gediminas Bučiūnas, siekiant išvengti painiavos vartojamoje terminologijoje, siūlo vartoti terminą *„kibernetinė erdvė“*, apibūdinant erdvę, apjungiančią telekomunikacinius, informacinius

[121] Lietuvos Respublikos Prokuratūra. 2014. *Rekomendacijos dėl ikiteisminio tyrimo organizavimo ir atlikimo tiriant elektroninius sukčiavimus.* Patvirtinta 2014 m. vasario 10 d. generalinio prokuroro raštu Nr. 12.14-40. Žiūrėta 2025 m. gruodžio 17 d. https://www.prokuraturos.lt/data/public/uploads/2015/12/rek-del-el-sukciavimu-2014-02-10.pdf

[122] Council of Europe. 2001. *Convention on Cybercrime (Budapest Convention). Budapest*: Council of Europe. Žiūrėta 2025 m. gruodžio 17 d., https://rm.coe.int/1680081561

[123] Lance Strate, Ronald L. Jacobson, and Stephanie B. Gibson, eds*., Communication and Cyberspace: Social Interaction in an Electronic Environment* (Cresskill, NJ: Hampton Press, 2002) cituojama iš: Bučiūnas, Gediminas. 2015. „*Terminų vartojimas tiriant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui*.“ Visuomenės saugumas ir viešoji tvarka 13:14 p. https://www.lituanistika.lt/content/73376

[124] Henthorne T. William Gibson: A Literary Companion. Jefferson: McFarland & Company, 2011. 176 p., cituota iš: Киселев, Александр Сергеевич, и Ксения Анатольевна Горбунова. 2023. „Особенности криминалистической характеристики преступлений в сфере компьютерной информации“. Актуальные проблемы государства и права: 372, p., https://cyberleninka.ru/article/n/osobennosti-kriminalisticheskoy-harakteristiki-prestupleniy-v-sfere-kompyuternoy-informatsii

tinklus ir sistemas, elektroninę įrangą, kurioje vykdomos nusikalstamos veikos[125]. Tą pačią problemą dėl terminų painiavos iškelia ir prof. dr. Darius Štitilis, kuris pažymi, jog šiuolaikinėje informacinėje visuomenėje sąvokos *„internetas“* ir *„elektroninė erdvė“* dažnai vartojamos kaip sinonimai, nors jų turinys iš esmės skiriasi. Mokslininko teigimu: „*elektroninė erdvė* – tai nepriklausoma, neturinti fizinių ar teisinių sienų komunikacijos aplinka, neturinti centralizuoto valdymo ar centralizuotų kontrolės mechanizmų, o internetas turėtų būti suprantamas tik kaip vienas iš elektroninės erdvės elementų“ [126]. Dėl to, anot D. Štitilio, net ir vietinis kompiuterių tinklas, neprijungtas prie interneto, taip pat sudaro elektroninės erdvės dalį[127]. Terminologijos painiava atsiskleidžia ir velėsniuose Europos Sąjungos dokumentuose. Europos Komisijos 2007 m. komunikato, skirto kovai su elektroniniais nusikaltimais[128], pavadinime anglų kalba vartojamas terminas „*cyber crime“*[129], kuris tiek tarptautiniuose dokumentuose, tiek mokslinėje literatūroje dažniausiai atitinka sąvoką *kibernetiniai nusikaltimai*. To paties 2007 m. komunikato oficialiame vertime į lietuvių kalbą naudojamas kitas terminas – *elektroniniai nusikaltimai*. Neatitikimą patvirtina ir ankščiau minėta Europos Tarybos 2001 m. Budapešto konvencija dėl elektroninių nusikaltimų (angl. *Convention on Cybercrime*), kurioje taip pat įtvirtintas terminas „*cybercrime“,* nors oficialiuose lietuviškuose vertimuose vartojama sąvoka „*elektroniniai nusikaltimai*“. Toks neatitikimas sudaro prielaidas, kad net ir ES lygmeniu trūksta terminologinio nuoseklumo, kas gali sukelti painiavą, nagrinėjant nusikalstamas veikas elektroninėje ar kibernetinėje erdvėje.

Apibendrinant, galima teigti, kad nors sąvokos „internetas“ ir „elektroninė erdvė“ kartais vartojamos kaip sinonimai, jų turinys nėra tapatus. Internetas tėra vienas iš elektroninės erdvės elementų. Tuo tarpu sąvokos „elektroniniai nusikaltimai“, „kibernetiniai nusikaltimai“ bei „elektroninė erdvė“ ir „kibernetinė erdvė“, nors iš pirmo žvilgsnio gali skirtis tiek pagal prasmę,

---

[125] Bučiūnas, Gediminas. 2015. „*Terminų vartojimas tiriant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui*.“ Visuomenės saugumas ir viešoji tvarka:14 p. https://www.lituanistika.lt/content/73376

[126] Štitilis, Darius, Paulius Pakutinskas, Marius Laurinaitis, ir Inga Dauparaitė. 2011. *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai.* Vilnius: Mykolo Romerio universitetas. 32,33 p., https://cris.mruni.eu/cris/bitstreams/a736de82-f1c9-449d-b91a-10401e0b1b4a/download

[127] Štitilis, D. 2003. Prekių ženklų naudojimas elektroninėje erdvėje: teisiniai aspektai, Jurisprudencija 41(33): 141 p. cituota iš: Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis, ir Inga Dauparaitė, *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai* (Vilnius: Mykolo Romerio universitetas, 2011 m., 32,33 p. https://cris.mruni.eu/cris/bitstreams/a736de82-f1c9-449d-b91a-10401e0b1b4a/download

[128] Europos Komisija. 2007. *Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų Komitetui – Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme,* KOM(2007) 267 galutinis, SEK(2007) 641, SEK(2007) 642. Briuselis. Žiūrėta 2025 m. gruodžio 17 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:52007DC0267

[129] European Commission. 2007. *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a General Policy on the Fight against Cyber Crime* COM(2007) 267 final. Žiūrėta 2025 m. gruodžio 17 d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0267

tiek taikymo kontekstu, Lietuvos teisinėje praktikoje gali būti vartojamos kaip tapačios reikšmės terminai. Šį terminų tapatumą patvirtina oficialių Europos Sąjungos dokumentų vertimo analizė, t. y. terminui „*cybercrime*“ lietuviškuose vertimuose taikomas atitikmuo „*elektroniniai nusikaltimai*“. Darbo autoriaus vertinimu, šie skirtumai yra daugiau lingvistinio nei teisinio ar praktinio pobūdžio, todėl tiek nusikaltimų, tiek veikos erdvės sąvokos gali būti laikomos tapačiomis. Remiantis tuo, pažymėtina, kad nors Lietuvos Respublikos teisės aktuose nėra aiškaus elektroninės erdvės apibrėžimo, Lietuvos Respublikos kibernetinio saugumo įstatymo 2 straipsnio 10 dalyje[130] pateikiama kibernetinės erdvės sąvoka, kuri apibrėžiama kaip aplinka, kurią sudaro kompiuteriai ir kita tinklų ir informacinių technologijų įranga ir juose sukuriami ir (ar) jais perduodami skaitmeniniai duomenys. Darbo autoriaus nuomone, minėtų sąvokų apibrėžimų trūkumą galima sieti su sparčiu technologijų vystymusi, todėl griežti apibrėžimai gali greitai prarasti aktualumą. Atsižvelgiant į šį sąvokų santykį ir reikšmę, toliau galima aptarti, kas laikytina elektroniniais (kibernetiniais) nusikaltimais.

Europos Komisijos komunikate dėl bendrosios politikos kovai su elektroniniais nusikaltimais[131] nurodoma, jog elektroniniais nusikaltimais laikomos nusikalstamos veikos, padarytos naudojant elektroninių ryšių tinklus ir informacines sistemas arba nukreiptos prieš tokius tinklus ir sistemas. Atkreiptinas dėmesys, kad D. Štitilio išsakytas požiūris[132] leidžia pagrįstai abejoti minėto termino „elektroniniai nusikaltimai“ tikslumu apibūdinant nusikalstamas veikas, vykdomas elektroninėje erdvėje. Šis terminas, pasak autoriaus, gali būti klaidinančiai siejamas su elektronikos mokslu, kuris apima tokias sritis kaip televizija, radijo technologijos ar automobilių pramonė, kuriose dominuoja analoginiai signalai. Tuo tarpu nusikalstamos veikos, kurios įvardijamos kaip „cybercrime“, yra labiau susijusios su kompiuterija, informatikos inžinerija ir skaitmeninių duomenų apdorojimu. Esminis bruožas yra tai, kad tokių veikų objektas dažniausiai yra skaitmenine (angl. digital) forma pateikiama informacija. Pats terminas „cybercrime“ kilo iš sąvokos „cyberspace“, kuri lietuviškai verčiama kaip „elektroninė erdvė“. Su tokiu Dariaus Štitilio požiūriu iš esmės sutinka ir informacinių sistemų katedros mokslininkai Nikolaj Goranin ir Dalius Mažeika, kurie, aptardami nusikalstamas veikas specifinėje aplinkoje, vartoja terminą „nusikaltimai elektroninėje erdvėje“. Pasak mokslininkų, nusikaltimai elektroninėje erdvėje apima tokias veikas, kurioms atlikti naudojami kompiuteriai ar kiti

[130] Lietuvos Respublikos kibernetinio saugumo įstatymas“. 2014. TAR, 2014-12-23, Nr. 2014-20553. Žiūrėta 2025 m. gruodžio 17 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.325977/asr

[131] Europos Komisija. 2007. *Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų Komitetui – Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme,* KOM(2007) 267 galutinis, SEK(2007) 641, SEK(2007) 642. Briuselis. Žiūrėta 2025 m. gruodžio 17 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:52007DC0267

[132] Štitilis, Darius. 2011. Elektroniniai nusikaltimai. Vilnius: Mykolo Romerio universitetas. 6 p. https://cris.mruni.eu/cris/bitstreams/ef36e100-b123-46b9-b67f-7631ca9498a5/download

išmanieji elektroniniai įrenginiai, siekiant neteisėtai perimti, sugadinti, sunaikinti, pašalinti duomenis, sutrikdyti ar nutraukti informacinės sistemos darbą, kai kompiuterinė ar programinė įranga yra nusikaltimo objektas ar įrankis, ir kitos neteisėtos veikos, susijusios su skaitmenine informacija ir jos apdorojimu[133]. Taigi, darytina išvada, jog kai sukčiavimas padaromas pasitelkiant informacines sistemas ar telekomunikacijų priemones – yra nusikalstama veika elektroninėje erdvėje. Todėl ir Lietuvos teisinėje praktikoje pagrįstai vartojamas terminas „nusikaltimai elektroninėje erdvėje“ ir kalbant apie tokio pobūdžio sukčiavimą.

Tęsiant temą apie sukčiavimo būdą kriminalistiniu požiūriu, S. Matulienė savo 2004 m. daktaro disertacijoje pažymi, kad to meto kriminalistinėje literatūroje nebuvo vieningo nusikaltimo būdo apibrėžimo. Buvo keliami klausimai, ar būdas būdingas visoms nusikalstamoms veikoms (įskaitant neatsargias), ar jis apima laiką bei vietą, ar privalo apimti visas veikos stadijas. Nepaisant šių požiūrių skirtumų, dauguma mokslininkų sutarė, kad nusikaltimo būdas yra svarbus informacijos šaltinis apie veikos kokybinius aspektus. Į šią sąvoką įeina ne tik kaltininko veiksmai (veikimas/neveikimas), bet ir nusikaltimo įrankiai bei priemonės, padarymo vieta, laikas. Taip pat pabrėžiama, kad būdas apima visus veikos etapus, t. y. nuo pasirengimo, veikos padarymo ir iki jos slėpimo etapo ir priklauso tiek nuo objektyvių, tiek nuo subjektyvių veiksnių[134].

Sutiktina, jog nusikalstamos veikos būdas priklauso nuo įvairių objektyvių (situacinių) ir subjektyvių (asmeninių) veiksnių visumos, kuri sudaro vadinamąjį nusikalstamo elgesio mechanizmą[135]. Kartais nusikalstamos veikos subjektas pasirenka sukčiavimo būdą, pasinaudodamas esamomis visuomeninėmis aplinkybėmis, tokiomis kaip teisės aktų spragos, gyventojų informuotumo stoka (prevencijos nepakankamumas), pasitikėjimas elektroninėmis paslaugomis[136] ar visuotinės krizės (pandemija, karas ir kt.). Vis dėlto ne mažiau aktualios ir individualios šios nusikalstamos veikos subjekto savybės, pavyzdžiui paties sukčiaus turimos technologinės žinios, gebėjimas naudotis moderniais įrankiais bei kūrybiškumas. Tokie asmenys taiko sudėtingas socialines inžinerijos taktikas, išnaudoja dirbtinio intelekto sistemas, automatizuoja bendravimą ar kuria įtikinamą, klaidinančią informaciją. Visa tai leidžia

---

[133] Nikolaj Goranin, Dalius Mažeika, Nusikaltimai elektroninėje erdvėje ir jų tyrimų metodikos, (Kaunas: 2011), 16 p., cituojama pagal Rasa Pažėrienė, Nusikaltimų elektroninėje erdvėje atskleidimo teisiniai ir praktiniai ypatumai, magistro baigiamasis darbas, Mykolo Romerio universitetas, Kaunas, 2021, https://cris.mruni.eu/cris/entities/etd/6ae160d4-a0e5-4b30-a296-af830d993d0b

[134] Matulienė, Snieguolė. 2004. *Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija*. Daktaro disertacija, Mykolo Romerio universitetas 51-54 p. https://cris.mruni.eu/cris/entities/etd/debef03a-a96a-4aad-b47c-6bf84efc5c12

[135] Justickis, Viktoras. 2001. *Kriminologija. 1 dalis: vadovėlis.* Vilnius: Lietuvos teisės universiteto Leidybos centras. 189 p., https://cris.mruni.eu/cris/entities/publication/532f2d65-74b9-4fb1-8158-e22bd4fbc659

[136] 15min. „Naujas sukčiavimo būdas: sukčiai naudojasi E. sveikatos portalo vardu.“ *15min.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.15min.lt/naujiena/aktualu/nusikaltimaiirnelaimes/naujas-sukciavimo-budas-sukciai-naudojasi-e-sveikatos-portalo-vardu-59-2356332

nusikalstamos veikos subjektui pasirinkti tokį būdą, kuris geriausiai atitinka jo įgūdžius ir siekiamą auditoriją.

Sukčiavimo padarymo būdas elektroninėje erdvėje išsiskiria tuo, kad ši veika padaroma specifinėje terpėje, panaudojus apgaulę. Apgaulės pobūdis priklauso nuo konkrečios veiklos srities, kurioje ji planuojama ir nuo pasirinkto sukčiavimo modelio. Sukčiavimo būdas glaudžiai susijęs ir su pasirenkamomis techninėmis priemonėmis – būtent jos dažnai lemia, kaip konkrečiai įgyvendinama apgaulė ir kokiu mastu veika realizuojama. Darbo autoriaus nuomone, sukčiavimo elektroninėje erdvėje būdas, kaip kriminalistinės charakteristikos elementas, gali būti analizuojamas dvejopai, t. y. pagal apgaulės turinį (pretekstą – kokią informaciją subjektas pateikia aukai, siekdamas ją suklaidinti) ir pagal jos techninį įgyvendinimą (specifinė apgaulė). Pažymėtina ir tai, kad tam tikri techniniai sukčiavimo metodai, tokie kaip pavyzdžiui „phishing“ (apgaulingų el. laiškų siuntimas), „smishing“ (SMS žinutės su fiktyviomis nuorodomis) galima vertinti kaip ir atskirą sukčiavimo kriminalistinės charakteristikos elementą – *įrankiai ir priemonės*, kuriomis realizuojamas konkretus apgaulės būdas. Šiuo aspektu aktuali D. Štitilio pozicija, jog: „kompiuteriniais nusikaltimais laikomos baudžiamojo įstatymo nustatytos visuomenei pavojingos veikos, kai kompiuterinė informacija yra nusikaltimo dalykas arba kai kompiuteris panaudojamas kaip nusikaltimo priemonė. Kitais žodžiais tariant, pasikėsinimo dalykas yra informacija, apdorojama kompiuterinėje sistemoje, o kompiuteris yra nusikaltimo įrankis. Šių nusikaltimų objektas skiriasi“[137]. Remiantis tokia D. Štitilio pozicija, darbo autoriaus manymu, siekiant nuoseklumo sukčiavimo kriminalistinės charakteristikos analizėje, techniniai sukčiavimo metodai (fišingas, smišingas ir pan.) visų prima turėtų būti priskiriami prie sukčiavimo kriminalistinio elemento – *būdo*, t. y. specifinės apgaulės įgyvendinimo formos. Tuo tarpu tokie techniniai įrenginiai (įrankiai) kaip kompiuteriai, išmanieji telefonai, planšetės ir kt. bei priemonės (kenkėjiškos, tapatybės maskavimo programos ir pan.) per kuriuos šie apgaulės metodai realizuojami, laikytini – *įrankiais ir priemonėmis*.

Pažymėtina, jog nors dalis kriminalistikos klasikų, kaip pažymį S. Matulienė, nusikaltimo būdą aiškina plačiai – kaip veiksmų, įrankių, aplinkybių ir stadijų visumą, toks požiūris yra pagrįstas, tačiau darbo autoriaus vertinimu, sukčiavimo elektroninėje erdvėje kontekste yra perteklinis. Darbo autoriaus vertinimu, *įrankius ir priemones* tikslinga vertinti kaip atskirą kriminalistinės charakteristikos elementą, nes analizuojant sukčiavimą vykdomą specifinėje – elektroninėje erdvėje, kur itin svarbus tampa informacinių technologijų vaidmuo, būtina aiškiau atriboti apgaulės turinio bei jos įgyvendinimo schemą būtent nuo konkrečių techninių įrankių ar priemonių per kurias ši apgaulė realizuojama. Toks atskyrimas leidžia

[137] Štitilis, Darius. 2011. Elektroniniai nusikaltimai. Vilnius: Mykolo Romerio universitetas. 6 p. https://cris.mruni.eu/cris/bitstreams/ef36e100-b123-46b9-b67f-7631ca9498a5/download

išskirti du savarankiškus kriminalistinės reikšmės elementus. *Būdas*, kuris apima nusikalstamos schemos esmę, t. y. yra, kaip veika buvo suplanuota ir įvykdyta apgaulės požiūriu bei *įrankius ir priemones*, kurie suprantami kaip techniniai įrenginiai (kompiuteris, išmanusis telefonas ir kt.) ir priemonės (kenkėjiškos, tapatybės maskavimo programos). Techniniai įrankiai ir priemonės kriminalistiniu požiūriu turi savitą reikšmę dėl savo techninių parametrų ir funkcinių ypatumų. Pavyzdžiui naudojamos specialios programos, skirtos neteisėtai duomenims rinkti[138], automatizuotoms apgaulingoms žinutėms siųsti (automatizuotas smishing'as)[139], peradresuoti telefono numerį, ar fiktyviems tinklalapiams generuoti[140]. Šios priemonės gali būti pritaikytos konkretiems nusikalstamiems tikslams, įrenginiuose gali būti įdiegta specializuota kenkėjiška ar klaidinanti programinė įranga, kurių analizė leidžia nustatyti net tik nusikaltimo vykdymo mechanizmą, bet ir asmens kvalifikaciją, nusikalstamo elgesio sudėtingumą bei pasirengimo lygį. Dėl šios priežasties *įrankių ir priemonių* vertinimas kaip atskiro kriminalistinio elemento, tačiau glaudžiai siejamo su *būdu* (kitu elementu) – yra būtinas. Šių elementų atskyrimas (konkretizavimas) visų pirma leistų išvengti „painiavos", analizuojant sukčiavimo *būdų bei įrankių ir priemonių* ypatumus, bei padėtų ne tik rekonstruoti veikos pasiruošimo, veikos padarymo ir jos slėpimo etapus, bet galimai ir susieti atskirus nusikalstamus epizodus, atskleisti veikimo modelius bei galiausiai plačiau apžvelgti šiuos sukčiavimo elektroninėje erdvėje kriminalistinės charakteristikos elementus.

Be to, atkreiptinas dėmesys, kad toks būdo ir techninių įrankių bei priemonių atribojimas turi ne tik kriminalistinę, bet ir baudžiamosios teisės taikymo reikšmę. Praktikoje vis dažniau susiduriama su situacijomis, kai sukčiavimo elektroninėje erdvėje padarymui pasitelkiamos vadinamosios dvejopo naudojimo (angl. dual-use) techninės priemonės ar programinė įranga, kurios pačios savaime nėra neteisėtos ir gali būti pavyzdžiui, skirtos informacinių technologijų produktų patikimumo, saugumo testavimui t.t. (2K-199-648/2019[141]) Dėl šios priežasties, siekiant išvengti nepagrįsto baudžiamosios atsakomybės taikymo, būtina aiškiai atriboti, kada tokios priemonės vertintinos kaip neutralūs techniniai įrankiai, o kada – kaip nusikalstamos veikos įrankiai, panaudoti turint tiesioginį ketinimą padaryti nusikalstamą

[138] Fortinet. „Spyware." *Fortinet CyberGlossary*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/resources/cyberglossary/spyware

[139] Insights2Techinfo. „The Rise of AI Smishing: Protecting Yourself from Next-Gen Scams." *Insights2Techinfo*, žiūrėta 2025 m. gruodžio 17 d., https://insights2techinfo.com/the-rise-of-ai-smishing-protecting-yourself-from-next-gen-scams/

[140] Ironscales. „Clone Phishing." *Ironscales*, žiūrėta 2025 m. gruodžio 17 d. https://ironscales.com/guides/phishing-prevention/clone-phishing

[141] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019.". *Infolex.* 2019, Nr. 52, p. 387–403 https://www.infolex.lt/tp/1744638

veiką BK 198-2 straipsnio prasme. (2K-188-489/2015[142]). Tokiu būdu bus aiškiau, kas sudaro pačią apgaulės esmę (būdą), o kas yra tik priemonės, padedančios ją įgyvendinti.

Sukčiavimo subjektai dažniausiai renkasi tokį veikimo modelį, kuris atitinka jų turimas technologines galimybes. Tačiau neretai tam tikslui subjektai pasitelkia ir kitus asmenis, kurie pasižymi informacinių technologijų išmanymu ir kurie padeda kurti ar įgyvendinti apgaulingas schemas elektroninėje erdvėje. Tokie asmenys (bendrininkai) gali būti atsakingi už techninių priemonių parengimą, fiktyvių svetainių kūrimą, žalingų programų ar apgaulingų pranešimų siuntimo automatizavimą ir kitus veiksmus, kurie padeda realizuoti apgaulę. Pastaruoju metu, elektroninėje erdvėje atsirado daug įvairių sukčiavimo būdų, kur technologijų pažanga sudaro sąlygas tiek masiškesnei, tiek individualizuotai apgaulei vykdyti. Atsižvelgiant į planuojamą apgaulės mąstą, iš esmės skiriasi tiek pasiruošimo sukčiavimui pobūdis, tiek pėdsakų slėpimo niuansai. Žemiau pateikiami dažniausiai pasitaikantys sukčiavimo atvejai pagal apgaulės pretekstą (t. y. melagingą informaciją, kuri pateikiama aukai, siekiant ją suklaidinti ir neteisėtai įgyti jos turtą ar duomenis), remiantis praktikoje bei viešojoje erdvėje dažnai minimais pavyzdžiais tiek Lietuvoje, tiek užsienyje:

- *Pretekstu įsigyti prekę, išsinuomoti turtą ar gauti paslaugą (auka raginama sumokėti avansą ar rezervacijos mokestį, tačiau prekė ar paslauga nesuteikiama (tipinis avansinis sukčiavimas))[143];*
- *Pretekstu įsigyti prekes (pvz. drabužius ar buitinę elektroniką) už itin patrauklią kainą per suklastotą internetinę parduotuvę (aukai pateikiama, arba surandama savarankiškai fiktyvi arba suklastota populiarios e. prekybos svetainės versija, kurioje atlikus apmokėjimą, prekės nepristatomos, o pateikti asmens ar mokėjimo duomenys gali būt panaudoti ir kitoms nusikalstamoms veikoms);*
- *Pretekstu pasiūlyti lengvą ar greitą uždarbio galimybę (žadamas pelnas ar darbo pasiūlymas, už kurį prašoma sumokėti „registracijos mokestį“ ar pateikti duomenis)[144];*
- *Pretekstu užmegzti pažintį socialiniuose tinkluose (romantinis sukčiavimas – pasinaudojama emociniu ryšiu, kad būtų išvilioti pinigai (dažnai ilgo bendravimo metu))[145];*
- *Pretekstu, kad užblokuota elektroninė piniginė ar banko sąskaita (pateikiamas*

[142] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015“. *Infolex.* https://www.infolex.lt/tp/1048281

[143] Vilniaus apskrities vyriausiasis policijos komisariatas. „Sukčiavimas apsiperkant internetu.“ *Vilnius.policija.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d., https://vilnius.policija.lrv.lt/lt/policija-pataria/sukciavimu-prevencija/sukciavimas-apsiperkant-internetu/

[144] Indeed. „Data Entry Job Scam: How To Spot and Avoid It.“ *Indeed Career Guide*, žiūrėta 2025 m. gruodžio 17 d., https://www.indeed.com/career-advice/finding-a-job/data-entry-job-scam

[145] Federal Bureau of Investigation. „Romance Scams.“ *FBI.gov*, žiūrėta 2025 m. gruodžio 17 d., https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams

melagingas pranešimas, siekiant išvilioti prisijungimo duomenis (phishing, smishing))[146]*;*

- *Pretekstu apie tariamą laimėjimą žaidime ar loterijoje (žadamas prizas, bet prašoma sumokėti „mokestį“, pateikti asmens ar kortelės duomenis)*[147]*;*
- *Pretekstu, kad reikalinga skubi finansinė pagalba (aukai skambina asmuo, apsimetantis draugu ar artimuoju, kuris neva pateko į nelaimę ir prašo pinigų (arba renkamos „paramos“))*[148]*;*
- *Pretekstu atnaujinti paskyros duomenis ar slaptažodį (siunčiami fiktyvūs pranešimai iš tariamų institucijų (bankų, „Google“, socialinių tinklų), siekiant gauti prisijungimo duomenis)*[149]*;*
- *Pretekstu dėl neapmokėtos sąskaitos ar skolos (pateikiamas tariamas įsiskolinimo pranešimas su prašymu apmokėti (el. paštu ar SMS))*[150]*;*
- *Pretekstu investuoti į kriptovaliutas ar kitas „pelningas“ schemas (žadamas didelis pelnas, bet tai – investicinis sukčiavimas ar finansinė piramidė)*[151]*;*
- *Pretekstu gauti ar atsiimti siuntinį (siunčiamos fiktyvios žinutės apie tariamą siuntą, prašant paspausti nuorodą, pateikti duomenis ar susimokėti siuntos mokestį)*[152]*;*

Kaip matyti, dažniausiai pasitaikantys sukčiavimo pretekstai grindžiami emociškai veikiančiomis situacijomis, nuo tariamų sandorių ar laimėjimų iki emocinio ryšio imitavimo ar skubios pagalbos prašymų. Šių pretekstų įgyvendinimas elektroninėje erdvėje dažniausiai susijęs su specifinių techninių metodų taikymų, leidžiančiu operatyviai perduoti apgaulingą informaciją bei išvilioti duomenis ir/ar turtą.

Remiantis 2024 m. Lietuvos policijos statistiniais duomenimis[153], net 53% visų

---

[146] Revolut. „Apie sukčiavimą ir apgavystes.“ *Revolut*, žiūrėta 2025 m. gruodžio 17 d., https://www.revolut.com/lt-LT/about-fraud-and-scam/

[147] Lrytas.lt. „Prisidengdami loterija, sukčiai bando išvilioti duomenis – paviešino, kokius laiškus siunčia.“ *Lrytas.lt*, žiūrėta 2025 m. gruodžio 17 d. https://www.lrytas.lt/lietuvosdiena/kriminalai/2022/04/12/news/prisidengdami-loterija-sukciai-bando-isvilioti-duomenis-paviesino-kokius-laiskus-siuncia-23041008

[148] Lietuvos policija. „Policija pataria.“ *Policija.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d., https://policija.lrv.lt/lt/policija-pataria/

[149] „Atvira Klaipėda. „Google“ vardą naudojantiems sukčiams atiteko dar 9200 eurų.“ *AtviraKlaipeda.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.atviraklaipeda.lt/2024/09/21/google-varda-naudojantiems-sukciams-atiteko-dar-9200-euru/

[150] Valstybinė mokesčių inspekcija. „Gavau įtartiną pranešimą iš VMI.“ *VMI.lt,* žiūrėta 2025 m. gruodžio 17 d. https://www.vmi.lt/evmi/gavau-itartina-pranesima-is-vmi

[151] LRT. „Sukčiai tyko visur: FNTT paaiškina, kaip atpažinti galimą investicinį sukčiavimą.“ *LRT.lt,* žiūrėta 2025 m. gruodžio 17 d. https://www.lrt.lt/naujienos/verslas/4/2047671/sukciai-tyko-visur-fntt-paaiskina-kaip-atpazinti-galima-investicini-sukciavima?srsltid=AfmBOoqsK9dStrhQkG1cAYK-qGlsbjTV4WbohfHj77iA2RLJYAYDC9Z3

[152] Lietuvos paštas. „Lietuvos paštas perspėja apie sukčių pinkles – jauku tampa bendrovės vardas.“ *Post.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.post.lt/lt/apie-mus/naujienos/lietuvos-pastas-perspeja-apie-sukciu-pinkles-jauku-tampa-bendroves-vardas

[153] Nacionalinis kibernetinio saugumo centras. „Nacionalinė kibernetinio saugumo būklės ataskaita 2024.“ *VDAI.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d., 12 p. https://vdai.lrv.lt/public/canonical/1748429329/942/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf

elektroninėje erdvėje padarytų nusikalstamų veikų sudarė įvairūs sukčiavimo modeliai, susiję su **apgaulingais el. laiškais, žinutėmis, telefoniniais skambučiais**, taip pat **investiciniai** bei **avansiniai sukčiavimai**. Vienas dažniausių tokių sukčiavimų yra vadinamasis fišingas (angl. phishing), kuris apima įvairias socialinės inžinerijos formas, t. y. nuo apgaulingų elektroninių laiškų ir SMS žinučių iki telefoninių skambučių ar net QR kodų. Šių atakų metų yra imituojama patikimų institucijų ar paslaugų teikėjų komunikacija, siekiant išvilioti asmeninius duomenis ar paskatinti vartotoją atlikti nepageidaujamus veiksmus. Terminas fišingas yra kilęs nuo žodžių angl. „password fishing“, reiškiančių „slaptažodžių žvejyba“. Minėtas terminas pirmą kartą viešai paminėtas dar 1996 metais interneto diskusijų grupėje, kur buvo aprašyti automatizuoti būdai išgauti vartotojų prisijungimo duomenis, pasitelkiant programinę įrangą AOHell[154]. Nors fišingas viešojoje erdvėje yra žinomas palyginti neseniai, tačiau vertinant informacinių technologijų raidos tempus, pagrįstai galima laikyti jau pakankamai senu ir istoriškai susiformavusiu reiškiniu. Pabrėžtina, jog fišingo atakos dažniausiai vykdomos masiškai ir nukreipiamos į įvairias vartotojų grupes, pavyzdžiui bankų klientus, siekiant išgauti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Tačiau vis dažniau taikomasi į populiarių elektroninių paslaugų, socialinių tinklų bei apsipirkimo platformų naudotojus. Tokiais atvejais sukuriamos netikros el. parduotuvės, suklastotos institucijų svetainės arba tiesiogiai siunčiami laiškai bei žinutės, imituojančios patikimų/tikrų paslaugų teikėjų komunikaciją. Pažymėtina, kad tokio pobūdžio atakos gali būti tiek plataus masto (masinio platinimo), tiek orientuotos į konkretų asmenį, įmonę ar instituciją, kas yra – angl. „spearphishnig“.

Atkreiptinas dėmesys, kad fišingas yra bendrinis terminas, kuris apima įvairias technikas ir veikimo būdus, kurių tikslas yra vienas – išgauti konfidencialius duomenis. Šis tikslas gali būti pasiektas naudojant skirtingus metodus ir informacijos perdavimo kanalus, kurie pateikiami žemiau esančioje lentelėje[155]:

KANALAI	**FIŠINGO ATMAINOS**	**„APGAULĖS“ FORMOS**	**TIKSLINĖS AUKOS**
Elektroniniai laiškai	Klasikinis fišingas	El. laiškai su nuorodomis/priedais	Bankų klientai, el. paslaugų naudotojai
SMS žinutės	Smišingas (smishing)	Apgaulingos SMS su nuorodomis, nukreipiantys į	Mobiliojo ryšio naudotojai

[154] Phishing.org. „History of Phishing.“ *Phishing.org,* žiūrėta 2025 m. gruodžio 17 d., https://www.phishing.org/history-of-phishing

[155] Fortinet. „Types of Phishing Attacks.“ *Fortinet CyberGlossary*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

		suklastotas svetaines	
Telefoniniai skambučiai	Višingas (vishing)	Apgaulingi skambučiai, apsimetant institucijomis	Vyresnio amžiaus asmenys, mažiau IT raštingi
QR kodai	Kvišingas (quishing)	Apgaulingi QR kodai, nukreipiantys į suklastotas svetaines	Viešų erdvių lankytojai, el. paslaugų vartotojai
Socialiniai tinklai	Socialinių tinklų fišingas (Angler phishing)	Netikrų paskyrų komentarai, su kenksmingomis nuorodomis ar failais	Socialinių tinklų naudotojai
Internetinės reklamos	Malvertising arba Clickbait	Apgaulingos internetinės reklamos	Vyresnio amžiaus asmenys, mažiau IT raštingi

Lentelė Nr. 2, Fišingo atmainos, autorius V. Golovko.

Lentelėje matyti, jog konfidencialių duomenų išgavimas elektroninėje erdvėje gali būti vykdomas įvairiais būdais ir atitinkamai, nukreipiamas į skirtingus visuomenės sluoksnius. Šių atakų įvairovė bei pasirenkami kanalai tiesiogiai atspindi technologijų pažangos poveikį įsilaužimo ir sukčiavimo metodams – nuo, jau galima tarti „tradicinių“ elektroninių laiškų iki šiuolaikiškų QR kodų. Kiekvienas iš išvardytų modelių pasižymi specifiniais veikimo požymiais ir kelia skirtingus probleminius aspektus kriminalistinei analizei bei prevencijai. Pažymėtina, kad išvardyti fišingo tipai nėra baigtiniai[156], kadangi egzistuoja ir kiti modeliai, orientuoti ne vien į tiesioginę turtinę naudą, bet ir į neteisėtą prieigą prie internetinių paskyrų ar duomenų, kuri gali tapti tolesnių turtinių nusikalstamų veikų pagrindu (pvz. išpirkos reikalavimai). Todėl, šiame darbe pagrindinis dėmesys skiriamas būtent toms atmainoms, kurios tiesiogiai arba numatytų veiksmų grandinės etapu orientuotos į turtinės naudos gavimą apgaule.

Fišingas

Viena labiausiai paplitusių ir istorinių požiūriu ankstyviausių **fišingo** formų yra elektroniniais laiškais vykdomos atakos (angl. email phishing). Tokios atakos prasideda nuo elektroninio laiško, kuris iš pirmo žvilgsnio atrodo gautas iš tikros institucijos ar asmens, tačiau siuntėjo el. pašto adresas yra suklastotas. Laiško turinyje pateikiama tariama priežastis (pretekstas), dėl kurios gavėjas turėtų skubiai atlikti veiksmus, susijusius su savo prisijungimo duomenų pateikimu. Priežastys gali būti įvairios, pavyzdžiui, teigiama, kad paskyros galiojimas laikinai sustabdytas, kol nebus pateikti papildomi duomenys, ar kad yra keičiama aptarnavimo

[156] Fortinet. „Types of Phishing Attacks.“ *Fortinet CyberGlossary*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

sistema ir reikia atnaujinti prisijungimo informaciją[157]. Tokiuose laiškuose gali būti pateikiamos aktyvios nuorodos, kurios nukreipia į klastotą internetinį puslapį (kloną), vizualiai beveik nesiskiriantį nuo tikros svetainės, o domenas (unikalus interneto adresas) gali skirtis vos vienu simboliu ar raide nuo tikrojo adreso. Įvedus konfidencialią informaciją suklastotoje svetainėje, ši automatiškai perduodama atakos vykdytojui. Verta pabrėžti, jog pasekmės nebūtinai apsiriboja duomenų nutekėjimu. Pavyzdžiui, suklastotoje svetainėje, kurioje natūralu atlikti finansines operacijas, auka, manydama, kad tai tikra ir teisėta svetainė, gali pati inicijuoti ir patvirtinti mokėjimą per „Smart-ID“ tapatybės patvirtinimo priemone, tokiu būdu pervesdama lėšas sukčiams. Be to, kai kuriais fišingo atvejais el. laiškuose, vietoje internetinių nuorodų gali būti prisegti priedai (failai) su kenkėjiška programa, kurią atidarius el. laiško gavėjo kompiuteryje, telefone ar kitame išmaniajame įrenginyje aktyvuojamas kenksmingas kodas. Tokiu būdu įsilaužėliai įgyja nuotolinę prieigą prie naudotojo sistemos bei joje esančių duomenų[158], kurie vėliau gali būti panaudojami prisijungiant prie aukų paskyrų ir apgaule įgyjant pinigines lėšas.

Šiuolaikinėje pinigų plovimo ir teroristų finansavimo prevencijos praktikoje fiksuojami atvejai, kai nusikalstamos grupės kuria oficialias valstybines e. paslaugas imituojančias svetaines. 2024 metų Finansinių nusikaltimų tyrimo tarnybos (FNTT) veiklos ataskaitoje pažymėta, kad vienu ryškiausių pavyzdžiu tapo svetainė, vizualiai atkurianti „e.sveikata.lt“ tikrąjį elektroninį puslapį. Ataskaitoje nurodoma, kad: „per internetinę paieškos sistemą ieškantys šios svetainės asmenys greičiausiai pasirenka ne oficialią, o fiktyvią svetainę. Asmenys, besijungiantys prie sistemos su asmeniniais banko duomenimis, turėjo „Smart ID“ programėlėje suvesti PIN1 ir PIN2 kodus – po šių veiksmų nukentėję asmenys pastebėjo, kad nuo jų banko sąskaitų buvo nuskaitytos lėšos ir pervestos į skirtingų asmenų banko sąskaitas tiek Lietuvoje, tiek užsienyje“. FNTT vertinimu, ateityje tokių sukčiavimo atvejų, susijusių su administracinių ir viešųjų elektroninių paslaugų portalų klastojimu, skaičius didės[159].

Atsižvelgiant į tai, matyti, jog fišingo veikimo mechanizmai neapsiriboja el. laiškais, o aukos pasiekiamos ir per interneto paieškos sistemų rezultatus. Toks apgaulės modelis laikytinas „**paieškos sistemų fišingu“** (angl. Search engine phishing[160]). Praktinis pavyzdys – 2025-11-30 d. paieškos sistemoje „Microsoft Edge“, suvedus užklausą „Infolex bk“, tarp paieškos rezultatų pateikiama suklastota „Infolex.lt“ svetainė, kurios domenas yra „prokurorai.lt“. Nepastebėjus šio

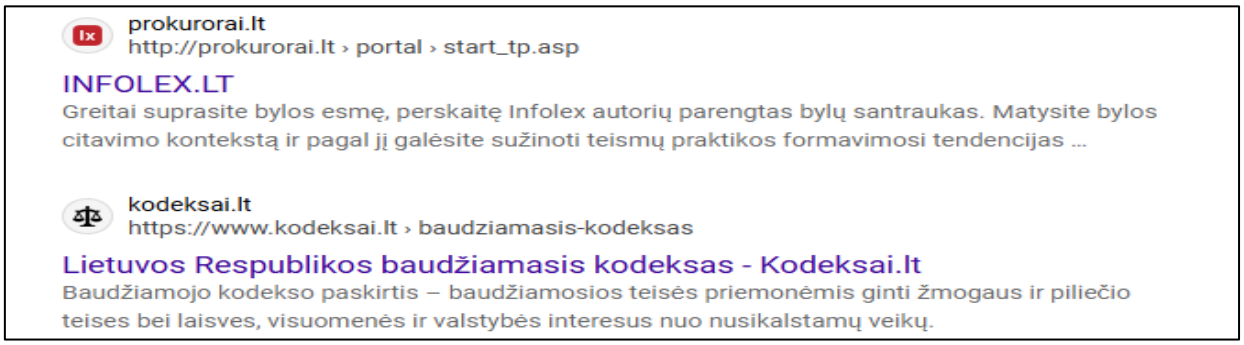
[157] Esaugumas. „Phishing laiškų pavyzdžiai.“ *Esaugumas.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.esaugumas.lt/phishing-laisku-pavyzdziai

[158] Esaugumas. „Kaip vyksta duomenų viliojimas (angl. phishing).“ *Esaugumas.lt,* žiūrėta 2025 m. gruodžio 17 d., https://esaugumas.lt/articles/kaip-vyksta-duomenu-viliojimas-angl-phishing

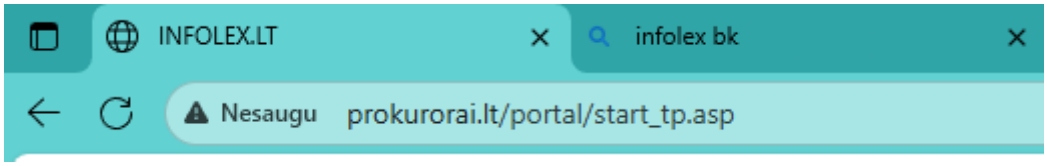
[159] Finansinių nusikaltimų tyrimo tarnyba. „Ataskaita 2024.“ *FNTT.lrv.lt,* žiūrėta 2025 m. gruodžio 17 d. 17 p., https://fntt.lrv.lt/public/canonical/1749447681/1063/Ataskaita_2024%20(1).pdf

[160] Fortinet. „Types of Phishing Attacks.“ *Fortinet CyberGlossary*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

domeno pavadinimo ir patekus į šią suklastotą svetainę (kloną), ją klaidingai laikant tikrąja „Infolex“ sistema, bei joje suvedus savo prisijungimo duomenis, tikėtina, jog jie bus nutekėti ir panaudoti. Tačiau nagrinėjamu atveju, vertinant tikrosios svetainės auditoriją, bei joje suvedamų duomenų kontekstą – mažai tikėtina, jog tokio pobūdžio klastotė skirta pasipelnymo tikslams, todėl tokį atvejį traktuoti kaip pasikėsinimą sukčiauti nėra pagrindo. (Žr. paveikslus Nr. 1, 2):



Paveikslas Nr. 1, (paieškos sistemoje „Microsoft Edge“, suvedus užklausą „Infolex bk“), autorius – V. Golovko.



Paveikslas Nr. 2, (paieškos sistemoje „Microsoft Edge“, suvedus užklausą „Infolex bk“ ir paspaudus ant rezultato „prokurorai.lt“), autorius – V. Golovko.

Šiais atvejais sukčiai ne tik kuria fiktyvias svetaines, bet ir taiko „paieškos sistemų nuodijimo“ priemones (angl. Search engine optimization (SEO) poisoning[161]) arba įsigyja mokamas „Google Ads“ paieškos reklamas, kurios panaudojamos apgaulingiems nukreipimams (angl. malvertising[162]). Reklamos perkamos pagal populiarius raktinius žodžius ir jų rašybos atmainas pavyzdžiui – „esveikata“, „e-sveikata“, ar klaidingos raidžių kombinacijos. Tokiu būdu suklastoti elektroniniai puslapiai iškeliami į aukštas pozicijas ar net rezultatų viršų (tinklapių pirmos pozicijos), todėl vartotojai, remdamiesi įpročiu spausti pirmąsias nuorodas, klaidingai jas vertina kaip teisėtas.

Elektroninėje erdvėje taip pat pasitaiko atvejų, kai vartotojas nukreipiamas į suklastotą svetainę net ir tuomet, kai naršyklėje suveda oficialų interneto adresą. Toks modelis priskirtinas ne fišingui, o farmingui (angl. pharming[163]). Vaidas Kalpokas ir Renata Marcinauskaitė savo moksliniame straipsnyje detaliai nagrinėja farmingo veikimo ypatumus, šią atakos rūšį įvardija

[161] Canadian Centre for Cyber Security. „Search Engine Optimization (SEO) Poisoning (ITSAP.00.013).“ *Cyber.gc.ca,* žiūrėta 2025 m. gruodžio 17 d., https://www.cyber.gc.ca/en/guidance/search-engine-optimization-poisoning-itsap00013

[162] Malwarebytes. „Что такое malvertising?“ *Malwarebytes*, žiūrėta 2025 m. gruodžio 17 d., https://www.malwarebytes.com/ru/malvertising

[163] Proofpoint. „Pharming.“ *Proofpoint,* žiūrėta 2025 m. gruodžio 17 d. https://www.proofpoint.com/us/threat-reference/pharming

kaip vieną iš galimų konfidencialios informacijos rinkimo būdų ir laiko modifikuotu fišingo variantu[164]. Farmingo atveju nukreipimą atlieka techninės priemonės (pvz. 1 - aukos įrenginyje veikiantis kenkėjiškas kodas, 2 - pakeisti DNS nustatymai), todėl užpuolikui nereikia, kad vartotojas pats spustelėtų nuorodą ar paieškos rezultatą. Farmingas – tai kibernetinės atakos rūšis, kai žiniatinklio srautas iš teisėtos svetainės nukreipiamas į suklastotą, siekiant pagrobti naudotojo vardą, slaptažodį, finansinius duomenis ar kitą asmeninę informaciją[165]. Nors farmingo tikslas artimas fišingui, jis laikytinas atskira kibernetinės apgaulės forma dėl techninio srauto peradresavimo pobūdžio.

Iš pirmo žvilgsnio gali atrodyti, jog fišingas yra paprasta apgaulės forma, tačiau jo techninis įgyvendinimas yra pakankamai sudėtingas procesas, reikalaujantis specifinių IT žinių, technologinių priemonių bei kruopštaus pasirengimo. Siekiant aiškumo, toliau pateikiami pagrindiniai techniniai terminai, apibūdinantys pagalbines priemones, naudojamas el. laiškais fišingo atakoms vykdyti:

TERMINAS	**TRUMPAS PAAIŠKINIMAS**	**PAVYZDYS**
Email spoofing	El. pašto siuntėjo adreso klastojimas, kad laiškas atrodytų siųstas iš patikimo šaltinio	El. laiškas iš support@swedbank.lt faktiškai siųstas iš kito serverio
Domain spoofing	Domeno vardo klastojimas (el. pašte ar svetainės adrese), vizualiai panašūs į tikrąjį	www.swedbank1.lt vietoje www.swedbank.lt
Website spoofing	Fiktyvios svetainės sukūrimas, imituojant tikros svetainės dizainą ir turinį	Svetainė www.swedbank1.lt su identišku dizainu, struktūra
Thread hijacking	Tikro el. pašto susirašinėjimo perėmimas ir kenkėjiško (fišingo) turinio įterpimas	Atsakymas į tikrą pokalbį su nuoroda į fiktyvų puslapį

Lentelė Nr. 3, Fišingo terminai, autorius V. Golovko.

Viena iš pagrindinių elektroninių laiškų fišingo atakose taikomų technikų yra vadinamasis „Email spoofing“[166]. Šios technikos esmė – suklastoti el. pašto adreso informaciją, dažniausiai „Nuo“ (angl. From) siuntėjo laukelio duomenis, taip, kad gavėjui susidarytų įspūdis, jog laiškas gautas iš tikros institucijos, įmonės, ar net artimo asmens, nors kaip jau buvo minėta, jo kilmė yra visiškai kita. (Žr. paveikslą Nr. 3):

[164] Kalpokas, Vaidas, ir Renata Marcinauskaitė. 2012. „Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas.“ *Teisės problemos* 3 (77), 35 p., https://www.lituanistika.lt/content/42148

[165] Malwarebytes. „Что такое фарминг (pharming)?“ *Malwarebytes,* žiūrėta 2025 m. gruodžio 17 d., https://www.malwarebytes.com/ru/pharming

[166] Proofpoint. „Email Spoofing.“ *Proofpoint,* žiūrėta 2025 m. gruodžio 17 d. https://www.proofpoint.com/us/threat-reference/email-spoofing

Paveikslas Nr. 3, Phishing laiško pavyzdys,
autorius – Lietuvos Respublikos ryšių reguliavimo tarnyba.

Ši klastojimo galimybė atsiranda dėl vadinamojo paprastojo pašto perdavimo protokolo (angl. Simple Mail Transfer Protocol)[167] trūkumų, kadangi šis protokolas netikrina, ar siuntėjo adresas yra tikras. Kitaip tariant, atakos vykdytojas, naudodamas specialius skriptus[168] ar programines užklausas, gali nurodyti bet kokį siuntėjo adresą, nepriklausomai nuo to, ar toks adresas apskritai egzistuoja. Toks išsiųstas el. laiškas keliauja per kelis tarpinius serverius, kurių IP adresai įrašomi į el. laiško antraštes. Ir nors antraštės leidžia nustatyti tikrąjį siuntėją, dauguma vartotojų jų netikrina. Kita pažangesnė fišingo technika yra „thread hijacking“[169], kai nusikaltėliai, neteisėtai įgiję prieigą prie vienos iš susirašinėjimo šalių elektroninio pašto paskyros (dažniausiai per fišingą, kenkėjišką programinę įrangą ar išnaudojant silpnus slaptažodžius) įsilaužia į tikrąjį susirašinėjimą ir perima pokalbį. Tokiuose, jau esančiuose pokalbiuose, gali būti įterpiamas fišingo turinys (nuorodos), o nukentėjusysis, matydamas žinomą siuntėją ir natūraliai tęsdamas pokalbį gali neįtarti jokios apgaulės ar klastotės[170].

Kitas esminis fišingo atakų elementas yra fiktyvių svetainių kūrimas – „website spoofing“[171]. Ši technika apima apgaulingos svetainės sukūrimą, vizualiai atkartojant tikros institucijos ar internetinės platformos dizainą, logotipus ir struktūrą, siekiant apgauti vartotoją. Sukūrus tokią svetainę, pastarajai reikalingas unikalus interneto adresas – domenas. Kai vartotojas paieškos naršyklėje įveda domeno vardą, pvz. „swedbank.lt“ (tikrasis), DNS konvertuoja domeno vardą į atitinkamą IP adresą ir nukreipia vartotoją į norimą svetainę.

[167] Proofpoint. „SMTP Relay.“ *Proofpoint,* žiūrėta 2025 m. gruodžio 17 d., https://www.proofpoint.com/us/threat-reference/smtp-relay

[168] Get Cyber Safe. „Script Spoofing: Protect Yourself.“ *GetCyberSafe.gc.ca*, žiūrėta 2025 m. gruodžio 17 d., https://www.getcybersafe.gc.ca/en/blogs/script-spoofing-protect-yourself

[169] Darktrace. „Thread Hijacking: How Attackers Exploit Trusted Conversations to Infiltrate Networks.“ *Darktrace,* žiūrėta 2025 m. gruodžio 17 d., https://www.darktrace.com/blog/thread-hijacking-how-attackers-exploit-trusted-conversations-to-infiltrate-networks

[170] MITRE ATT&CK. „T1566: Phishing.“ *MITRE ATT&CK*, žiūrėta 2025 m. gruodžio 17 d., https://attack.mitre.org/techniques/T1566/

[171] Mimecast. „Website Spoofing.“ *Mimecast*, žiūrėta 2025 m. gruodžio 17 d., https://www.mimecast.com/content/website-spoofing/

Paprastai apgaulingai svetainei sukuriamas panašus domeno vardas „domain spoofing“[172], kuris vizualiai beveik nesiskiria nuo tikrojo. Kaip minėta ankščiau, domeno pavadinimas gali skirtis vos vienu simboliu ar raide, arba naudojamas netinkamas prefiksas prieš bendrovės pavadinimą (pvz. **info-**swedbank.lt (klastotė), vietoje tikrojo – swedbank.lt). Tokios apgaulės gali likti nepastebėtos net naršyklės saugumo indikatoriuose, jei piktybinė svetainė pasirūpina galiojančiu „https“ sertifikatu (pavyzdžiui - **https**://www.info-swedbank.lt/private). Https (raidė „s“ – angl. secure, liet. saugus) – reiškia, jog ryšys tarp naršyklės ir serverio šifruojamas, užtikrinamas duomenų vientisumas naršyklė patvirtina domeno serverį[173], kitaip tariant, kartais tai yra papildomas indikatorius, jog svetainė yra saugi. Galiausiai, kad apgaulinga svetainė būtų pasiekiama, reikalingas turinio talpinimas „hostingas“ (angl. hosting). Tai yra paslauga, kai teikėjas savo serveriuose saugos su domeno vardu „svetainės“ susijusius failus ir užtikrina jų prieigą internete[174]. Pažymėtina, kad „domeno zonos“ arba kitaip tariant aukščiausio lygio domenai (angl. Top-Level domain – TLD), tokie kaip .lt[175] (nacionalinė LT zona, registruojama internetu per akreditoriaus registratorius[176]) ar .com (bendrinė gTLD, registruojama per tarptautinių registratorių tinklą[177]), yra nuomojami ir registruojami nustatytam terminui ir periodiškai pratęsiami, tuo tarpu „hostingas“ yra atskira nuomos paslauga. Elektroninėje erdvėje egzistuoja kompanijos, suteikiančios registruotojo privatumo paslaugą. Tai reiškia, kad tikrasis domeno savininkas lieka anonimas.

Taigi, iš aptarto matyti, jog šiuolaikinėse fišingo atakose nusikalstamos veikos padarymo būdas įgyvendinamas pasitelkiant, be kita ko, tokias kruopščias technikas, arba kalbant iš kriminalistinės charakteristikos perspektyvos – įrankius ir priemones, kaip „email spoofing“, „domain spoofing“, „website spoofing“, „thread hijacking“. Akcentuotina, kad tai tik dalis galimų technologinių priemonių, tačiau jos yra esminės formuojant atakos vykdymo modelį, didinant jo „realumą“ ir tikimybę, kad auka savarankiškai atliks nusikaltėliui naudinga veiksmą, t. y. paspaudus nuorodą, pateks į suklastotą svetainę ir joje suves konfidencialius duomenis, kurie bus neteisėtai perimti ir panaudoti fišingo atakos vykdytojo.

Pabrėžtina, kad fišingas tampa ypač pavojingas, kai derinamas su kitomis socialinės

---

[172] Proofpoint. „Domain Spoofing.“ *Proofpoint*, žiūrėta 2025 m. gruodžio 17 d., https://www.proofpoint.com/us/threat-reference/domain-spoofing

[173] Amazon Web Services. „В чём разница между HTTPS и HTTP?“ *AWS*, žiūrėta 2025 m. gruodžio 17 d., https://aws.amazon.com/ru/compare/the-difference-between-https-and-http/

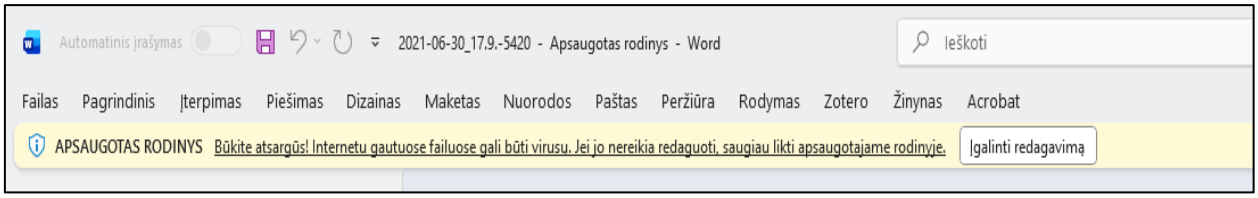
[174] IBM. „Web Hosting.“ *IBM*, žiūrėta 2025 m. gruodžio 17 d., https://www.ibm.com/think/topics/web-hosting

[175] Interneto vizija. „Domeno registracijos gidas.“ *Domreg.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.domreg.lt/duk/domain_registration_guide.pdf

[176] Interneto vizija. „Procedūrinis reglamentas.“ *Domreg.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.domreg.lt/informacija/dokumentai/procedurinis-reglamentas.pdf

[177] ICANN. „.com Registry Agreement.“ *ICANN.org*, žiūrėta 2025 m. gruodžio 17 d., https://itp.cdn.icann.org/en/files/registry-agreements/com/com-agreement-pdf-01-12-2024-en.pdf

inžinerijos priemonėmis. Pavyzdžiui, atakos metu gali būti siunčiami laiškai, su prisegtais priedais (failais) – „Microsoft Word“ (dokumentas) ar „Excel“ (skaičiuoklė), turintys įgalintas makrokomandas. Tokie priedai pasižymi formatais „.docm“ arba „.xlsm“, kuriuos atidarius vartotojas skatinamas „aktyvuoti“ ar „įgalinti“ turinį. (Žr. paveikslą Nr. 4):



Paveikslas Nr. 4, siūlymas „įgalinti redagavimą“ „Microsoft Word“ dokumente, autorius – V. Golovko.

Jei el. laiško gavėjas tai padaro, aktyvuojamas „VBA macro“ kodas, kuris paleidžia „PowerShell“ komandas. Šios komandos naudojamos kenksmingai programai parsiųsti bei įdiegti[178]. Po sėkmingo fišingo įvyksta antrasis etapas – sistemos pažeidimas, kuriuo metu į aukos įrenginį patenka kenkėjiška programa. Dažniausiai pasitelkiama programinė įranga vadinama „Remote Acces Trojans“ (RAT), pavyzdžiui „Remcos“ ar „AsyncRAT“. Šie įrankiai leidžia nusikaltėliui nuotoliniu būdu visiškai kontroliuoti vartotojo įrenginį, t. y. stebėti ekraną, įrašinėti klavišų paspaudimus (angl. key logging[179]), peržiūrėti ar kopijuoti failus, įjungti kamerą ar mikrofoną ir panašiai[180]. Šios įdiegtos programos veikia fone, neretai naudodamos „process hollwoing“ ar „thread hijacking“ metodus, būtent tai leidžia kenksmingam kodui „pasislėpti“ sistemos procesuose, kad antivirusinės programos jų neaptiktų[181]. Po sėkmingos „infekcijos“ „RAT“ susisiekia su vadinamuoju C2 (command and control) serveriu, per kurį vykdomas tolesnis valdymas. Ryšys būna šifruotas TLS protokolu, o pats duomenų turinys papildomai apsaugotas AES algoritmu, kas leidžia atakos vykdytojui išvengti aptikimo[182]. Tokiu būdu surinkti prisijungimo duomenys ar kiti jautrūs failai gali būti naudojami tiek tiesiogiai, pavyzdžiui prisijungiant prie el. bankininkystės ir atliekant neteisėtus pinigų pervedimus, tiek netiesiogiai, t. y. perparduodant gautą informaciją juodojoje rinkoje ar pasinaudojant ją kitose nusikalstamose schemose.

Atkreiptinas dėmesys, kad fišingas šiuo atveju apima tik pirmąją nusikalstamos grandinės dalį (socialinės inžinerijos veiksmus), kurios metu siekiama suklaidinti auką ir

[178] SentinelOne. „Deconstructing PowerShell Obfuscation in Malspam Campaigns.“ *SentinelOne*, žiūrėta 2025 m. gruodžio 17 d., https://www.sentinelone.com/blog/deconstructing-powershell-obfuscation-in-malspam-campaigns/

[179] Radware. „Keylogging.“ *Radware DDoSpedia*, žiūrėta 2025 m. gruodžio 17 d., https://www.radware.com/security/ddos-knowledge-center/ddospedia/keylogging/

[180] Fortinet. „Latest Remcos RAT Phishing Campaign Uses XWorm to Deliver Malware.“ *Fortinet Blog*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing

[181] The Hacker News. „Fileless Remcos RAT Delivered via Weaponized Windows LNK Files.“ *The Hacker News*, žiūrėta 2025 m. gruodžio 17 d., https://thehackernews.com/2025/05/fileless-remcos-rat-delivered-via-lnk.html

[182] Fortinet. „Latest Remcos RAT Phishing Campaign Uses XWorm to Deliver Malware.“ *Fortinet Blog*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing

paskatinti ją atidaryti kenkėjišką failą. Tolesni veiksmai, susiję su kenkėjiškos programos įdiegimu ir jos vykdymo procesais – nelaikytini fišingu. Tai yra atskira techninės atakos priemonė (angl. malware[183]) ir priskirtina kitoms kibernetinių nusikaltimų rūšims. V. Kalpokas ir R. Marcinauskaitė 2012 m. moksliniame straipsnyje nagrinėdami kenkimo programų veikimo principus, pažymi, jog įdiegus vartotojo kompiuteryje kenkimo programas, pastarosios pačios surenka ir persiunčia reikalingus duomenis[184]. Praktikoje šie etapai dažnai yra neatsiejamai susiję su sėkminga fišingo ataka ir išplečia galutinį nusikalstamos veikos poveikį. Todėl, atsižvelgiant į šiuolaikinių technologijų galimybes bei fišingo atakų mąstą, tokios atakos gali būti vykdomos ne vien siekiant tiesioginės turtinės naudos. Gauti duomenys gali būti panaudojami kibernetiniam šnipinėjimui, žvalgybai ar pasirengimui kitoms nusikalstamoms veikoms. Ši technologinė grandinė, pradedant nuo suklastoto el. laiško ir baigiant nuotoline prieiga prie aukos įrenginio, leidžia ne tik išgauti duomenis, bet ir juos tikslingai panaudoti. Būtent įsilaužėlio galutinis tikslas yra esminis kriterijus, leidžiantis kvalifikuoti tokio pobūdžio veiką kaip sukčiavimą, o ne tik kaip neteisėtą duomenų gavimą ar įsilaužimą į informacinę sistemą.

Smišingas

Kita fišingo atmaina yra **smišingas**[185] (angl. smishing), kai atakos vektoriumi tampa ne elektroninis paštas, o trumposios SMS žinutės. Kaip ir tipinio fišingo atveju, pagrindinis tikslas yra apgaule išgauti asmens duomenis, siekiant vėliau juos panaudoti nusikalstamiems tikslams. Tačiau galimas ir tiesioginis sukčiavimas, kai auka fiktyvioje svetainėje pati inicijuoja ir patvirtina mokėjimą. Terminas „smishing“ yra sudurtinis žodis, kilęs iš „SMS“ ir „phishing“. Šiuo atveju apgaulingi veiksmai pasireiškia siunčiant tekstines žinutes į mobiliuosius įrenginius, kuriose pateikiama apgaulinga nuoroda su raginimu atlikti tam tikrą veiksmą. Dažniausiai pasirenkamos tokios temos kaip siuntų pristatymo pranešimai, banko duomenų atnaujinimo prašymai ar prisijungimo prie sistemų patvirtinimai, nes jos atrodo patikimos ir skatina adresatą reaguoti skubiai. Vėlgi, tokie pranešimai atrodo yra siunčiami iš patikimo šaltinio (banko, valstybės institucijos ir kt.), nes pasitelkiama siuntėjo identifikavimo klastojimo technologija „SMS spoofing“. Paspaudus tokią nuorodą, vartotojas, kaip ir tradicinio fišingo atveju nukreipiamas į fiktyvią svetainę, kurioje suvesti konfidencialūs duomenys tiesiogiai perduodami atakos vykdytojui arba, patvirtinus mokėjimą, lėšos pervedamos sukčiams[186].

---

[183] Microsoft. „What Is Malware?“ *Microsoft Security*, žiūrėta 2025 m. gruodžio 17 d., https://www.microsoft.com/en-us/security/business/security-101/what-is-malware

[184] Kalpokas, Vaidas, ir Renata Marcinauskaitė. 2012. „Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas.“ *Teisės problemos* 3 (77), 37 p., https://www.lituanistika.lt/content/42148

[185] Proofpoint. „Smishing.“ *Proofpoint*, žiūrėta 2025 m. gruodžio 17 d https://www.proofpoint.com/us/threat-reference/smishing

[186] Proofpoint. „Smishing.“ *Proofpoint*, žiūrėta 2025 m. gruodžio 17 d https://www.proofpoint.com/us/threat-reference/smishing

Skirtingai ne fišingo atveju, smišingo veiksmingumas slypi ne techniniuose aspektuose, o psichologinėje vartotojo reakcijoje į SMS žinučių formą ir kontekstą. Dėl mobiliojo telefono ekrano riboto informacijos atvaizdavimo vartotojui būna sunkiau aptikti įtartiną turinį, t. y. trumpesnę nuorodą, neaiškų domeno vardą ar neoficialią kalbą, kurie gali likti nepastebėti. Be to, žinutės turinys suformuluojamas taip, kad gavėjas jaustų spaudimą veikti skubiai, pavyzdžiui: „Jūsų paskyra bus užblokuota per 24 valandas“, „Siunta laukia patvirtinimo“ ar „Reikia patvirtinti mokėjimą“. Tokie SMS pranešimai siunčiami naudojantis automatizuotomis sistemomis, vadinamaisiais „SMS šliuzais“ (angl. SMS gateway[187]), kurie leidžia vienu metu perduoti tūkstančius identiškų pranešimų ir maskuoti siuntėjo tapatybę. Šios priemonės įprastai nesunkiai prieinamos tamsiojoje interneto rinkoje (angl. Dark web). Be to, nusikaltėliai gali naudotis paslaugomis, suteikiančiomis galimybę siųsti SMS iš virtualių numerių arba padirbti žinomą siuntėjo pavadinimą (angl. sender ID spoofing), pavyzdžiui „Swedbank“, „Lietuvos Paštas“ ar VMI, taip padidinant pranešimo tikrumą[188].

Višingas

Dar viena paplitusi fišingo atmaina yra **višingas** (angl. vishing). Tai yra sukčiavimo ataka, kuri vykdoma telefonu arba naudojantis balso perdavimo internetu technologijomis (angl. Voice over Internet Protocol – toliau ir VoIP[189]), pavyzdžiui „WhatsApp“, „Telegram“, „Viber“, „Messneger“ ir pan. programėlėmis. Pagrindinis tikslas, kaip ir kituose fišingo formose yra socialinės inžinerijos būdu išgauti konfidencialius asmens duomenis bei gauti prieigą prie finansinių sąskaitų, pinigų ar kitokios vertingos informacijos. Tokiais atvejais aukai skambinama sukuriant skubos ar grėsmės įspūdį. Pavyzdžiui teigiama, kad banko sąskaita užblokuota, joje aptikta įtartinų operacijų ar būtina nedelsiant patvirtinti tapatybę. Skambintojai gali prisistatyti finansų įtaigų, policijos, mokesčių ar kitų institucijų vardu.

Pastaruoju metu Lietuvoje yra paplitęs hibridinis sukčiavimo modelis, sudarytas iš smišingo (apgaulinga SMS žinutė), fišingo (apgaulinga nuoroda ir svetainė), višingo (apgaulingas skambutis telefonu ar VoIP). Šių veiksmų derinys suformuoja vientisą apgaulės grandinę ir lemia tiesioginę turtinę žalą.

Iš pradžių auka gauna SMS žinutę neva iš telekomunikacijų bendrovės dėl plano sustabdymo ar duomenų atnaujinimo, kurio esą reikia atlikti paspaudus nuorodą į tariamą telekomunikacijos bendrovės svetainę (fiktyvią). Aukai įvedus duomenis klastotėje, netrukus

---

[187] „SMS gateway.“ *Wikipedia*, žiūrėta 2025 m. gruodžio 17 d., https://en.wikipedia.org/wiki/SMS_gateway

[188] Proofpoint. „Smishing.“ *Proofpoint*, žiūrėta 2025 m. gruodžio 17 d https://www.proofpoint.com/us/threat-reference/smishing

[189] Carrillo-Mondéjar, Javier, José Luis Martínez, ir Guillermo Suarez-Tangil. 2022. „On how VoIP attacks foster the malicious call ecosystem.“ *Computers & Security*. https://www.sciencedirect.com/science/article/pii/S0167404822001535

skambina asmuo, pristatantis banko darbuotoju. Skambučio atlikimui gali būti naudojami laikini (vienkartiniai) telefono numeriai, kuriuos galima įsigyti per SMS aktyvinimo paslaugas už labai mažą kainą (paslaugos kaina priklauso nuo pasirinktos tel. numerio šalies), todėl telefono numeris pats savaime neužtikrina patikimo ryšio su realia asmens tapatybe[190]. Skambutis taip pat gali būti vykdomas per VoIP programas. Tokiu atveju ryšio atsekamumas siejamas ne vien su telekomunikacijų operatorių išklotinėmis, bet ir su IP adresu fiksuojama informacija, kuri taip pat ne visais atvejais tiesiogiai atspindi galutinio naudotojo tapatybę[191]. Siekiant paslėpti IP adresą gali būti naudojamas lengvai prieinamas įrankis VPN. VPN sukuria duomenims šifrą, taip paslėpdamas tiek asmens tapatybę, tiek IP adresą, tai reiškia, kad asmenį galintys padėti nustatyti duomenys šifruojami, o srautas nukreipiamas ne per tiesioginį, bet per VPN serverio IP adresą, taip paslepiant tikrąjį naudotojo IP adresą. Be to pažymėtina, jog IP adresai gali būti statiniai ir dinaminiai. Statinis IP adresas yra pastovus IP adresas, kuris priskiriamas kompiuteriui, serveriui ar kitam įrenginiui tinklo aplinkoje ir nesikeičia, priešingai jam, dinaminis IP adresas gali keistis kaskart, kai įrenginys prisijungia prie tinklo[192]. Taigi paskambinęs tariamas banko darbuotojas pokalbio metu nuosekliai taiko psichologinį spaudimą, neva matantis įtartiną veiklą aukos banko profilyje, klausia ar šiuo metu vykdė bankinius pervedimus, ar pastaroji nespaudė neaiškių nuorodų ir t.t. Pokalbio metu aukai siūlomi skubūs problemos sprendimai, pvz. patariama laikinai užblokuoti paskyrą ir/ar pervesti banko sąskaitoje esančias lėšas į vadinamąją saugią sąskaitą. Pokalbio pabaigoje aukai pranešama, jog netrukus susisieks policijos pareigūnas ir plačiau pateiks tolimesnius nurodymus. Po trumpos pauzės per tą pačią programėlę vaizdo skambučiu paskambina kitas asmuo, prisistatantys policijos pareigūnu. Vaizdo skambutis organizuojamas tuoj pat, išlaikant nuolatinį laiko spaudimą ir informacijos perkrovą, kad būtų nuslopintas aukos gebėjimas kritiškai vertinti situaciją ir neliktų laiko savarankiškai pasitikrinti informaciją. Vaizdo pokalbio metu siekiama padidinti patikimumo įspūdi, kadangi auka mato uniformuotą Lietuvos Respublikos pareigūną, norintį „padėti“ aukai. Šiuo atveju auka raginama neatidėlioti ir imtis veiksmų apsaugoti savo lėšas. Apsimetėlis nurodo pervesti lėšas į tam tikrą sąskaitą arba perduoti banko kortelę su PIN kodu voke kitam atvyksiančiam policijos pareigūnui ar tariamam banko darbuotojui (bendrininkui). Tačiau gali būti ir taip, jog „kurjeriais“ tampantys asmenys iš esmės nebūna susiję su sukčiais, kadangi pastarieji surandami internetu, pvz. „Telegram“ grupėse, kur skelbiami tariami vienkartiniai darbo pasiūlymai dėl dokumentų

[190] Reuters. „Key barrier to online fraud can be bypassed for pennies, say researchers.“ *Reuters,* žiūrėta 2025 m. gruodžio 17 d., https://www.reuters.com/business/media-telecom/key-barrier-online-fraud-can-be-bypassed-pennies-say-researchers-2025-12-11/

[191] Twingate. „VoIP Spoofing.“ *Twingate Blog*, žiūrėta 2025 m. gruodžio 17 d., https://www.twingate.com/blog/glossary/voip%20spoofing?

[192] „IP adresas.“ *Vikipedija,* žiūrėta 2025 m. gruodžio 17 d. https://lt.wikipedia.org/wiki/IP_adresas ., https://lt.wikipedia.org/wiki/IP_adresas

pervežimo iš vieno taško į kitą už atlygį. Kurjeriui palikus voką nurodytoje vietoje (koordinatės), šį voką pasiima sukčių bendrininkai ar kiti vadinamieji „pinigų mulai“ ir lėšos išgryninamos bankomatuose. Išgryninimai gali vykti kitame šalies mieste ar net užsienyje.

Žvelgiant į LAT praktikos pavyzdžius, buvo tirtas atvejis, kai asmuo paskambino nukentėjusiajai telefonu ir apgaulingai prisistatęs gydytoju, pranešė, kad jos dukra nelaimingo atsitikimo metu, krisdama nuo laiptų, sužalojo mergaitę, kuriai esą reikalinga operacija, kainuojanti 7 000 Eur. Patikėjusi pateikta informacija, nukentėjusioji atvykusiam asmeniui prie savo namų perdavė grynuosius pinigus. Tokiu būdu kaltininkas apgaule įgijo svetimą turtą. (Lietuvos Aukščiausiojo Teismo 2023 m. birželio 22 d. nutartis baudžiamojoje byloje 2K-170-495/2023)[193].

Neatmetami atvejai, kai nepavyksta įtikinti aukos suvesti el. bankininkystės duomenų (pvz. dėl senyvo amžiaus, skaitmeninio raštingumo stokos ar nemokumo). Prisitaikydami prie aukos, sukčiai gali paskatinti įsidiegti viešai prieinamas nuotolinės prieigos programas, tokiais kaip „AnyDesk“, „Teamviewer“ ir suteikti jiems kompiuterio ar net išmaniojo telefono[194] valdymą, esą „padedant“ atlikti nuotolinius mokėjimus ar tvarkyti el. bankininkystę. Aukai sutikus, pervedimai gali būti vykdomi net nepasitelkiant suklastotų svetainių, o per oficialius bankų puslapius, kadangi veiksmai registruojami kaip atlikti iš aukos priskirto IP adreso. Pasikėsinimo suma paprastai priklauso nuo aukos sąskaitos likučio. Sukčiavimo subjektai taip pat gali paskatinti auką pasididinti pervedimo ar išgryninimo limitus. Įkyrūs sukčiai papildomai gali domėtis terminuotaisiais indėliais ir mėginti įtikinti auką indėlį nutraukti, o lėšas pervesti į debetinę sąskaitą arba vėlgi išgryninti. Pažymėtina, kad šis aprašytas apgaulės modelis tėra vienas iš galimų variantų. Praktikoje kombinacijos, vaidmenys, apgaulės pretekstai gali kisti (pvz. susisiekimas ir bendravimas vien per VoIP, apsimetimas kitų institucijų, įmonių atstovais, atvykęs bendrininkas gali teigti, kad aukos turimi grynieji pinigai galimai netikri ir pažadėti vakare atvežti „tikrus“). Patikimumui didinti aukai gali būti siunčiami suklastoti dokumentai iš banko, ikiteisminio tyrimo įstaigos ir t. t. Tokių dokumentų, net ir pasų klastojimą gali atlikti ir dirbtinis intelektas pavyzdžiui „ChatGPT“[195]. Todėl konkretus apgaulės modelis ir mechanizmas priklauso nuo situacijos aplinkybių, kaltininko(-ų) bei aukos charakteristikų.

Vienas iš dažnai naudojamų višingo taktikos elementu yra skambinančiojo numerio

---

[193] „Lietuvos Aukščiausiasis Teismas, Baudžiamųjų bylų skyrius, 2023 m. birželio 22 d. nutartis baudžiamojoje byloje Nr. 2K-170-495/2023“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2173648

[194] BioCatch. „Let’s Hack Your Mind.“ *BioCatch Blog*, žiūrėta 2025 m. gruodžio 17 d., https://www.biocatch.com/blog/lets-hack-your-mind

[195] Borys Musielak @ Warsaw, įrašas socialiniame tinkle *X* (buv. Twitter), https://x.com/michuk/status/1907078798908248478

klastojimas (angl. caller ID spoofing[196]), kai ekrane rodomas patikimai atrodantis numeris ar pavadinimas. Patikrinus tokį numerį viešuosiuose šaltiniuose, galima pastebėti, jog toks telefono numeris oficialiai priskirtas tikrai institucijai ar policijos pareigūnui. Kaip ir smišingo atveju, nusikaltėliai siekia, jog auka jaustų spaudimą veikti skubiai ir nespėtų kritiškai įvertinti situacijos. Tuo pačiu gali būti panaudojama iš kitų šaltinių gauta informacija, leidžianti skambutį pritaikyti konkrečiam asmeniui. Taip pat gali būti taikomos automatizuotos numerių rinkimo sistemos (angl. wardialing)[197], leidžiančios greitai pasiekti daug potencialių aukų.

Dėl analogiško veikimo principo šiame darbe plačiau nebus nagrinėjamos kitos lentelėje pateiktos fišingo atmainos, kadangi jų esminis mechanizmas išlieka tas pats – apgaule išgauti konfidencialius duomenis arba nukreipti vartotoją į fiktyvią svetainę, siekiant gauti prieigą prie finansinių sąskaitų, lėšų ar kitos vertingos informacijos.

Po fišingo ar jo atmainų atakų įvykdymo, įprastai pradedama paskutinė nusikalstamos veikos grandinės fazė – pėdsakų slėpimas. Šis etapas, kaip ir bet kurioje nusikalstamoje veikoje yra būtinas tam, kad būtų apsunkintas nusikaltimo išaiškinimas ir užkirstas kelias duomenų (įrodymų) surinkimui. Šioje vietoje svarbu trumpai aptarti pėdsakų (įkalčių) ypatumus nusikaltimų elektroninėje erdvėje kontekste. Kriminalistikoje pėdsakai yra skirstomi materialiuosius ir idealiuosius. Materialūs pėdsakai lieka ant fizinių objektų ir jų pavidalas taip pat fizinis. Idealieji pėdsakai lieka asmens atmintyje reiškinio prisiminimo ir jo suvokimo pavidalu, todėl galima teigti, kad šis pėdsakas priklauso nuo asmens, priimančio informaciją, intelekto[198]. Tokio pobūdžio pėdsakai būdingi nusikaltimams, kurie vykdomi fizinėje aplinkoje. Pasak Šarūno Grigaliūno, nusikaltimai elektroninėje erdvėje atliekami pasitelkus kompiuterius, kompiuterinius tinklus, šiuolaikines informacines technologijas. Kadangi šie įrankiai naudojami informacijai rinkti, nusikalstamai veiklai planuoti ir vykdyti, tokių įkalčių paieškai atlikti reikalingos specifinės eksperto žinios bei techninės priemonės[199]. Kalbant apie fišingą, kaip ir apie kitus šiame darbe analizuojamus apgaulės modelius, kurie priskirtini nusikaltimams, daromiems elektroninėje erdvėje, akivaizdu, jog šiuo atveju atsiranda „virtualiųjų“ pėdsakų grupė, sąlygota specifinių „kibernetinėje erdvėje“ vykstančių procesų, kurie žmogaus juslėmis

[196] CrowdStrike. „What Is a Vishing Attack?“ *CrowdStrike,* žiūrėta 2025 m. gruodžio 17 d., https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/vishing-attack/

[197] Ibid.

[198] Kaminskaitė, Gertrūda. 2023. „Prekybos žmonėmis nusikaltimų kriminalistinė charakteristika.“ *Mykolo Romerio universiteto Viešojo saugumo akademija*, 824 p., https://cris.mruni.eu/cris/bitstreams/7f8f5221-7327-4c7e-8b1d-477f96f2f6db/download

[199] Grigaliūnas, Šarūnas. 2020. *Nusikaltimų elektroninėje erdvėje ekspertinio tyrimo metodas*. Daktaro disertacijos santrauka, Kauno technologijos universitetas; Vilniaus Gedimino technikos universitetas. 3 p., https://epubl.ktu.edu/object/elaba:68107071/68107071.pdf

nesuvokiami, todėl užima tarpinę padėtį tarp materialiųjų ir idealiosios prigimties pėdsakų[200]. Atsižvelgiant į šiuolaikinio sukčiavimo įgyvendinimo galimybes, darbo autorius vertinimu, prie Š. Grigaliūno minimu įrankių papildomai priskirtini ir mobilieji bei kiti išmanieji įrenginiai, suteikiantys prieigą prie interneto arba sudarantys sąlygas tiek nusikalstamai veikai vykdyti, tiek virtualiesiems pėdsakams formuotis.

Virtualūs pėdsakai gali likti keliuose šaltiniuose:

- įrenginiuose, kuriais buvo vykdoma nusikalstama veika (kompiuteryje, telefone, planšetėje ir pan.);
- ryšio ir komunikacijos kanaluose (el. pašte, žinutėse, socialiniuose tinkluose, pokalbių programėlėse ir pan.);
- interneto paslaugose ir sistemose, su kuriomis buvo sąveikauta (svetainėse, paskyrose, serveriuose, duomenų bazėse ir pan.);
- kituose skaitmeniniuose įrenginiuose ar laikmenose (plačiau žr. šaltinį)[201].

Virtualieji pėdsakai yra labai nepastovūs, jie gali būti pašalinti, koreguoti arba būti saugomi tik tam tikrą laiką.

Kadangi fišingo branduoliniu įrankiu įprastai laikytini kompiuteriai – pirmiausia imamasi skaitmeninių, arba kitaip tariant įvykių žurnalų (angl. Logs) pašalinimo arba modifikavimo[202]. Įvykių žurnalai yra skaitmeniniai įrašai, kurie fiksuoja įvykius informacinėse sistemose ir tinkluose, įskaitant kompiuterio naudotojų veiksmus, sistemos klaidas, prisijungimus ir kitus techninius procesus. Tokie žurnalai yra vienas pagrindinių skaitmeninių duomenų (įrodymų) šaltinių atliekant kibernetinių nusikaltimų tyrimus, nes tai leidžia rekonstruoti įvykių seką, nustatyti įsilaužimo būdą bei galimai nustatyti įtariamąjį. Viena didžiausių kibernetinio saugumo sertifikavimo švietimo, mokymo ir paslaugų įmonė „EC-Council“[203] pažymi, jog įvykių žurnalų ištrynimas yra įprastą kibernetinių nusikaltėlių praktika, kai sąmoningai pašalinami įrašai, galintys būti pripažinti įrodymais teisme. Tokie veiksmai iš esmės eliminuoja nustatyti atakos mastą, jos priežastis bei veikimo mechanizmą, taip apsunkinant tyrimą[204]. Be kita ko, pasitaiko atveju, kai nusikalstamos veikos subjektai imasi tyčinio klaidinimo taktikos, siekdami ne tik sunaikinti pėdsakus, bet ir sukurti klaidinančią

[200] Grigaliūnas, Šarūnas. 2015. Elektroninių nusikaltimų pėdsakų ir įtariamojo įpročių koreliacija. Magistro baigiamasis darbas, Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra. 11, 12 p. https://epubl.ktu.edu/object/elaba:8641422/8641422.pdf

[201] АМИА. „Преступления в информационной сфере.“ *Amia.by*, žiūrėta 2025 m. gruodžio 17 d., 18 p., https://www.amia.by/book/umk/Kaf_rasl_prestypleniy/itsfera/project/DswMedia/tekstlekcii.pdf

[202] „EC-Council. „Clearing Logs in Ethical Hacking: What You Need to Know.“ *EC-Council,* žiūrėta 2025 m. gruodžio 17 d., https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/clearing-logs/

[203] EC-Council. „International Council of E-Commerce Consultants.“ *EC-Council,* žiūrėta 2025 m. gruodžio 17 d., https://www.eccouncil.org/

[204] EC-Council. „Clearing Logs in Ethical Hacking: What You Need to Know.“ *EC-Council,* žiūrėta 2025 m. gruodžio 17 d., https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/clearing-logs/

tyrimo aplinką. Tokiu atveju į žurnalus gali būti įrašomi fiktyvūs duomenys, kuriami nereikalingi vartotojų profiliai ar atliekami veiksmai, kurie nukreipia tyrimą šalutine kryptimi ir kliudo nustatyti tikruosius nusikalstamos veikos tikslus bei mechanizmą[205].

Kita svarbi kliūtis nustatant tokio pobūdžio nusikalstamas veikas yra veiklos maskavimas naudojant anonimiškumą užtikrinančias technologijas, tokias kaip virtualūs privatūs tinklai (angl. VPN), tarpiniai serveriai (angl. proxy servers)[206] ar anoniminis „Tor“[207] tinklas. Šios priemonės leidžia nuslėpti tikrąją IP adreso kilmę, todėl net ir nustačius įsilaužimo laiką ir kitus svarbius techninius požymius – atsekti realų vykdytojo buvimo vietos adresą tampa sudėtinga arba neįmanoma. Tokiu būdu sukuriamas tarpininkų grandinės efektas, kai tyrimą apsunkina daugybė virtualių „pereinamųjų“ mazgų, dažnai išsidėsčiusių skirtingose jurisdikcijose, kas lemia ne tik techninius, bet ir teisės taikymo bei duomenų rinkimo sunkumus, reikalaujančius tarptautinio bendradarbiavimo ir specialių teisinių procedūrų. Kai kuriais atvejais nusikaltėliai pasitelkia pažangias priemonės, tokias kaip savaime išsitrinančios kenkėjiškos programos (angl. self-deleting malware), kurios po užduoties įvykdymo automatiškai pašalina veiklos pėdsakus[208], taip dar labiau apsunkindamos skaitmeninių duomenų paiešką ir analizę.

Analizuojant fišingo ir jo atmainų veikimo mechanizmus matyti, kad šių nusikalstamų veikų įgyvendinimas nėra spontaniškas procesas, o jam būdingas kruopštus ir iš anksto suplanuotas pasirengimas. Pasirinkus konkretų fišingo būdą – atitinkamai pasirenkamas atakos kanalas, kuriuo bus siekiama pasiekti taikinį. Masinio pobūdžio fišingo atakose planavimo etapas daugiausia apima techninių bei socialinės inžinerijos priemonių parinkimą, siekiant suformuoti įtikinamą bendrinį pranešimo turinį (pretekstą), skirta kuo platesnei auditorijai. Tuo tarpu tikslingose fišingo (angl. spearphishing) ar individualizuotose atakose, taip pat višingo atvejais, pasirengimo metu gali būti renkama ir analizuojama konkreti informacija apie pasirinktą auką (jos vardas, pavardė, gyvenamoji vieta, kiti kontaktiniai duomenys), kuri vėliau naudojama siekiant klaidinti auką. Kaip pagalbinė priemonė fišingo atakų pasirengimo etape gali būti naudojamos dirbtinio intelekto priemonės, tokios kaip „KawaiiGPT“, leidžiančios generuoti apgaulingų pranešimų turinį ir supaprastinti atakos planavimo procesą[209]. Toks įrankis

---

[205] Veriato. „How Cyber Attackers Hide Their Tracks After Committing Digital Fraud.“ *Veriato,* žiūrėta 2025 m. gruodžio 17 d., https://veriato.com/blog/how-cyber-attackers-hide-their-tracks-after-committing-digital-fraud/

[206] Nacionalinis kibernetinio saugumo centras. „Tarpinės stoties paslauga (Proxy).“ *NKSC.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.nksc.lt/rekomendacijos/tarpines_stoties_paslauga_proxy.html

[207] Esaugumas. „Anoniminis tinklas TOR.“ *Esaugumas.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.esaugumas.lt/articles/anoniminis-tinklas-tor

[208] Gupta, Rahul. „Self Deleting Malware: Antivirus Bypass Techniques Using Batch Scripting.“ *LinkedIn,* žiūrėta 2025 m. gruodžio 17 d., https://www.linkedin.com/pulse/self-deleting-malware-antivirus-bypass-techniques-using-gupta--m2dsc

[209] Unit 42. „The Dilemma of AI: Malicious LLMs.“ *Palo Alto Networks – Unit 42*, žiūrėta 2025 m. gruodžio 17 d., https://unit42.paloaltonetworks.com/dilemma-of-ai-malicious-llms/

nusikalstamiems tikslams yra patrauklūs nes, skirtingai nei „ChatGPT“, jis neturi įdiegtų turinio ribojimų ir saugumo patikrų, todėl leidžia generuoti tokio pobūdžio pranešimus be papildomų apribojimų[210]. Pasitelkiama ir „phishing-as-a-service“ rinka, kai įsigyjami jau parengti fišingo atakų rinkiniai, talpinimo ir nukreipimo paslaugos bei aukų duomenų paketai, o atsiskaitoma už tai kripotvaliutomis[211]. Pasirengimo etape taip pat numatomi pėdsakų slėpimo būdai, pasirenkamos anonimiškumo technologijos, sukuriamos ar tamsiojoje interneto rinkoje įsigyjamos reikiamos priemonės. Neretais atvejais suburiama specializuota bendrininkų grupė, kurioje kiekvienas dalyvis atlieka aiškiai apibrėžtą funkciją – nuo techninio parengimo iki aukų paieškos bei gautų duomenų panaudojimo. Tokia nuosekli veiksmų seka atskleidžia tyčini bei organizuotą veikos pobūdį, būdinga sudėtingoms šiuolaikinėms sukčiavimo formoms.

Vertinant aukščiau aptartus metodus, pažymėtina, jog tokie veikimo būdai negali būti tapatinami vien tik su sukčiavimu, kadangi kartais jie neturi tiesioginių požymių, būdingu klasikinio sukčiavimo sudėčiai. Tam tikrais atvejais šios veikimo schemos gali būti vertinamos kaip duomenų vagystė, kai išviliota informacija panaudojama ne iš karto ar ne būtinai siekiant tiesioginės turtinės naudos, bet pavyzdžiui, neteisėtam prisijungimui prie informacinių sistemų (BK 198-1 str.) elektroninių duomenų perėmimui ir panaudojimui (BK 198 str.) ar pasirengimui kitoms nusikalstamoms veikoms, kurios reglamentuojamos kitose BK normose. Kalbant apie sukčiavimą padaryta elektroninėje erdvėje, o konkrečiai pasitelkiant fišingo metodus, tokie atvejai turėtų būti kvalifikuojami kaip idealioji nusikalstamų veikų sutaptis, t. y. apimanti ne tik sukčiavimą, bet ir kitas veikas, susijusias su el. įsilaužymu, neteisėtu duomenų gavimu ir jų panaudojimu. Be to, atkreiptinas dėmesys, kad tradicinio sukčiavimo atvejais nusikaltimo dalyku laikomas apgaulės būdu įgytas svetimas turtas (kilnojamieji ar nekilnojamieji daiktai). Tuo tarpu fišingo ir jo atmainų sukčiavimo elektroninėje erdvėje atvejais pirminiu nusikalstamos veikos tikslu/dalyku tampa ne pats turtas, o jautri informacija, t. y. prisijungimo prie elektroninės bankininkystės sistemos duomenys, autorizacijos kodai, elektroninių mokėjimo priemonių rekvizitai ar kiti prieigos raktai. Tokia informacija vėliau gali būti panaudojama neteisėtoms finansinėms operacijoms ar kitų nusikalstamų veikų realizavimui. Taigi ši informacija tampa tarpine, bet esmine grandimi visame nusikalstamos veikos mechanizme. Dėl to aukščiau aptarti veikimo modeliai neturėtų būti traktuojami tik kaip techninės priemonės ar komunikacijos kanalai. Jie iš esmės atspindi nusikalstamos veikos būdą, kaip konkretus apgaulės metodas, kuriame derinamas melagingas turinys ir jo technologinė įgyvendinimo forma. Tokiu būdu

[210] Abnormal Security. „Combating WormGPT.“ *Abnormal.ai,* žiūrėta 2025 m. gruodžio 17 d., https://abnormal.ai/blog/combating-wormgpt

[211] Europol. 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Luxembourg: Publications Office of the European Union. Žiūrėta 2025 m. gruodžio 17 d., https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf

galima aiškiau atriboti, kas laikytina apgaulės turiniu (veikos būdu), o kas tik priemonėmis padedančiomis šią apgaulę įgyvendinti.

Investicinis sukčiavimas

Kalbant apie šiuolaikinio skaitmeninio pasaulio raida, neatsitiktinai ankščiau minėtoje nusikalstamumo elektroninėje erdvėje statistikoje investicinis sukčiavimas išskiriamas kaip viena iš labiausiai paplitusių sukčiavimo formų[212]. Pastaraisiais metais investavimas tapo itin populiaria finansinio elgesio forma, kurią skatina tiek augantis visuomenės finansinis raštingumas, tiek ir visuotinė praktika ieškoti alternatyvų apsaugoti santaupas nuo infliacijos bei pasyviai gauti papildomą pelną[213]. Tokia tendencija, be abejo, sudaro palankią terpę ir nusikalstamoms schemoms, kuriomis pasinaudojama siekiant apgaule įgyti asmenų lėšas.

Vienoje LAT nagrinėjamoje byloje, asmuo buvo nuteistas už tai, kad apgaule savo naudai įgijo didelės vertės svetimą turtą. O būtent – jis, turėdamas tikslą apgaule savo naudai įgyti didelės vertės svetimą turtą ir žinodamas, kad neturi licencijos, suteikiančios teisę Lietuvos Respublikoje nuolat ir profesionaliai teikti investicines paslaugas, sukūrė interneto puslapį, kuriame melagingai reklamavo investicinį projektą, žadėdamas per 10 mėn. mokėti 8 proc. palūkanas, o po metų grąžinti visą investuotą sumą. Tęsdamas šią schemą ir veikdamas per tarpininką, jis suklaidino kelis investuotojus, kurie į nurodytą banko sąskaitą pervedė iš viso 91 000 Eur, taip apgaule perduodami didelės vertės svetimą turtą. Siekdamas sudaryti patikimumo įspūdį, investuotojams buvo išduoti projekto sertifikatai, kuriuose nurodytos investavimo sąlygos ir kontaktai. Investuotojams buvo mokamos 8 proc. palūkanos, tačiau vėliau mokėjimai nutraukti, o elektroniniu paštu melagingai pranešta, kad lėšos neva užšaldytos dėl pinigų plovimo politikos. Praėjus metams nuo investavimo dienos, investuotojams pinigai negrąžinti. (Lietuvos Aukščiausiojo Teismo 2024 m. vasario 13 d. nutartis baudžiamojoje byloje 2K-13-654/2024[214]).

JAV Federalinio tyrimų biuras (angl. FBI Internet Crime Complaint Center) investicinį sukčiavimą apibrėžia kaip apgaulę, kai asmenys viliojami pažadais dėl mažos arba visai nerizikingos investicijos, kuri iš tiesu realybėje neegzistuoja. Įprastai sukčiai siekia įtikinti potencialius investuotojus siūlydami grąžą, kurios dydis akivaizdžiai „per geras, kad būtų tiesa“.

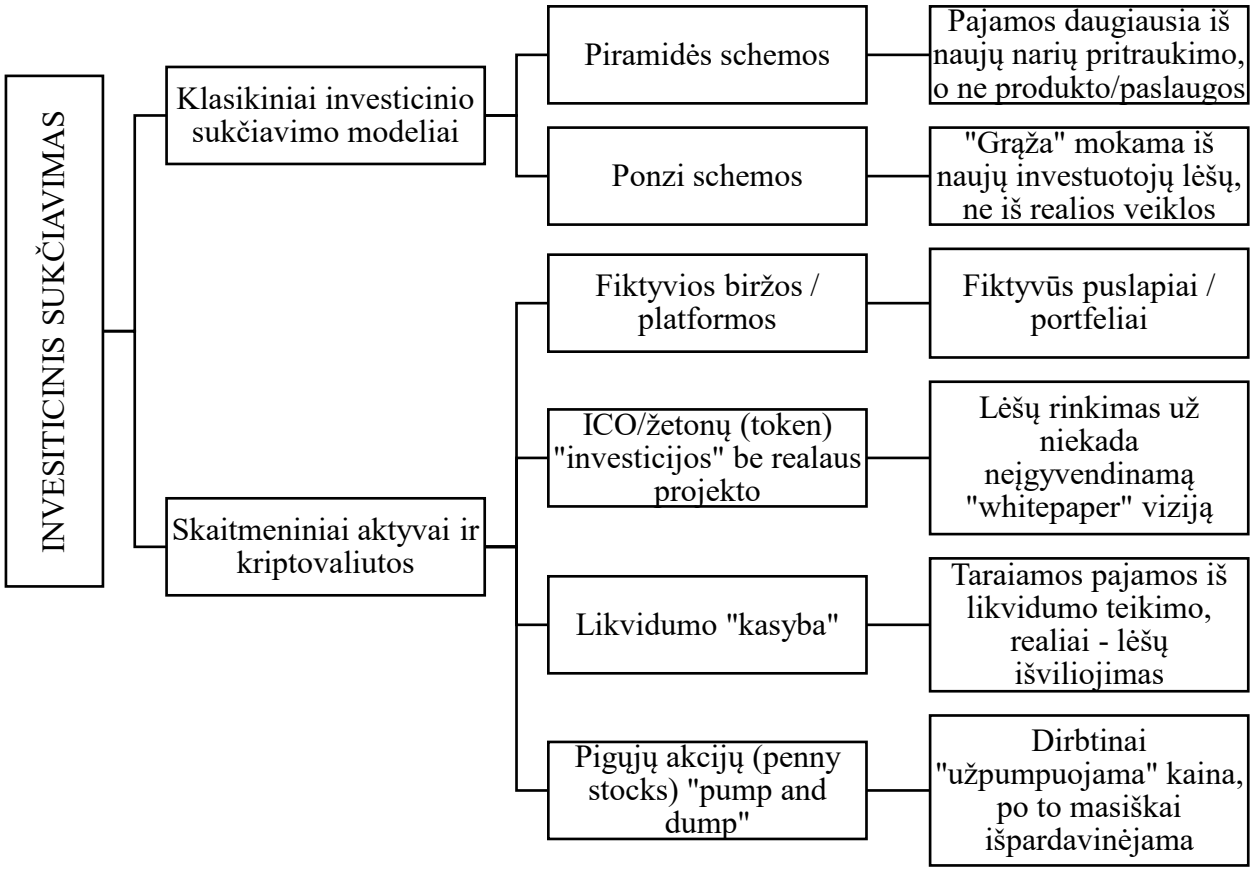
---

[212] Paysera. „Dažnos finansinės apgaulės.“ *Paysera.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.paysera.lt/v2/lt-LT/blog/daznos-finansines-apgaules

[213] Mano pinigai. „Gyventojų investavimas: tendencijos teigiamos, bet esminis lūžis dar neįvykęs.“ *Manopinigai.vz.lt,* žiūrėta 2025 m. gruodžio 17 d., https://manopinigai.vz.lt/investavimas/gyventoju-investavimas-tendencijos-teigiamos-bet-esminis-luzis-dar-neivykes/

[214] „Lietuvos Aukščiausiasis Teismas, Baudžiamųjų bylų skyrius, 2024 m. vasario 13 d. nutartis baudžiamojoje byloje Nr. 2K-13-654/2024“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2225669

Tokie garantuotos grąžos pažadai yra vienas iš pagrindinių apgaulės požymių[215]. Darbo autoriaus vertinimu sąvoka „investicinis sukčiavimas“, gali būti interpretuojama kaip bendrinis šio nusikalstamo elgesio terminas, kadangi šis neteisėtas veikimas praktikoje pasireiškia įvairiomis formomis skirtingose srityse.



Lentelė Nr. 4, Investicinio sukčiavimo rūšys, autorius – V. Golovko.

Kaip matyti lentelėje, investicinis sukčiavimas gali būti labai įvairus, t. y. nuo seniai žinomų Ponzi ar piramidinių schemų[216] iki sąlyginai naujų formų, susijusių su skaitmenine ekonomika bei kriptovaliutų rinka. Nors piramidės ir Ponzi schemos šiais laikais gali pasireikšti elektroninėje erdvėje, jos jau yra išsamiai analizuotos mokslinėje literatūroje[217] ir teisėsaugos praktikoje[218]. Rezonansiniais šių schemų pavyzdžiais laikytini Charleso Ponzi[219] bei Sergejaus

[215] Internet Crime Complaint Center (IC3). „Investment Fraud.“ *IC3.gov*, žiūrėta 2025 m. gruodžio 17 d., https://www.ic3.gov/CrimeInfo/Investment

[216] U.S. Securities and Exchange Commission. „Investment Scams Targeting Groups.“ *Investor.gov,* žiūrėta 2025 m. gruodžio 17 d., https://www.investor.gov/protect-your-investments/fraud/types-fraud/investment-scams-targeting-groups

[217] Buzaitė, Indrė. 2014. *Finansinių piramidžių poveikio valdymas tiesioginio pardavimo įmonių veikloje.* Magistro baigiamasis darbas, Vytauto Didžiojo universitetas. https://portalcris.vdu.lt/server/api/core/bitstreams/ab842dbd-30ba-4939-acba-d1601eb3c783/content

[218] Lietuvos policija. „Apgaulės piramidė: kaip nepakliūti į naujausias finansines pinkles.“ *Policija.lrv.lt,* žiūrėta 2025 m. gruodžio 17 d., https://policija.lrv.lt/lt/naujienos/apgaules-piramide-kaip-nepakliuti-i-naujausias-finansines-pinkles/

[219] Smithsonian National Postal Museum. „Ponzi Scheme.“ *National Postal Museum,* žiūrėta 2025 m. gruodžio 17 d., https://postalmuseum.si.edu/exhibition/behind-the-badge-case-histories-scams-and-schemes/ponzi-scheme

Mavrodžio „MMM“[220] sukurtos finansinės schemos, tapusios klasikiniu investicinio sukčiavimo simboliu. Dėl šios priežasties šiame darbe pagrindinis dėmesys bus sutelktas į inovatyvias, technologiniu požiūriu pažangesnes investicinio sukčiavimo formas, pasireiškiančias elektroninėje erdvėje.

Skaitmeniniai aktyvai ir kriptovaliutos

Kriptovaliutų sektorius pastaraisiais metais išgyvena intensyvią plėtrą. Tarptautinės kriptovaliutų mokėjimų įmonės „Triple-A“ duomenimis, 2024 m. daugiau nei 560 milijonų asmenų visame pasaulyje disponavo kriptovaliutomis, tai sudarė apie 6,8 % to meto pasaulio populiacijos[221]. Iš pirmo žvilgsnio toks procentas viso pasaulio gyventojų gali atrodyti menkas, tačiau vertinant jį aktyvios ir finansiškai raštingos visuomenės dalies kontekste, tokia apimtis liudija plačią kriptovaliutų integraciją į globalią finansų sistemą. Šį reiškinį lemia tiek technologinės naujovės, tiek investuotojų susidomėjimas alternatyviomis kapitalo įdarbinimo galimybėmis. Kriptovaliutų idėja gimė 2008 m., kai Satoshi Nakamoto paskelbė dokumentą „Bitcoin: A Peer-to-Peer Electronic Cash System“[222], kuriame buvo aprašyta decentralizuota elektroninių pinigų sistema, paremta „blockchain“ technologija. Šiandien kriptovaliuta suprantama kaip skaitmeninė valiuta, leidžianti atlikti finansinius sandorius tiesiogiai tarp naudotojų, apeinant trečiųjų šalių tarpininkus. Ši valiuta veikia decentralizuotai, todėl jos nekontroliuoja ir nereguliuoja nei vyriausybės, nei centriniai bankai. Nors toks modernus finansinis modelis ir išplečia prieigą prie finansinių paslaugų ir mažina tarpininkavimo kaštus, tačiau jis kartu didina kibernetinio saugumo rizikas, ypač kalbant apie tarpvalstybinius sandorius. Šalia to susiformavo decentralizuotų finansų sistema, kurioje veikia tarpusavio atsiskaitymai, skolinimo ir keitimo protokolai bei decentralizuotos keityklos, kas sukčiavimo atvejais sukuria apčiuopiamų kibernetinio saugumo bei atsekamumo problemų. Todėl, tokia aplinka suteikia kibernetiniams nusikaltėliams papildomų galimybių anonimiškai plauti pinigus ir vykdyti sukčiavimus[223].

Kriptovaliutų vertė formuojasi pagal paklausos ir pasiūlos principą, t. y. kuo didesnis susidomėjimas ir pirkėjų skaičius, tuo labiau kyla jų kaina ir atvirkščiai. Būtent dėl šios priežasties kriptovaliuta išlieka nepastovi ir linkusi sparčiai kisti, todėl ji laikoma ne tik

[220] „MMM“, *Vikipedija*, https://lt.wikipedia.org/wiki/MMM

[221] TripleA. „Cryptocurrency Ownership Data.“ *TripleA*, žiūrėta 2025 m. gruodžio 17 d, https://www.triple-a.io/cryptocurrency-ownership-data

[222] Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*., https://bitcoin.org/bitcoin.pdf

[223] Badi, Sadi. 2024. *The Digital Evolution of Financial Crime: How Cross-Border Fraud Is Reshaping Cybersecurity*. ResearchGate. Žiūrėta 2025 m. gruodžio 16 d., https://www.researchgate.net/publication/389939761_The_Digital_Evolution_of_Financial_Crime_How_Cross-Border_Fraud_is_Reshaping_Cybersecurity

atsiskaitymo priemone, bet ir rizikingu investavimo objektu[224].

Investicinis sukčiavimas per fiktyvius ICO ir kitus žetonų platinimus

KRIPTOTERMINAI	TRUMPAS PAAIŠKINIMAS
Blockchain (blokų grandinė)	Decentralizuota skaitmeninė duomenų bazė, kurioje informacija (pvz. sandoriai) saugoma chronologiškai sujungtose ir nekintamuose blokuose, kas sudaro grandinę[225].
Smart contract (išmanioji sutartis)	Kodo ir duomenų rinkinys, įdiegtas į blokų grandinės tinklą kriptografiškai pasirašytomis transakcijomis, kurį vykdo tinklo mazgai, užtikrinant, kad visi gautų tą patį vykdymo rezultatą, o pastarieji būtų įrašomi į blokų grandinę[226].
Cryptocurrency Wallet (kriptoturto piniginė)	Įrenginys ar programa, kuri saugo kriptovaliutų raktus ir suteikia sąsają pasiekti kriptoturtą. Tokia piniginė turi adresą ir privačius raktus, kuriais pasirašomos kriptovaliutų transakcijos[227].
CEX / DEX	CEX (centralizuota birža) – prekybos platforma, kuri veikia kaip tarpininkė tarp pirkėjų ir pardavėjų kriptovaliutų rinkoje. Ji suveda pavedimus, valdo naudotojų paskyras ir kontroliuoja privačius raktus. DEX (decentralizuota birža) – tai tarpusavio (peer-to-peer) platforma, kurioje prekiaujama kriptovaliutomis tiesiogiai su kitais vartotojais, be tarpinikavimo.[228]
Coin (moneta)	„Veikia savo pačių blokų grandinėje ir pirmiausia naudojamos kaip mainų priemonė, pavyzdžiui, Bitcoin ir Ether“.[229]
Token (žetonas)	„Veikia esančioje blokų grandinėje (pvz., Ethereum) ir paprastai atlieka konkretesnes funkcijas projekto ekosistemoje, pavyzdžiui, suteikia prieigą prie paslaugų ar valdymo teises“.[230]
Altcoin (altkoinas)	Skaitmeninė valiuta, alternatyvi bitkoinui. Žodis „altcoin“ yra sudarytas

[224] Swedbank. „Kriptovaliutos.“ *Swedbank Blogas,* žiūrėta 2025 m. gruodžio 17 d., https://blog.swedbank.lt/zodynelis/kriptovaliutos

[225] Encyclopedia Britannica. „What Is Blockchain?“ *Britannica*, žiūrėta 2025 m. gruodžio 17 d., https://www.britannica.com/money/what-is-blockchain

[226] Ethereum Foundation. „Išmaniosios sutartys.“ *Ethereum.org*, žiūrėta 2025 m. gruodžio 17 d., https://ethereum.org/lt/developers/docs/smart-contracts/

[227] Encyclopedia Britannica. „Cryptocurrency Wallet.“ *Britannica*, žiūrėta 2025 m. gruodžio 17 d., https://www.britannica.com/money/cryptocurrency-wallet

[228] „Централизованная биржа (CEX) против децентрализованной (DEX): полный разбор.“ *Cryptomus,* žiūrėta 2025 m. gruodžio 17 d., https://cryptomus.com/ru/blog/centralized-exchange-cex-vs-decentralized-exchange-dex-complete-comparison

[229] Telco. „Kuo skiriasi kriptovaliutos moneta ir žetonas?“ *Telco.in,* žiūrėta 2025 m. gruodžio 17 d., https://www.telco.in/lt/support-center/cryptocurrency-basics/what-is-the-difference-between-a-coin-and-a-token

[230] Ibid.

	iš žodžių „alternatyvus“ ir „moneta“ santraukos. Kitaip tariant tai yra visos kriptovaliutos išskyrus bitkoiną[231].

Lentelė Nr. 5, Kriptoterminai, autorius – V. Golovko.

Plėtojantis kriptovaliutų rinkai, kartu atsirado ir nauji kapitalo pritraukimo būdai. Viena ryškiausių tokių priemonių tapo „pirminiai virtualiojo turto žetonų siūlymai[232]“ (angl. Inital Coin Offering – ICO)[233]. ICO – tai sąlyginai nauja finansavimo forma, leidžianti ankstyvosios stadijos įmonėms ar projektų kūrėjams pritraukti lėšų, išleidžiant skaitmeninius žetonus ir juos parduodant investuotojams mainais už kriptovaliutas arba tradicines valiutas. Tokiu būdu ICO laikomi alternatyva tradiciniams finansavimo būdams, tokiems kaip rizikos kapitalas ar verslo angelų[234] investicijos.

ICO procesui būdingi keli pagrindiniai elementai. Pirmiausia, išleidžiami žetonai, kurie gali atlikti skirtingas funkcijas:

- Valiutiniai žetonai naudojami atsiskaitymams;
- Paslaugų žetonai suteikia prieigą prie būsimo produkto ar paslaugos;
- Investiciniai žetonai gali garantuoti teisę į būsimas pajamas ar kitą ekonominę naudą.

Projekto iniciatoriai parengia vadinamąją „baltąją knygą“ (angl. white paper)[235], kurioje pateikiama informacija apie projektą, numatoma technologiją, žetonų pasiūlą, kainodarą bei platinimo mechanizmą. Esminę reikšmę ICO kampanijoje turi internetinė rinkodara, pavyzdžiui socialiniai tinklai, kriptovaliutų forumai ir kitos skaitmeninės platformos, kurios tampa pagrindiniu informacijos sklaidos kanalu. Nors ICO ir viešasis akcijų siūlymas (angl. Initial Public Offering – IPO) turi tam tikrų panašumų – abu naudojami kapitalui pritraukti ir gali sudominti plačią investuotojų bazę, visgi, jų teisinis reguliavimas iš esmės skiriasi. IPO yra griežtai reglamentuojami, reikalaujant registracijos ir nuolatinės priežiūros, tuo tarpu ICO ilgą laiką veikė teisinės neapibrėžties sąlygomis, nes nei nacionaliniu, ne tarptautiniu lygmeniu nebuvo aiškių taisyklių dėl žetonų prigimties ir jų platinimo procedūrų. Dėl to ICO tapo patrauklia priemone „startuoliams“ – jaunoms, aktyviosios stadijos įmonėms, kurios siekia greitai pritraukti kapitalo be tarpininkų, išvengti sudėtingų derybų dėl dalyvavimo kapitale bei

[231] bitFlyer. „What Is an Altcoin?“ *bitFlyer*, žiūrėta 2025 m. gruodžio 17 d., https://bitflyer.com/en-eu/faq/55-7

[232] Lietuvos bankas. „Vertybinių popierių požymių turinčių žetonų siūlymo gairės.“ *Lietuvos bankas,* žiūrėta 2025 m. gruodžio 17 d., https://www.lb.lt/uploads/documents/files/STO_gaires_pakartotinai_20190904.pdf?

[233] Europos Parlamentas. 2021. *Impact of Cryptocurrency – In-depth Analysis (BRIE 696167).* Žiūrėta 2025 m. gruodžio 17 d., https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS_BRI(2021)696167_EN.pdf

[234] „Verslo angelai,“ *Vikipedija,* https://lt.wikipedia.org/wiki/Verslo_angelai

[235] Europos Parlamentas. 2021. *Impact of Cryptocurrency – In-depth Analysis (BRIE 696167).* Žiūrėta 2025 m. gruodžio 17 d., https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS_BRI(2021)696167_EN.pdf

brangių reguliacinių procedūrų.

Nors ICO suteikė galimybę pasiekti globalią investuotojų auditoriją ir sąlyginai paprastesnį lėšų surinkimo modelį, tačiau kartu iškilo ir nemaža rizika investuotojams. Dėl informacijos asimetrijos, nepatikrintų „baltųjų knygų“ turinio, žetonų teisinės prigimties neaiškumo bei skaidrumo stokos investuotojai dažnai susiduria su kapitalo praradimu. Europos Parlamento tyrimų tarnybos 2021 m. ataskaitoje pažymima, kad dauguma ICO projektų nepajėgė peraugti į realiai veikiančius verslus, o dalis jų pasirodė esą visiškai fiktyvūs. Tokiais atvejais investuotojai liko be veiksmingos teisinės apsaugos, nes žetonų platinimas ilgą laiką vyko reguliacinio vakuumo sąlygomis. Taigi vienas ryškiausių ICO sukčiavimo modeliu yra vadinamasis „exit scam“[236]. Finansinių paslaugų platforma „Volity“[237] jį apibrėžia kaip iš anksto suplanuotą apgaulę, kai projekto kūrėjai, surinkę lėšas iš investuotojų per ICO ar kitus žetonų platinimus, tyčia nutraukia projektą, išjungia visus komunikacijos kanalus, stabdo žetonų perlaidas ir perveda surinktą kapitalą į sunkiai atsekamas pinigines. Tokia apgaulės schema vystosi keliais etapais. Iš pradžių sukuriamas bei pristatomas projektas, išleidžiami žetonai. Juos sukūrus, skelbiama išankstinė prekyba, parengiama fiktyvi „baltoji knyga“, intensyviai vykdoma rinkodara. Techniniu lygmeniu išmaniojoje sutartyje (kontrakte) gali būti paliekamos kūrėjui palankios funkcijos, pavyzdžiui, savininko privilegijos, neribota žetonu emisija, galimybė išjungti pervedimus ar inicijuoti slaptus išėmimus ir t.t. Po kurio laiko, pritraukus investuotojus bei sukaupus pakankamą kapitalą, apgaulingas projektas uždaromas, o surinktos lėšos išskaidomos. Sukčiai maskuoja savo nusikalstamus veiksmus pervesdami lėšas tarp skirtingų tinklų (tiltais), konvertuojamos, dėl ko realus lėšų judėjimo atsekimas tampa itin apsunkintas. Investuotojams faktiškai lieka beverčiai žetonai.

Ryškiausia ICO plėtros banga buvo fiksuota 2017-2018 m.[238], tačiau tokie sukčiavimo atvejai fiksuojami iki šiol[239]. Šiuo metu tokie investiciniai pasiūlymai dažniau organizuojami mažiau reguliuojamose jurisdikcijose arba pasitelkiant modifikuotas formas, tokias kaip pirminiai biržų siūlymai (angl. IEO), saugumo žetonų siūlymai (angl. STO), ar decentralizuoti žetonų platinimai (angl. IDO)[240]. Nepaisant formos, investuotojų rizikos išlieka tos pačios, t. y. informacijos asimetrija, „baltųjų knygų“ nepatikimumas, žetonų teisinio statuso neapibrėžtumas

[236] Seth, Shobhit. „What Is a Cryptocurrency Exit Scam? How Do You Spot One?“ *Investopedia*, žiūrėta 2025 m. gruodžio 17 d., https://www.investopedia.com/tech/whats-cryptocurrency-exit-scam-how-spot-one/

[237] Volity Team. „What Is a Crypto Exit Scam?“ *Volity.io*, žiūrėta 2025 m. gruodžio 17 d., https://volity.io/crypto/exit-scams/

[238] Swartz, Lana. 2017. „Theorizing the 2017 Blockchain ICO Bubble as a Network Scam.“ *New Media & Society*, Special Issue: Scams, Fakes, and Frauds. Preprint. https://llaannaa.com/preprint_swartz_nms_ico.pdf

[239] Alfa.lt. „FNTT atlieka kratas su „Bankera“ siejamose įmonėse.“ *Alfa.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.alfa.lt/aktualijos/lietuva/fntt-atlieka-kratas-su-bankera-siejamose-imonese/377143/

[240] Flagship. „How to Protect Yourself from ICO, IEO, and IDO Scams: A Quick Guide.“ *Flagship.fyi,* žiūrėta 2025 m. gruodžio 17 d., https://flagship.fyi/outposts/market-insights/how-to-protect-yourself-from-ico-ieo-and-ido-scams-a-quick-guide/

bei ribota priežiūra. Dėl šių priežasčių „ICO schema“ išlieka viena aktualių investicinio sukčiavimo formų.

Likvidumo „kasyba“

Likvidumo kasyba (angl. liquidity mining) arba pelningumo ūkininkavimas (angl. yield farming), yra viena iš decentralizuoto finansų (angl. DeFi)[241] ekosistemos investavimo formų. Šis investavimas paremtas idėja, kad kriptoturto savininkai gali uždirbti pasyvias pajamas įnešdami savo lėšas (kriptovaliutas) į decentralizuotą biržą (angl. DEX)[242] ar kitą likvidumo fondą. Tokiu būdu investuotojai prisideda prie rinkos likvidumo užtikrinimo, o mainais gauna atlygį, pavyzdžiui palūkanos, prekybos mokesčių dalis arba valdymo žetonai, suteikiantys tam tikras teises dalyvauti platformos valdyme. Šį praktika pati savaime yra teisėta ir funkcionuoja kaip investicijos alternatyva tradiciniams būdams.

Vis dėlto, pasitaiko atveju kai yra išnaudojamas investuotojo pasitikėjimas tariamai veikiančia sistema. Likvidumo „kasybos“ atvejais apgaulė maskuojama DeFi terminija ir dApp[243] sąsajomis[244]. Federalinio tyrimų biuro Interneto nusikaltimų skundų centras išanalizavo tokios investicinės apgaulės taktiką[245]. Visų pirma sukčiai per socialinius tinklus ar susirašinėjimo programėles užmezga asmeninį ar profesinį ryšį (kelias dienas ar savaites augina pasitikėjimą) ir vilioja dalyvauti „populiarioje“ investicijoje bei žada 1-3 % „dienos grąžą“. Jei auka dar neturi kriptovaliutos, pastaroji nuosekliai apmokoma jos įsigijimo ir galiausiai gauna nuorodą į tariamą likvidumo kasybos dApp‘ą programėlę. Vėliau aukos prašoma susieti savo kriptopiniginę ir suaktyvinti dalyvavimą (pvz. paspaudžiant tam tikrą mygtuką). Atsidariusiame lange, kuris vizualiai imituoja teisėtos piniginės sąsają, prašoma suteikti plačius turtinius leidimus. Suteikus perteklines leidimų teisęs, sukčiai per išmaniąją sutartį gali nurašyti visą piniginėje laikomą kriptoturtą be atskiro patvirtinimo. Tačiau aukai rodomas suklastotas pelningumo langas, kuriame fiksuojama tariamą grąža. Taigi principas toks kaip investiciniame sukčiavime per fiktyvias platformas, t. y. auka, manydama, kad investicija sėkminga – didina įnašus. Galiausiai visos lėšos ištuštinamos į sukčių valdomas pinigines, o tariamas „klientų aptarnavimas“ pateikia įvairius pasiteisinimus (neva mokesčius padengti, „priežiūros“ rinkliava) ir reikalauja papildomų įmokų lėšoms atrakinti, tačiau išmokos taip ir neįvyksta.

---

[241] Mpost. „DeFi.“ *Mpost.io,* žiūrėta 2025 m. gruodžio 17 d., https://mpost.io/lt/glossary/defi/

[242] RWaltz. „Liquidity Mining in DEX: How It Works and Its Benefits.“ *RWaltz.com,* žiūrėta 2025 m. gruodžio 17 d., https://www.rwaltz.com/blog/liquidity-mining-in-dex-how-it-works-and-its-benefits

[243] dYdX. „What Are dApps?“ *dYdX*, žiūrėta 2025 m. gruodžio 17 d., https://www.dydx.xyz/crypto-learning/dapps

[244] California Department of Financial Protection and Innovation. „Crypto Scam Tracker.“ *DFPI.ca.gov,* žiūrėta 2025 m. gruodžio 17 d., https://dfpi.ca.gov/consumers/crypto/crypto-scam-tracker/#:~:text=In%20a%20liquidity%20mining%2Fyield,victims%20purchase%20additional%20crypto%20assets

[245] Internet Crime Complaint Center (IC3). „IC3 Warns of Increase in Use of Remote Desktop Protocol to Facilitate Fraud.“ *IC3.gov,* žiūrėta 2025 m. gruodžio 17 d., https://www.ic3.gov/PSA/2022/PSA220721

Investicinis sukčiavimas „pump and dump“

Dar vienas iš labiausiai atpažįstamų investicinio sukčiavimo modelių kriptovaliutų rinkoje yra vadinamoji angl. „pump and dump“ (kainos išpūtimo ir pardavimo) schema. Šio mechanizmo ištakos siekia dar XIX a., kai Volstrito spekuliantai, tokie kaip Daniel Drew, pasitelkdavo gandus ir koordinuotus pirkimus, kad dirbtinai pakeltų pasirinktų bendrovių akcijų kainą ir vėliau jas parduotų pelningai, palikdami nuostolius vėliau prisijungusiems investuotojams[246]. XX a. pradžioje tokios praktikos išsivystė į vadinamąją angl. „Pool operation“, kai investuotojų grupės ir biržos makleriai susitardavo dėl bendro akcijų pirkimo, dirbtinai sukurdavo paklausą ir keldavo pasirinktų bendrovių akcijų kainą, vėliau, pasiekus piką, jas išsiparduodavo. Tokios manipuliacijos buvo taikomos tiek mažiau žinomoms, tiek didelėms bendrovėms, pavyzdžiui „Chrysler“, „RCA“ ir sukeldavo pastebimus rinkos svyravimus bei lėmė investuotojų nuostolius[247]. Garsiu pavyzdžiu laikomas ir „Anaconda Copper“ atvejis 1928-1929 m. Tuomet J. D. Ryan ir W. Rockefeller, veikdami susitarę, ribojo vario pasiūlą ir per vadinamą bendrąją sąskaitą sukaupė apie 1,5 milijono bendrovės akcijų, taip dirbtinai skatindami jų kainos kilimą. Nuo maždaug 40 JAV dolerių 1928 m. gruodį „Anaconda“ akcijų kursas pakilo iki 128 JAV dolerių 1929 m. kovą. Pasiekus piką pradėtas intensyvus išsipardavimas lėmė staigų kainos kritimą ir didelius smulkiųjų investuotojų nuostolius[248].

Šiuolaikinėje kriptoturto rinkoje „pump and dump“ veikia pagal tą pačią paklausos ir pasiūlos principą kaip ir tradicinėse finansų rinkose, tačiau paklausa į tam tikrą finansinį aktyvą sukuriama dirbtinai, kas lemia trumpalaikį kainos šuolį. Pirmiausia parenkamas lengvai paveikiamas taikinys, tai gali būti menkai žinoma, mažos kapitalizacijos moneta (angl. coin) ar žemo likvidumo ar neseniai išleistas žetonas (angl. token). Sukčiai iš anksto įsigyja didelį kiekį pasirinkto aktyvo, taip iškart padidindami prekybos apimtį ir sudarydami „judėjimo“ iliuziją[249]. Reklaminė „pump“ dalis vykdoma anonimiškai socialiniuose tinkluose, kuriamos fiktyvios grupės, arba įsigyjamos jau egzistuojančios su tūkstančiais narių, juose skelbiami atgaliniai skaičiavimai iki pirkimo „signalo“, platinamos žinutės, kuriančios skubos, tariamo populiarumo įspūdį ir t.t[250]. Pritraukius masę dalyvių, papildomi pirkimai trumpam dar labiau pakelia skaitmeninių aktyvų kainą.

Vėliau seka „dump“ dalis, t. y. pasinaudodami dirbtinai išreklamuota paklausa, sukčiai

---

[246] Investopedia. „A Brief History of Fraud.“ *Investopedia*, žiūrėta 2025 m. gruodžio 17 d., https://www.investopedia.com/articles/financial-theory/09/history-of-fraud.asp

[247] „Pool operation”, *Wikipedia,* https://en.wikipedia.org/wiki/Pool_operation

[248] „Anaconda Copper,“ *Wikipedia,* https://en.wikipedia.org/wiki/Anaconda_Copper

[249] Bitstamp. „What Are Pump and Dump Schemes?“ *Bitstamp.net,* žiūrėta 2025 m. gruodžio 17 d., https://www.bitstamp.net/learn/crypto-trading/what-are-pump-and-dump-schemes/

[250] U.S. Commodity Futures Trading Commission. „Customer Advisory: Beware of Pump-and-Dump Schemes.“ *CFTC.gov,* žiūrėta 2025 m. gruodžio 17 d., https://www.cftc.gov/sites/default/files/2019-12/customeradvisory_pumpdump0218.pdf?utm

parduoda savo turimus aktyvus už išpūstą kainą, palikdami kitus investuotojus su nuvertėjusiais žetonais ar monetomis. Visas pirkimo-pardavimo ciklas gali trukti vos kelias minutes. Jei tradicinėse rinkose ši schema istoriškai sieta su mažai žinomoms akcijoms ar bendrovėms, tai kriptoturto aplinkoje jos paplitimą didina techninis naujų žetonų paleidimo paprastumas, galimybė nedidelei grupei kontroliuoti pasiūlą ir apimtis bei anonimiškumas.

Pažymėtina ir tai, kad „pump and dump“ sukčiavimo schema siejasi su kitomis investicinio sukčiavimo metodais, jau minėtas „exit scam“ ir vadinamasis „rug pull“[251] (sukčiavimo sudedamoji, kai nutraukiamas apgaulingas projektas ir pasisavinamos investuotojų lėšos). Visais šiais atvejais sukčiai dirbtinai sukelia didelį ažiotažą aplink naują skaitmeninį turtą (tai gali būti ne tik kriptovaliuta, bet ir unikaliais skaitmeniniais žetonais (angl. Non-Fungible token – NFT[252])), siekia pritraukti kuo daugiau investuotojų ir pakelti turto vertę iki maksimaliai įmanomo lygio. Vėliau, kai tik sukaupiamas pakankamas kapitalas, projekto kūrėjai dingsta[253].

Investicinis sukčiavimas per fiktyvias biržas ir platformas

Analizuojant sustabdytus ikiteisminius tyrimus 2020-2024 m. šiuo klausimu, pastebima, jog investicinis sukčiavimas, vykdomas per fiktyvias biržas ir platformas, yra gana sudėtingas, ypač vertinant jo techninį įgyvendinimą. Paprastai tokios schemos nėra vieno asmens darbas. Tokiam įgyvendinimui suburiama bendrininkų grupė, kur kiekvienas narys atlieka tam tikrą funkciją: vieni atsakingi už IT įrankių sukūrimą, įgijimą, kiti už aukų pritraukimą bei jų verbavimą, treti už pinigų srautų nukreipimą bei paslėpimą. Šios apgaulės mechanizmą galima išskirti į 4 etapus.

Pirmasis etapas apima fiktyvios biržos ar prekybos platformos sukūrimas. Kaip ir ankščiau aptartoje fišingo dalyje, sukčiai tuo pačiu principu sukuria internetinę svetainę arba programėlę, kuri savo dizainu, struktūra ir funkcionalumu imituoja teisėtą investavimo aplinką. Skirtumas tas, jog tokiose platformose įprastai įdiegiami visi tipiški investavimo aplinkos atributai – registracijos formos, „portfelio“ valdymo langai, dirbtinai generuojami realaus laiko rodikliai, sukuriantys investicijų augimo iliuziją. Tokia simuliacija formuoja patikimumo įspūdį ir paskatina auką investuoti.

Antrasis etapas apima aukų pritraukimą. Šiame etape nusikalstamos veikos subjektai aktyviai naudojasi reklamos priemonėmis socialiniuose tinkluose, pranešimų siuntimo programėlėse ar netgi telefoniniais skambučiais, pristatydami investiciją kaip patikimą galimybę

---

[251] CoinMarketCap. „Rug Pull.“ *CoinMarketCap Academy*, žiūrėta 2025 m. gruodžio 17 d., https://coinmarketcap.com/academy/glossary/rug-pull

[252] Business Insider. „NFT Meaning: What Is an NFT and How Does It Work?“ *Business Insider,* žiūrėta 2025 m. gruodžio 17 d., https://www.businessinsider.com/personal-finance/investing/nft-meaning

[253] Organization for Security and Co-operation in Europe. „OSCE Supports Uzbekistan’s Efforts to Combat Money Laundering and Terrorism Financing.“ *OSCE.org*, žiūrėta 2025 m. gruodžio 17 d., https://www.osce.org/oceea/587475

užsidirbti. Paprasčiausias ir pasyviausias būdas pritraukti auditoriją yra melagingos tekstinės, vaizdo reklamos, suklastoti atsiliepimai socialinių tinklų grupėse bei skelbimų komentaruose iš fiktyvių profilių, kurių tikslas sudaryti įspūdį, jog investicija yra plačiai naudojama ir patikima. Pavyzdžiui, suinteresuotas asmuo, pamatęs „Facebook“ skelbimą, gali užpildyti anketą palikdamas savo vardą, pavardę, telefono numerį ar el. paštą. Šie duomenys vėliau naudojami tiesioginiam susiekimui ir tolimesniam aukos verbavimui. Pastaruoju metu taip pat pastebima, kad sukčiai pasitelkia ir pažangias informacines technologijas, pavyzdžiui, dirbtinio intelekto algoritmus bei vadinamąsias giliąsias klastotes (angl. deepfake)[254]. Gilioji klastotė – tai technologija, veikianti dirbtinio intelekto ir gilaus mokymosi (angl. deep learning) pagrindu, naudojanti neuroninius tinklus suklastotiems vaizdo ir garso įrašams kurti, kai asmens veidas ar balsas pakeičiamas kitu. Pažymėtina, kad veidų keitimas nuotraukose daugelį metų buvo įprasta praktika naudojant „Photoshop“ programą, tačiau, plėtojančios informacinės technologijos, dirbtinio intelekto sukūrimas, sudarė pagrindą atsirasti giliosioms klastotėms. Įtikinamam „deepfake“ vaizdo įrašui sukurti pakanka 1-3 asmens nuotraukų skaičiaus. Sistema naudoja žmogaus atvaizdo sintezę, t. y. sujungia kelias nuotraukas, kuriose asmuo pavaizduotas iš skirtingų kampų, su skirtingomis veido išraiškomis ir generuoja judantį vaizdą. Analizuodamas vaizdus, algoritmas mokosi, kaip žmogus atrodo ir gali judėti. Garso giliosios klastotės atveju programai pakanka labai trumpos, net ir 5 sekundžių balso įrašo ištraukos, kad būtų galima imituoti konkretaus asmens balso tembrą ir tartį. Toks „mėginys“ lengvai gaunamas iš trumpo telefoninio pokalbio ar viešo įrašo ir gali būti naudojamas tiek iš anksto sugeneruotiems pranešimams, tiek realiojo laiko skambučiams[255]. Tokiu būdu gali būti imituojami vadovų, giminaičių skambučiai ar net žinomų asmenų veidai ir balsai vaizdo įrašuose, sukuriant klaidingą patikimumo įspūdį[256]. Pavyzdžiui, Hack Forums svetainėje siūloma sukurti vaizdo įrašą, kurio vertė priklauso nuo trukmės (20 JAV dolerių už minutę). Galima rasti skelbimų, kuriuose nurodoma, kad asmuo pasirengęs sumokėti 16 000 JAV dolerių už giliųjų klastočių gaminimo paslaugas (vaizdo įrašai ir nuotraukos)[257]. Lietuvos Respublikoje taip pat fiksuoti atvejai, kai socialiniuose tinkluose buvo platinami suklastoti vaizdo įrašai, imituojantys žiniasklaidos

[254] BBC Newsround. „What Is Cyber Crime?“ *BBC,* žiūrėta 2025 m. gruodžio 17 d. https://www.bbc.co.uk/newsround/69009887

[255] Moin, Md Tahmid, Jobayer Hossain, and Selim S. A. Bhuiyan. „Cyber Fraud Detection Using Machine Learning: A Comprehensive Review.“ *arXiv*, žiūrėta 2025 m. gruodžio 17 d. https://arxiv.org/abs/2402.18085

[256] АМИА. „Преступления в информационной сфере.“ *Amia.by*, žiūrėta 2025 m. gruodžio 17 d., 11, 12 p., https://www.amia.by/book/umk/Kaf_rasl_prestypleniy/itsfera/project/DswMedia/tekstlekcii.pdf

[257] Biometric Update. „Dark news from dark web: Deepfakers are getting their act together.“ *BiometricUpdate.com*, žiūrėta 2025 m. gruodžio 17 d https://www.biometricupdate.com/202105/dark-news-from-dark-web-%20deepfakers-are- getting-their-act-together

reportažus, kuriais siekta išvilioti lėšas[258]. Nors šiuo konkrečiu atveju buvo kalbėta apie tariamus prizus, tokios apgaulės pagrindą sudarančios technologijos gali būti taikomos ir siekiant pritraukti investuotojus į fiktyvias platformas.

Trečiasis etapas – investuotojų klaidinimas. Po kurio laiko, ar net tą pačią dieną po užpildytos anketos, palikto komentaro, su auka susisiekiama telefonu ar el. paštu. Bendravimo metu sukčiai žada didelį pelną ir beveik visišką investicijų saugumą, teigiama, jog jų investicinė svetainė ar programėlė yra plačiai naudojama visoje Europoje, pateikiami fiktyvūs sertifikatai. Tokiu būdu pasinaudodami asmenų siekiu apsaugoti santaupas nuo infliacijos arba gauti greitą pelną. Auka įtikinama palaipsniui. Pradinis etapas apima asmeninį kontaktą telefonu, el. paštu arba socialinių tinklų žinutėmis, pristatant tariamas investavimo galimybes. Aukai pateikiamos vizualiai profesionalios ir patikimai atrodančios internetinės platformos, kuriose demonstruojami fiktyvūs investicijų grafikai ir statistiniai duomenys. Pokalbio metu neretai nurodoma atsisiųsti į savo telefoną ar kompiuterį nuotolinio valdymo įrangą, pvz., „TeamViewer“, ar „Anydesk“. Tokiais atvejais sukčiai nuotoliniu būdu padeda įdiegti „investavimo“ programėlę bei išsiunčia el. paštu prisijungimo duomenis.

Įtikinta pabandyti, aukai nurodoma papildyti savo profilio sąskaitą. Iš pradžių tai gali būti nedidelė pradinė suma (pvz. 50-200 Eur). Vos tik lėšos pervedamos, platformoje pradedamas rodyti tariamas investicijų augimas. Siekiant sustiprinti pasitikėjimą, gali būti organizuojamas vaizdo skambutis, kurio metu demonstruojami bei aptariami itin geri „investicijos rezultatai“. Auka netgi gali gauti realią nedidelę išmoką (pvz. 100-300 Eur), taip dirbtinai sukuriamas įspūdis, kad investicija jau duoda grąžą. Vėliau, manipuliuojant emocijomis pasitelkiami argumentai apie „rinkos pokyčius“, „geriausią progą“ arba „norint užsidirbti daugiau – reikia daugiau investuoti“, t. y. raginama investuoti didesnes sumas ar net imti paskolas. Sukčiai gali nurodyti, jog jų tariama investavimo įmonė numato galimybę savo klientams skolinti lėšas programėlėje (fiktyvi birža → fiktyvi piniginė → fiktyvus papildymas). Tačiau po suteiktos skolos, auka beveik iškart raginama ją grąžinti, t. y. papildant investavimo įmonės balansą. Aukai neturint lėšų papildomiems įnašams ar „skolos“ padengimui, sukčiai, įtikindami bei pasinaudodami įrenginių nuotolinio valdymo instrumentu padeda pastarajai pasiimti paskolą bei atlikti reikiamus įnašus.

Taigi iš bylų analizės matyti, jog sukčiai gali siūlyti „pagalbą“ atliekant pavedimus, pildant paskolos paraiškas, taip įtvirtindami kontrolę. Tipiška apgaulės grandies dalis yra tariami „mokesčiai“ arba „depozitai“, būtini neva tam, kad auka galėtų „išsiimti“ jau uždirbtą pelną. Šie

[258] LRT. „Įspėjama apie sukčius, kurie dengiasi žinomais LRT vardais.“ *LRT.lt*. 2025 m. rugpjūčio 17 d. Žiūrėta 2025 m. gruodžio 17 d. https://www.lrt.lt/naujienos/lietuvoje/2/2635297/ispejama-apie-sukcius-kurie-dengiasi-zinomais-lrt-vardais?srsltid=AfmBOopvZGs6hS7GP0W0gpy0qgCfVd4gE3S5rqhx1YH-9CQs7x4fd13X

reikalavimai, tik su naujomis priežastimis kartojasi kaskart po įvykdyto mokėjimo. Tokia praktika atitinka „pig-butchering“[259] modelį, kai auka palaipsniui įtraukiama vis gilesniam finansiniam įsipareigojimui, kol galiausiai praranda visas lėšas. Analogiškas laipsniško įtraukimo į nuoseklaus finansinių prašymų didinimo mechanizmas būdingas ir **romantiniam sukčiavimui**. Tokiais atvejais sukčiai interneto pažinčių ar bendravimo svetainėse kuria netikrus profilius ir medžioja aukas. Vėliau, užmezgus emocinį, romantinį ryšį su auka iš pradžių atsiranda smulkūs finansiniai prašymai, o vėliau pereinama prie didesnių sumų, kurias sukčiai pagrindžia netikėtomis aplinkybėmis (pvz. liga, kelionė, muitai ir t.t.)[260]. Tokie procesai gali tęstis mėnesius ar net metus, kol auka, suvokia apgaulės mąstą.

Ketvirtasis etapas – pinigų pasisavinimas ir platformos uždarymas. Pasiekus finansinį tikslą arba kilus aukos įtarimams, platforma paprastai staiga nustoja veikti, interneto svetainė išnyksta, o investuotojas praranda bet kokią galimybę atgauti lėšas. Praktikoje tai paprastai reiškia, kad lėšos iki platformos „užsidarymo“ jau būna išvestos, pavyzdžiui per nekaltų tarpininkų elektronines pinigines, virtualius IBAN → į kriptovaliutų biržas → į kitas pinigines, kuriose faktiškai prarandama galimybė nustatyti galutinį lėšų savininką. Siekiant dar labiau apsunkinti finansinių srautų atsekimą, gali būti atliekami smulkūs pervedimai per skirtingas jurisdikcijas, kuriose pinigai yra išgryninami pasitelkiant vadinamuosius „pinigų mulus“, po ko lėšos keliauja toliau. Šiuo atveju tapatybei maskuoti gali būti naudojamos ankščiau minėtos anonimiškumo priemonės, tokios kaip IP adresų keitimai, TOR tinklai, botnet, VoIP, vienkartiniai numeriai ir t.t.

Sukčiavimas su išankstiniais mokėjimais (avansinis)

Sukčiavimas su išankstiniais mokėjimais arba kitaip tariant avansinis sukčiavimas savo veikimo mechanizmu, tarp jau aptartų apgaulės būdų, yra artimiausias tradiciniams sukčiavimo modeliams. Sukčiavimo padarymo būdas visada susijęs su apgaule aktyvia, pasyvia forma ar per trečiuosius asmenis. Šiuo atveju tai yra tokia apgaulės forma, kai nukentėjusysis įtikinamas tiesiogiai ar netiesiogiai iš anksto sumokėti mokestį, avansą ar „administracines“ išlaidas už žadamą prekę, paslaugą ar finansinę naudą, kuri neįvyksta, t. y. prekė nepristatoma, paslauga nesuteikiama, grąža negrąžinama. Esminis skirtumas nuo tradicinio veikimo yra tas, kad apgaulė įvykdoma elektroninėje erdvėje. Ši apgaulė plačiai paplitusi vartojimo santykiuose, pavyzdžiui fiktyvios e. parduotuvės, nuomos, siuntų, rezervacijos ar loterijos mokesčiai. Susisiekimas su auka gali būti vykdomas tiek tiesiogiai – el. paštu, SMS, per socialinius tinklus, tiek netiesiogiai

[259] California Department of Financial Protection and Innovation (DFPI). *Pig Butchering – How to Spot and Report the Scam.* Žiūrėta 2025 m. gruodžio 17 d., https://dfpi.ca.gov/news/insights/pig-butchering-how-to-spot-and-report-the-scam/

[260] Pinigų plovimo prevencijos kompetencijų centras. „Sukčiavimo prevencija gyventojams.“ *AMLcenter.lt.* Žiūrėta 2025 m. gruodžio 17 d., https://amlcenter.lt/sukciavimo-prevencija/sukciavimo-prevencija-gyventojams/

– per internetines paieškas, internetines reklamas. Apgaulės pretekstai gali būti varijuojami nuo ypač patrauklios kainos prekių pasiūlymų iki tariamų apgyvendinimo paslaugų ar laimėto prizo, kurių suteikimui neva būtinas išankstinis ar mokesčių apmokėjimas. Apgaulei gali būti naudojami fiktyvūs, „vogti“ socialinių paskyrų profiliai (fišingo aukos), pasisavinamos svetimų parduodamų prekių nuotraukos, vaizdo įrašai. Aukai atlikus el. mokėjimą, jokia prekė neatsiunčiama, paslauga nesuteikiama. Sukčiai gali nurodyti įvairias priežastis, dėl kurių paslaugos atlikimas ar prekės išsiuntimas bus vilkinamas, tačiau vėliau apgaulingas skelbimas, svetainė ar paskyra, kurie buvo naudojami kaip priemonė apgaulei įvykdyti, panaikinama arba apribojama nukentėjusiojo prieiga (blokavimas). Gautos lėšos gali būti nukreipiamos į tarptautines banko sąskaitas arba tiesiogiai į vietinių trečiųjų asmenų banko sąskaitas, kurių turėtojams už jų banko sąskaitų panaudojimą atlygintina dalis sumos. Tokie įtraukti į apgaulę asmenys iš esmės nesuvokia tikros lėšų kilmės ar paskirties ir pasilieka procentinę dalį kaip tariamą užmokestį, o likusi suma išgryninama ir perduodama per kurjerius. Pažangesniais atvejais, trečiasis asmuo iš anksto užverbuojamas per tariamo darbo internetu pasiūlymus ir įkalbinėjamas susikurti kriptoturto keityklos paskyrą, kurioje papildoma kriptopiniginė, o šis skaitmeninis aktyvas persiunčiamas į organizatorių kontroliuojamas kriptopinigines, taip sukuriant papildomas grandis, kurios apsunkina lėšų atsekamumą.

Pavyzdžiui, vienoje Vilniaus apygardos teismo nagrinėtoje byloje asmuo buvo nuteistas už sukčiavimą, nes interneto puslapyje www.autoplius.lt paskelbė netikrą skelbimą apie tariamai parduodamą mikroautobusą. Pirkėjas iš užsienio, susisiekęs su pardavėju nurodytu telefonu, susitarė įsigyti kelis tokius mikroautobusus už bendrą sutartą sumą ir pavedimais pervedė avansą, o vėliau – likusią kainos dalį į pardavėjo nurodytą banko sąskaitą. Kadangi pirkėjas tuo metu negalėjo atvykti į Lietuvą, su pardavėju buvo sutarta transporto priemones laikinai laikyti iki pirkėjo atvykimo. Atvykęs pirkėjas sužinojo, kad mikroautobusai parduoti tretiesiems asmenims, o pervesti pinigai nebus grąžinti. Tokiu būdu pardavėjas apgaule įgijo pirkėjui priklausiusias lėšas. (Vilniaus apygardos teismo 2025 m. spalio 23 d. nutartis baudžiamojoje byloje Nr. 1A-235-1036/2025)[261].

Analizuojant aptartas sukčiavimo elektroninėje erdvėje formas, matyti, kad jų kvalifikavimas ir tyrimas neatsiejamas nuo kriminalistinės charakteristikos elementų tarpusavio ryšio. Nors baudžiamoji teisė nustato bendras sukčiavimo sudėties ribas, realus apgaulės įgyvendinimas elektroninėje erdvėje vyksta pasitelkiant konkrečias technines priemones ir naudojamus informacijos perdavimo kanalus, kurie lemia tiek nusikalstamos veikos eigą, tiek pėdsakų susidarymo ir slėpimo ypatumus. Aptarti apgaulės mechanizmai rodo, kad šiuolaikinės

[261] „Vilniaus apygardos teismas, Baudžiamųjų bylų skyrius, 2025 m. spalio 23 d. nutartis baudžiamoji byla Nr. 1A-235-1036/2025“,. *Infolex.* https://www.infolex.lt/tp/2344316

sukčiavimo schemos įgyvendinamos pagal iš anksto parengtą veikimo modelį, apimantį psichologinio poveikio, technologines priemones ir finansinių srautų maskavimą. Priklausomai nuo veikimo būdo, elektroninėje erdvėje pirminiu pasikėsinimo objektu neretai tampa ne pats turtas, kaip įprasta tradicinio sukčiavimo atvejais, o jautrūs duomenys, kurie vėliau, tarsi raktas nuo seifo, panaudojami kaip priemonė turtinei žalai padaryti. Dėl sukčiavimo elektroninėje erdvėje savotiško specifiškumo, jo vertinimas vien tik per formalius baudžiamosios teisės požymius yra nepakankamas, kadangi veikos pobūdį ir sudėtingumą atskleidžia kriminalistinė analizė. Nukentėjusiojo ir kaltininko portretai šiame poskyryje neaptariami, nes kitame skyriuje jie bus nagrinėjami remiantis sustabdytų ikiteisminių tyrimų duomenimis ir moksline literatūra, taip nuosekliai papildant šiame poskyryje aptartų kriminalistinės charakteristikos elementų analizę.

3. SUKČIAVIMO ELEKTRONINĖJE ERDVĖJE TYRIMO YPATUMAI: PRADĖJIMAS, TYRIMO EIGA IR KLIŪTYS

BPK 2 straipsnis įpareigoja prokurorą bei ikiteisminio tyrimo pareigūnus reaguoti į kiekvieną informaciją apie galimai padarytą nusikalstamą veiką ir atlikti visus reikalingus proceso veiksmus bei sprendimus, kad nusikalstama veika būtų atskleista. Į teisėsaugos instituciją dėl įžvelgtos galimai padarytos nusikalstamos veikos gali kreiptis visi asmenys, o tikrinti gautą informaciją apie galimai padarytą nusikalstamą veiką, rinkti nusikalstamą veiką pagrindžiančius ar paneigiančius duomenis (įrodymus) yra ikiteisminio tyrimo pareigūnų pareiga. Kita vertus, tiek pradedant baudžiamąjį procesą, tiek jau vykstančio proceso metu privalu įsitikinti, jog nėra priežasčių, dėl kurių procesas negali būti vykdomas. Priešingu atveju, neatsakingai pradėtas ir nepagrįstas baudžiamasis persekiojimas būtų neteisėtas ir grubiai pažeistų persekiojamų asmenų teises ir interesus.

3.1 Ikiteisminio tyrimo pradėjimas ir duomenų šaltiniai sukčiavimo elektroninėje erdvėje bylose

BPK 166 straipsnio 1 dalies 1 punkte numatytos ikiteisminio tyrimo pradėjimo sąlygos: 1) skundo, pareiškimo ar pranešimo apie nusikalstamą veiką gavimas ir 2) prokurorui ar ikiteisminio tyrimo pareigūnui patiems nustačius nusikalstamos veikos požymius. BPK 168 straipsnio 1 dalis numato, kad prokuroras ar ikiteisminio tyrimo pareigūnas gali atsisakyti pradėti ikiteisminį tyrimą esant vienai iš dviejų numatytų alternatyvių sąlygų – kai skunde, pareiškime ar pranešime apie nusikalstamą veiką nurodyti faktai yra akivaizdžiai neteisingi arba yra aiškios BPK 3 straipsnio 1 dalyje nurodytos aplinkybės. Tai reiškia, jog gavus skundą, pareiškimą ar pranešimą apie nusikalstamą veiką, BPK 168 straipsnio 1 dalyje numatyta galimybė nepradedant ikiteisminio tyrimo patikrinti pateiktą informaciją (atlikti patikslinamuosius veiksmus - *kurie nesusiję su procesinėmis prievartos priemonėmis: įvykio vietos apžiūra, įvykio liudytojų apklausos, taip pat iš valstybės ar savivaldybės įmonių, įstaigų, organizacijų, pareiškėjo ar asmens, kurio interesais pateiktas skundas, pareiškimas ar pranešimas, reikalaujami duomenys ar dokumentai, atliktos pareiškėjo ar asmens, kurio interesais pateiktas skundas, pareiškimas ar pranešimas, apklausos*[262]), o įvertinus gautus duomenis, atsižvelgiant į išdėstytą teisinį reglamentavimą nustačius, ar nenustačius objektyvių duomenų priimamas sprendimas dėl ikiteisminio tyrimo pradėjimo/nepradėjimo.

Kalbant apie ikiteisminio tyrimo pradėjimą, tame tarpe ir pagal BK 182 straipsnį, kiekvienas ikiteisminio tyrimo pradžios atvejis registruojamas vadovaujantis Lietuvos

[262] Lietuvos Respublikos baudžiamojo proceso kodeksas, 168 str., redakcija nuo 2020-11-20. Teisės aktų registras. Žiūrėta 2025 m. gruodžio 17 d https://www.infolex.lt/ta/10708:str168

Respublikos generalinio prokuroro 2008 m. rugpjūčio 11 d. įsakymu Nr. I-110 „Dėl Rekomendacijų dėl ikiteisminio tyrimo pradžios ir jos registravimo tvarkos patvirtinimo“[263]. Vadovaujantis BPK 167 straipsniu, ikiteisminis tyrimas dėl nusikalstamų veikų, numatytų BK 182 straipsnio 1 ir 4 dalyse, pradedamas tik tuo atveju, kai yra nukentėjusiojo skundas ar jo teisėto atstovo pareiškimas. Ikiteisminis tyrimas dėl sukčiavimų pagal BK 182 straipsnio 2 ir 3 dalis (dėl didelės ir labai didelės vertės) gali būti pradedamas prokuroro reikalavimu. Tai reiškia, jog nukentėjusio asmens skundas ar jo teisėto atstovo pareiškimas ar pranešimas apie nusikalstamą veiką nebūtinas, o ikiteisminis tyrimas pradedamas nustačius nusikalstamos veikos požymius.

Ikiteisminio tyrimo atlikimo vietą ir įstaigą, kuri bus atsakinga už ikiteisminio tyrimo atlikimą, nustato prokuroras, vadovaudamasis minėtomis rekomendacijomis dėl ikiteisminio tyrimo pradžios ir jos registravimo tvarkos. Paprastai ikiteisminį tyrimą pradeda tos ikiteisminio tyrimo įstaigos, kurios veiklos teritorijoje gyvena nukentėjusysis, pareigūnai. Ikiteisminių tyrimų dėl sukčiavimų elektroninėje erdvėje eigose, dažnai pasitaiko atvejų, kai nustatoma, jog nukentėjusiojo ir sukčiavimo subjekto vietovės skiriasi. Pavyzdžiui, tyrimas gali būti pradėtas pagal nukentėjusiojo gyvenamąją vietą Vilniaus mieste, o tyrimo eigoje paaiškėti, jog veika iš esmės įvykdytą (veikos baigtumas) Visagino mieste. Tokiais atvejais, vadovaujantis BPK 174 straipsniu ir Rekomendacijomis dėl ikiteisminio tyrimo organizavimo ir vadovavimo jam, patvirtintų Lietuvos Respublikos generalinio prokuroro 2025 m. gegužės 30 d. įsakymu Nr. I-123 „Dėl Rekomendacijų dėl ikiteisminio tyrimo organizavimo ir vadovavimo jam patvirtinimo“[264] 39, 40 punktų nuostatomis, siekiant užtikrinti, kad nusikalstama veika būtų ištirta kuo greičiau ir išsamiau, tolimesnio tyrimo organizavimui ir vadovavimui ikiteisminis tyrimas perduodamas atitinkamos apygardos prokuratūrai.

Pradedant bei atliekant ikiteisminius tyrimus dėl sukčiavimo elektroninėje erdvėje atvejais, ikiteisminio tyrimo įstaigos vadovaujasi Lietuvos Respublikos generalinio prokuroro metodinėmis rekomendacijomis dėl sukčiavimo elektroninėje erdvėje nusikalstamų veikų kvalifikavimo ir tyrimo[265]. Tai iš esmės yra pagalbinis instrumentas, kuriame nurodomi kriterijai, kuriais reikėtų vadovautis nustatant šių nusikalstamų veikų ikiteisminio tyrimo atlikimo vietą,

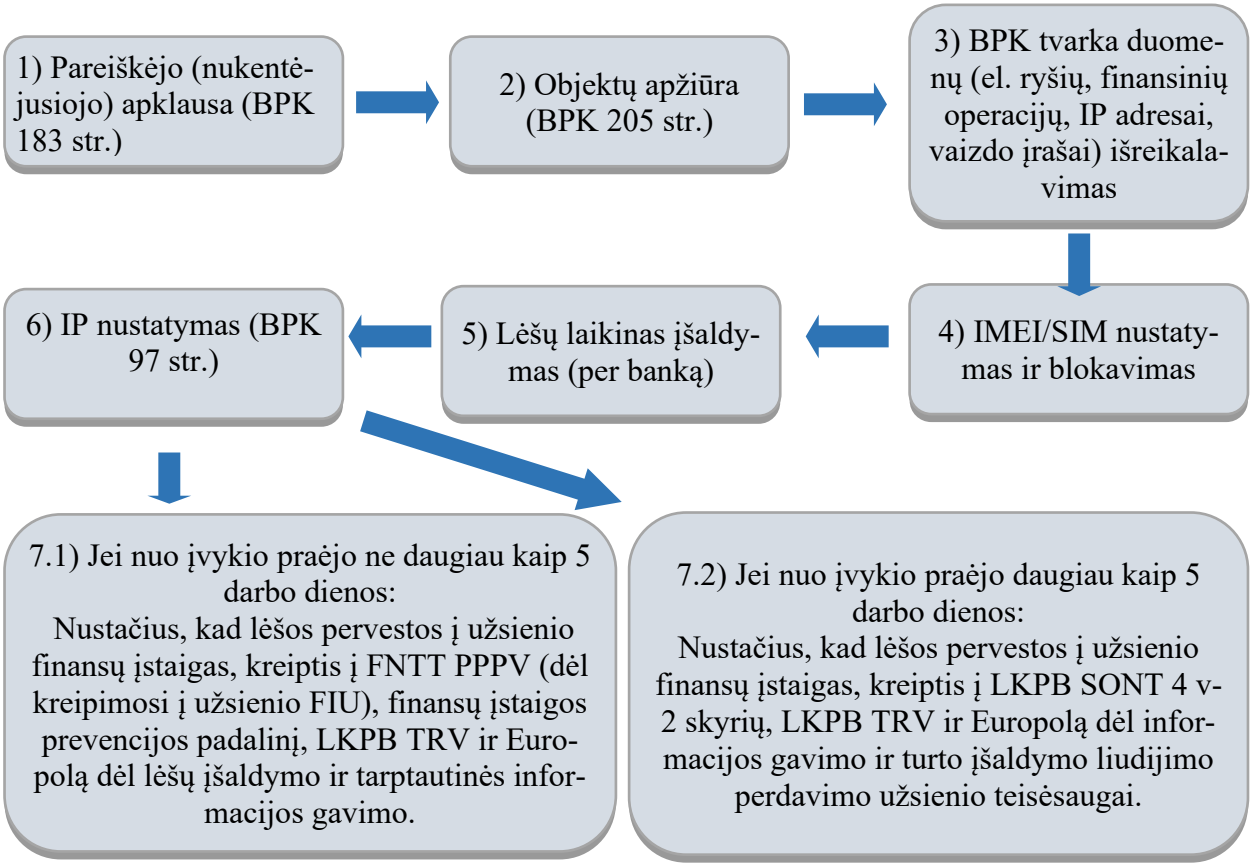
[263] Lietuvos Respublikos generalinio prokuroro Įsakymas „Dėl Rekomendacijų dėl ikiteisminio tyrimo pradžios ir jos registravimo tvarkos patvirtinimo“, 2008 m. rugpjūčio 11 d., Nr. I-110, „Žin.“ 2008, Nr. 94-3713 , https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.325977/asr

[264] Lietuvos Respublikos generalinio prokuroro Įsakymas „Dėl rekomendacijų dėl ikiteisminio tyrimo organizavimo ir vadovavimo jam patvirtinimo“, 2025 m. gegužės 30 d., Nr. I-123, INFOLEX,, https://www.infolex.lt/ta/1039667

[265] Lietuvos Respublikos generalinio prokuroro įsakymas Nr. I-262 „Dėl Lietuvos Respublikos generalinio prokuroro 2014 m. vasario 10 d. įsakymo Nr. I-36 „Dėl metodinių rekomendacijų dėl elektroninėje erdvėje vykdomų sukčiavimų (telefoninio sukčiavimo) tyrimo ir nusikalstamų veikų kvalifikavimo patvirtinimo“ pakeitimo“, Vilnius, 2022 m. rugsėjo 1 d.

atskleidžiama tyrimo specifika ir taktikos ypatumai, pateikiami praktiniai patarimai, kaip teisingai atlikti tam tikrus proceso veiksmus ir greičiau gauti tyrimui reikšmingus duomenis, aptariamos kvalifikavimo problemos.

Sukčiavimas elektroninėje erdvėje savaime reiškia, jog dažniausiai paliekami pėdsakai (įkalčiai) iš esmės nėra materialūs, o virtualūs. Tai reiškia, jog ikiteisminio tyrimo metu susiduriama su virtualiųjų pėdsakų nešiotojais – su įvairiais įrenginiais (kompiuteriai, mobilieji telefonai, kietėji diskai ir kt.), kuriuose gali būti aptikta elektroninių duomenų, taip pat su įvairiose informacinėse sistemose saugomais, tvarkomais, išrenkamais ir interneto pagalba perduodamais duomenimis. Šie elektroniniai duomenys paprastai saugomi tik tam tikrą laiką, juos pakankamai lengva pakeisti, sunaikinti ar kitaip paslėpti, todėl pradėjus ikiteisminį tyrimą būtina nedelsiant atlikti pirminius tyrimo veiksmus ir surinkti kaip įmanoma daugiau duomenų apie nusikaltimo padarymo aplinkybes. Atsižvelgiant į tai, nepriklausomai nuo sukčiavimo elektroninėje erdvėje pobūdžio, vadovaujantis Lietuvos Respublikos generalinio prokuroro metodinėmis rekomendacijomis dėl sukčiavimo elektroninėje erdvėje nusikalstamų veikų kvalifikavimo ir tyrimo, pirminiais atliktinais procesiniais veiksmais laikytini šie:



Lentelė Nr. 6, Pirminiai atliktini veiksmai el. sukčiavimo tyrime, autorius – V. Golovko.

Visų pirma, darbo autoriaus vertinimu, rekomendacijose sukčiavimas elektroninėje erdvėje konceptualiai siejamas su veikų grandine, sudarančia idealiosios sutapties situaciją (su

BK 214, BK 198-1, BK 215, BK 182). Kitaip tariant, sukčiavimas elektroninėje erdvėje čia suprantamas kaip prisijungimo duomenų užvaldymo ir/ar neteisėto prisijungimo ir/ar neteisėtų finansinių operacijų ir tik tuomet galutinio svetimo turto įgijimo derinys. Toks modeliavimas rodo, kad „elektroninė erdvė“ rekomendacijose pirmiausia siejama būtent su šiomis gretutinėmis veikomis (duomenų užvaldymu, įsibrovimu), o ne vien per apgaulės mechaniką BK 182 straipsnio prasme. Todėl tokios situacijos, pavyzdžiui kai nukentėjusysis, telefonu ar internetu apgaulės paveiktas, pats inicijuoja pavedimus ir kai nėra jokių įsibrovimo ar duomenų užvaldymo požymių, pagal rekomendacijų logiką į šį modelį patenka ribotai ir formaliai nebūtinai kvalifikuotinos kaip „sukčiavimas elektroninėje erdvėje“? Juolab kad tokiais atvejais visas apgaulės procesas, t. y. komunikacija, apgaulės poveikis, lėšų pervedimas vyksta virtualioje, skaitmeninėje erdvėje, nors gretutinės veikos, su kuriomis rekomendacijos sieja „elektroninį“ kontekstą, apskritai nepasireiškia.

Taigi, detaliau apžvelgiant minėtas rekomendacijas, matyti, jog sukčiavimo elektroninėje erdvėje pirminiai procesiniai veiksmai, iš esmės taip pat siejami su aukščiau minėtoms „gretutinėms veikoms“. Rekomendacijose akcentuojama, jog pirmiausia rekomenduojama išsamiai apklausti nukentėjusįjį, siekiant nustatyti, kokiu būdu buvo užvaldyti prisijungimo duomenys, kokiais kontaktiniais kanalais bendrauta, kokiu metu tai vyko ir iš jo gauti finansų įstaigos sąskaitų išrašus arba sutikimą juos išreikalauti. BPK 205 straipsnyje nustatyta tvarka atliekama nukentėjusiojo naudojamų įrenginių apžiūra, fiksuojant telefono atmintyje ar kitame įrenginyje esančius duomenis apie kontaktus, bendravimą, prisijungimus prie elektroninių platformų, taip pat nustatant galimai įdiegtą programinę įrangą ar kenkimo priemones. BPK nustatyta tvarka iš elektroninių ryšių paslaugų teikėjų išreikalaujami duomenys apie telefono ryšio sujungimus, veikimo zonas ir kitą ryšio informaciją, atliktina IMSI/IMEI analizė. Iš finansų įstaigų išreikalaujami duomenys apie lėšų judėjimą nukentėjusiojo ir gavėjų sąskaitose, IP adresai, iš kurių jungtasi prie paskyrų ar inicijuotos finansinės operacijos. Taip pat iš interneto paslaugų teikėjų nustatoma, kam priklauso konkrečiam tyrimui reikšmingi IP adresai, vadovaujantis BPK 97 straipsniu ir Lietuvos policijos informacinių sistemų naudojimo tvarka. Nustačius, kad finansinės lėšos pervestos į užsienio finansų įstaigas, veiksmai atliekami atsižvelgiant į tai, kiek laiko praėjo nuo pervedimo. Jei praėjo ne daugiau kaip 5 darbo dienos, kreipiamasi į FNTT Pinigų plovimo prevencijos valdybą dėl kreipimosi į užsienio finansinės žvalgybos padalinį, taip pat į finansų įstaigos prevencijos padalinį, Lietuvos kriminalinės policijos biuro Tarptautinių ryšių valdybą ir Europolą dėl lėšų įšaldymo. Jei praėjo daugiau kaip 5 darbo dienos, kreipiamasi į Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo tyrimo 4-osios valdybos 2-ąjį skyrių, o taip pat į Tarptautinių ryšių valdybą ir Europolą dėl informacijos gavimo ir turto įšaldymo liudijimo perdavimo užsienio teisėsaugai.

Tyrimo veiksmų apimtis ir eiliškumas gali skirtis priklausomai nuo konkrečių bylos aplinkybių.

Analizuojant metodinėse rekomendacijose nurodytus pirminius procesinius veiksmus dėl sukčiavimo elektroninėje erdvėje, matyti, jog veiksmų sąrašas, darbo autoriaus vertinimu, yra universalaus pobūdžio ir yra pritaikytas visiems sukčiavimo elektroninėje erdvėje atvejams. Iš esmės jis neindividualizuoja atliktinų veiksmų pagal konkrečius sukčiavimo būdus (pvz. atskiri procesiniai veiksmai tiriant fišingo el. paštu, smišingo SMS, farmingo, investicinio sukčiavimo atvejus ir t.t.). Dėl šios priežasties tyrėjas kiekvienu konkrečiu atveju turi atrinkti tikslingus procesinius veiksmus pagal bylos aplinkybes ir konkretų sukčiavimo būdą, o ne mechaniškai taikyti visą rekomendacijose pateiktą veiksmų sąrašą.

Šios metodinės rekomendacijos yra pakankamai naudingas praktinis įrankis tiriant sukčiavimą elektroninėje erdvėje, tačiau jose fragmentiškai realizuojami atskiri kriminalistinės charakteristikos elementai, nesudarant vientiso pažintinio modelio. Rekomendacijose daugiausia dėmesio skiriama procesiniams aspektams – tyrimo organizavimui, duomenų rinkimo tvarkai, institucijų sąveikai ir kvalifikavimo niuansams. Tuo tarpu kriminalistinė charakteristika apima platesnį pažintinį lygmenį bei leidžia suprasti nusikalstamos veikos būdą kaip visumą. Be to, ji leidžia ne tik apibrėžti, kaip rinkti duomenis, bet ir kokius duomenis rinkti, kodėl jie svarbūs ir kaip jie siejasi tarpusavyje. Kitaip tariant, metodinės rekomendacijos reglamentuoja tyrimo veiksmų atlikimą, o kriminalistinė charakteristika tyrimo „mąstymą“. Dėl to, darbo autoriaus vertinimu, esamos metodinės rekomendacijos tik iš dalies realizuoja kriminalistinės charakteristikos turinį, tačiau jo neapima visiškai. Pavyzdžiui, jose detaliai apibrėžiami elektroninių duomenų šaltiniai ir tyrimo seka, tačiau trūksta sisteminio požiūrio, tipinių sukčiavimo būdų mechanizmų aprašymo, pėdsakų susidarymo ypatumų analizės, kurie kriminalistikos požiūriu yra būtini siekiant kurti tipines tyrimo versijas, nusibrėžti atliktinų veiksmų vektorių bei įžvelgti tyrimo kliūtis. Papildomai, siekiant atsakyti į klausimą „*kokius duomenis rinkti, kodėl jie svarbūs ir kaip jie siejasi tarpusavyje*“, metodinėse rekomendacijose galėtų būti įtvirtinti tipiniai rizikos indikatoriai, kitaip vadinamieji angl. „red flags“, kurie leistų tyrėjui pradinėje tyrimo stadijoje aptikti tam tikriems sukčiavimo būdams būdingus požymius[266] ir nustačius šių indikatorių atitiktį konkrečiam sukčiavimo modeliui, spręsti dėl konkrečių duomenų išreikalavimo apimties ir krypties. Supratimui, kokius duomenis rinkti ir kaip juos vertinti, sustiprintų trumpas specifinių sąvokų žodynėlis prie kiekvieno sukčiavimo būdo (pvz. kas yra domenas, slapukai, moneta, žetonas ir pan.), kuriame būtų aiškiai apibrėžta, kokius duomenis tokie terminai apima ir kokia jų reikšmė tyrimui.

[266] Pinigų plovimo prevencijos kompetencijų centras. „AML mokymai: Red Flags.“ *AMLcenter.lt,* žiūrėta 2025 m. gruodžio 17 d., https://amlcenter.lt/wp-content/uploads/2025/10/AML-mokymai-red-flags.pdf

Be to, kaip pažymėta rekomendacijose, jog *elektroniniai duomenys saugomi tik tam tikrą laiką*, kas suponuoja, jog pirminiai procesiniai veiksmai turi būti atlikinti nedelsiant – tokie kriminalistiniai elementai sudarytų prielaidas ne tik techniniam tyrimo veiksmų atlikimui, bet ir sisteminiam nusikalstamos veikos supratimui, leidžiančiam operatyviau formuluoti tyrimo versijas, nustatyti galimą organizuotumą (pvz., ar veika pavienė, ar organizuotos grupuotės), numatyti galimus tolimesnius nusikaltėlių veiksmus bei, galiausiai, efektyviau planuoti atliktinus procesinius veiksmus.

Reikia pažymėti, kad tokio pobūdžio metodinių rekomendacijų papildymas galėtų būti vertinamas kaip perteklinis ar resursų reikalaujantis. Vis dėlto, darbo autoriaus vertinimu, tokia rekomendacijų modifikacija, preliminariai leistų nustatyti sukčiavimo būdą jau remiantis nukentėjusiojo apklausos metu surinktais duomenis. Apklausos struktūra galėtų būti organizuojama dviem lygmenimis. Pradiniame etape užduodami bendro pobūdžio klausimai, skirti nustatyti kontaktavimo kanalus, nukentėjusiojo atliktus veiksmus ir pagrindines finansinių operacijų aplinkybes. Nustačius, kad šie pirminiai duomenys atitinka konkrečiam sukčiavimo būdui būdingus rizikos indikatorius (angl. red flags), apklausa būtų gilinama taikant konkrečiam sukčiavimo modeliui pritaikytą klausimų bloką. Tokia konstruktyvi ir išsami pareiškėjo (nukentėjusiojo) apklausa, kurioje fiksuojama, kaip vyko kontaktas (pvz., telefoninis skambutis, SMS su nuoroda, elektroninis laiškas ar kt.), kokie buvo paskutiniai aukos atlikti veiksmai (pvz., pavedimo inicijavimas, nuorodos paspaudimas, prisijungimo duomenų suvedimas, programinės įrangos įdiegimas) bei kokios finansinės operacijos įvyko, tyrėjas galėtų preliminariai nustatyti sukčiavimo tipą. Pagal šią „ankstyvą“ klasifikaciją būtų taikomas kiekvienam būdui pritaikytas veiksmų rinkinys – tiek pirminiai ir tolimesni procesiniai veiksmai, tiek kriminalistinės charakteristikos elementai (pvz., viešai prienami duomenų rinkimo šaltiniai, pėdsakų susidarymo mechanizmo klausimai, kaltininko ir aukos portreto kriterijai). Toks apklausos struktūravimas sudarytų sąlygas jau po pirminės apklausos operatyviai inicijuoti tikslinius duomenų ir daiktų-objektų išreikalavimo veiksmus (pvz. banko sąskaitų išrašų, IP adresų, ryšio išklotinių gavimą, naudojamų įrenginių paėmimą) bei užtrinks, kad esminė kriminalistinių požiūriu naudinga informacija būtų fiksuojama nuosekliai, nepriklausomai nuo konkretaus tyrėjo patirties ar specializacijos.

Ši kriminalistinė charakteristika turi būti formuojama bei tobulinama praktiniu lygmeniu remiantis realia ikiteisminio tyrimo praktika, sistemingai fiksuojant, kokie sukčiavimo elektroninėje erdvėje modeliai dažniausiai pasitaiko, kokie tyrimo veiksmai pasirodo esantys efektyviausi, kokiose tyrimo stadijose kyla didžiausių kliūčių, kokios informacijos parprastai trūksta ir kokios priemonės leidžia šiuos trūkumus „kompensuoti“. Toks realios praktikos pagrindu kuriamas kriminalistinės charakteristikos modelis ypač būtų naudingas tarptautinio

bendradarbiavimo kontekste. Naujoviški sukčiavimo modeliai dažnai apima skirtingas jurisdikcijas, t. y. lėšų nukreipimą į užsienio finansų/banko įstaigas, mokėjimų apdorojimą trečiųjų šalių platformose, IP adresu maršrutus per užsienio serverius, kriptovaliutų keityklas ar socialinių tinklų paskyras, administruojamas kitose jurisdikcijose. Todėl, šiuo aspektu būtina sistemingai rinkti tiek statistinius duomenis, tiek kokybinę informaciją apie tai į kokias užsienio valstybes, institucijas ar privačius subjektus dėl kokių duomenų įprastai kreipiamasi, kokie yra vidutiniai atsakymų terminai, kokiomis priežastimis grindžiami atsisakymai teikti duomenis ir kokiais atvejais apskritai negaunamas atsakymas. Tokio tipo informacija leistų ne tik žinoti kokio pobūdžio informacija turi būti renkama konkrečiam sukčiavimo modeliui, bet ir nustatyti subjektus, iš kurių duomenys realiai nėra gaunami (sąlyginis „juodasis sąrašas“) taip išvengiant ekonomiškai ir procesiškai nepagrįstų užklausų bei racionaliau naudojant tarpvalstybinio bendradarbiavimo instrumentus.

Taigi, kriminalistinės charakteristikos elementų integravimas į metodines rekomendacijas suteiktų galimybę tyrimą organizuoti ne vien reaguojant į jau įvykusią nusikalstamą veiką, bet ir iš anksto vertinant tikėtiną veikos scenarijų (prognozavimas)[267], pėdsakų susidarymo vietas, įrankius ir technologijas, kuriomis galėjo būti pasinaudota. Toks sisteminis požiūris ypač aktualus tiriant masinio pobūdžio sukčiavimus, kai panašaus turinio skundai, pareiškimai gaunami iš dešimčių, šimtų ar net tūkstančių nukentėjusiųjų, o nusikalstamos veikos mechanizmas kartojasi cikliškai. Kartu svarbu atkreipti dėmesį į technologinį dinamiškumą, dėl kurio nuolat kinta ir elektroninėje erdvėje naudojamos apgaulės schemos. Dėl šios priežasties kriminalistinės charakteristikos elementai, nepriklausomai nuo to, ar jie būtų plėtojami metodinėse rekomendacijose, ar formuojami kaip atskiras pagalbinis instrumentas – turi būti periodiškai atnaujinamas, koreguojamas atsižvelgiant į naujai aptiktus sukčiavimo būdus, siekiant net tik reaguoti į jau susiformavusius nusikalstamus mechanizmus, bet ir juos aplenkti. Darbo autoriaus vertinimu, tokia kriminalistinės charakteristikos plėtra nėra vien teorinė prielaida, bet praktinė būtinybė. Šiuolaikinis sukčiavimas elektroninėje erdvėje glaudžiai siejasi su pinigų plovimo schemomis, kriptovaliutų ekosistemomis, dirbtinio intelekto priemonių panaudojimu ir kitomis aukštųjų technologijų sritimis. Todėl tokių sukčiavimų tyrimas reikalauja ne tik teisinių žinių, bet ir pakankamo informacinių technologijų raštingumo bei pažangių analitinio mąstymo gebėjimų. Šiuo požiūriu kriminalistinė charakteristika turėtų būti suprantamas kaip kompleksinis instrumentas, kurio turinį pagal savo kompetenciją formuotų ne tik teisėsaugos institucijos, bet ir kiti praktikoje dalyvaujantys subjektai – bankai, elektroninių ryšių paslaugų teikėjai, kibernetinio saugumo, informacinių technologijų specialistai ir pan.

[267] Яблоков, Н. П., ред. 2005. *Криминалистика: учебник*. 3-е изд., перераб. и доп. Москва: Юристъ. 39, 150 p. http://koldin-msu.ru/wp-content/uploads/2015/03/Учебник-классический-2005.pdf

3.2 Ikiteisminio tyrimo eiga: tipinės situacijos, tyrimo kryptys ir kliūtys

Analizuojant 2020-2024 m. Vilniaus apygardos prokuratūros veiklos teritorijoje sustabdytų ikiteisminių tyrimų sąrašą (iš viso 95 ikiteisminiai tyrimai susiję su sukčiavimu elektroninėje erdvėje pagal BK 182 straipsnį arba jų sutaptis pagal 198, 198-1, 198-2, 214, 215 straipsnius), matyti, jog didžioji dalis tyrimų pradėti gavus skundą, pareiškimą ar pranešimą apie nusikalstamą veiką. Visų šių tyrimų eigoje buvo atlikti visi įmanomi procesiniai veiksmai ir išnaudotos visos galimybės nustatyti nusikalstamą veiką padariusį(-ius) asmenį(-is), tačiau asmenys nenustatyti, dėl ko, vadovaujantis BPK 3^1 straipsniu, ikiteisminiai tyrimai buvo sustabdyti.

Žemiau pateikiami keli atrinktų sustabdytų ikiteisminių tyrimų pavyzdžiai, iliustruojantys tipines situacijas, tyrimo krypčių pasirinkimą ir dažniausias kliūtis, susijusias su skirtingomis sukčiavimo realizavimo būdais. Atkreiptinas dėmesys, jog nagrinėjami ikiteisminiai tyrimai gali būti atnaujinti bet kuriuo metu, jeigu paaiškėtų naujos aplinkybės, kadangi apkaltinamųjų nuosprendžių priėmimo senatys nėra suėjusios. Dėl šių priežasčių, siekiant išsaugoti tyrimo konfidencialumą ir nepažeisti tolimesnių procesinių perspektyvų, tam tikros detalės (datos, institucijos, nukentėjusieji ir kiti identifikuojantys duomenys bus pakeisti/paslėpti).

1. *„Lietuvos Policijos komisariate buvo atliekamas ikiteisminis tyrimas pagal BK 182 straipsnio 2 dalį (BK redakcija 2007-07-21 - 2023-05-31) į , dėl 2023-**-** A. L. pareiškimo, kuriame nurodoma, kad 2022 metų *** mėnesį A. L., gim. **** m. socialiniame tinklalapyje „Facebook“, tyrimo metu nenustatytoje grupėje pastebėjo skelbimą, kuriame buvo siūloma investuoti ir užsidirbi pinigų. A. L. skelbimu susidomėjo, paspaudė nuorodą ir užpildė anketą, kad su ja susisiektų dėl investavimo. Tą pačią dieną A. L. paskambino moteris, kuri paaiškino investavimo galimybes, kad investuojama per programėlę, kuri veikia visoje Europoje. Skambinusi moteris paprašė A. L. atsisiųsti „*****“ (įrenginio nuotolinio valdymo programėlę), ko pasėkoje galimai matė A. L. telefono ekraną ir jame atliekamus veiksmus. Ta pati moteris A. L. padėjo į telefoną instaliuoti „*****“ bei „*****“ (investavimo bei kriptovaliutų programėles) ir nurodė, kad investavimo pradžiai reikia atlikti 250 Eur pavedimą į „*****“ (investavimo programėlę), ką A. L. ir atliko. Po to investavimo klausimais A. L. bendravo su asmeniu D. L., kurį moteris pristatė kaip instruktorių, kuris paaiškins, kaip vykdyti investavimą. A. L. bendraujant su D. L. bei po to bendraujant su moterimi vardu A. ir vykdant jų nurodymus dėl investavimo, ji paėmė 15 000 Eur paskolą iš kredito įstaigos „*****“, bei 15 000 Eur iš „*****“, 2000 Eur pasiskolino iš giminaičių ir pinigines lėšas pervedė į „*****“ (investavimo programėlę). A. L. pastebėjo, jog investavimo programėlėje „*****“ ji turėjo užsidirbusi 60 000 Eur, todėl nusprendė juos nusiimti, tačiau tai*

*padaryti galėjo tik įnešant į minėtą programėlę 5 procentus nuo turimos pinigų sumos. A. L. dar kartą pasiskolino 3 000 Eur, kuriuos įnešė į „*****“ (investavimo programėlę), tačiau uždirbtos pinigų sumos atsiimti nepavyko ir D. L. nurodė, jog reikia pabandyti uždirbtus 60 000 Eur nusiimti pervedant mažesnę sumą, o būtent 1 500 Eur. A. L. vėl pasiskolino 1 500 Eur, kuriuos pervedė į „*****“ (investavimo programėlę). Tačiau po 1 500 Eur pervedimo vis tiek uždirbtų 60 000 Eur nusiimti nepavyko. D. L. nurodė, kad reikia dar 2 000 Eur, tačiau A. L. jam paaiškino, kad ji jau neturi iš ko jų pasiskolinti. D. L. jai davė daugiau laiko pinigams surinkti. A. L. turėdama surinkusi 2 000 Eur, juos vėl pervedė į „*****“ (investavimo programėlę). Po 2 000 Eur pervedimo A. L. negalėjo susisiekti su D. L., tačiau tada su ja 2022 metų gruodžio mėnesyje susisiekė asmuo vardu A. U., kuris paaiškino, jog yra iš investavimo kompanijos, kurioje buvo įsidarbinęs D. L. ir paaiškino, kad D. L. apgaudinėjo žmones. A. U. nurodė, jog norint išsiimti savo uždirbtus pinigus, į sąskaitą turi įnešti 2,5 procento nuo norimos nusiimti sumos. A. L. suprato, kad ją bando apgauti ir daugiau jokių veiksmų neatliko. Sukčiavimo būdu A. L. buvo padaryta apie 38 750 Eur turtinė žala.“*

2. *„Lietuvos Policijos komisariate buvo atliekamas ikiteisminis tyrimas pagal nusikalstamų veikų, numatytų BK 182 str. 3 d. ir 198 str. 1 d., požymius, dėl sukčiavimo ir neteisėto elektroninių duomenų perėmimo ir panaudojimo. Tyrimas pradėtas gavus 2020-**-** UAB „*****“ direktoriaus G. R. pareiškimą, kuriame nurodoma apie tai, kad buvo įsilaužta į UAB „*****“ susirašinėjimą su verslo partneriais, 2020-**-** neteisėtai perimti UAB „*****“ elektroniniai duomenys, atsiųsta pakeista sąskaita į kurią UAB „*****“ neva turi pervesti pinigines lėšas, atliktas 49000 Eur pavedimas iš UAB „*****“ banko sąskaitos Nr. LT**********, esančios „*****“ (bankas), į banko sąskaitą, kurios Nr. ES**********, esančią „*****“ (Ispanijos bankas). Iš šios sąskaitos piniginės lėšos buvo perkeltos į kitas sąskaitas, dalis pinigų išgryninta.“*
3. *„Lietuvos Policijos komisariate buvo atliekamas ikiteisminis tyrimas pagal požymius nusikalstamų veikų, numatytų BK 182 str. 2 d., 198-1 str. 1 d., 214 str. 1 d., 215 str. 1 d., dėl to, kad laikotarpiu nuo 2021-10-21 iki 2022-06-03 nukentėjusieji Lietuvos Respublikos piliečiai, tariamai iš Lietuvoje veikiančių bankų į savo mobiliojo ryšio telefonus gaudavo trumpąsias SMS žinutes, apie tai, kad jų paskyros yra užblokuotos, ar neteisėtai nuskaityti pinigai, o norint sąskaitą atblokuoti, ar blokuoti neteisėtus pinigų pervedimus, būtina paspausti žinutėje pateiktą nuorodą. Nukentėjusiesiems paspaudus gautas nuorodas ir suvedus savo elektroninės bankininkystės prisijungimo duomenis, jų piniginės lėšos apgaulės būdu buvo pervedamos į jiems nepažįstamų asmenų Airijos*

*piliečių banko sąskaitas, atidarytas Lietuvos finansinėse įstaigose - UAB „*****“ (absoliuti dauguma), o taip pat UAB „*****“, UAB „*****“. Tokiu būdu nukentėjusieji apgaulės būdu prarado įvairaus dydžio pinigines sumas.“*

Šie 3 pavyzdžiai pateikiami lyginimui ir bendrųjų tendencijų demonstravimui. Tačiau tolimesnėje analizėje detaliau nagrinėjamas trečiasis pateiktas atvejis, kadangi jis apima didžiausią nukentėjusiųjų asmenų skaičių, labiausiai iliustruoja nagrinėjamų sukčiavimo mechanizmų technologinę sudėtingumą ir leidžia išsamiai atskleisti tyrimo kryptis bei kliūtis.

Apibendrinant trečiojo ikiteisminio tyrimo duomenis, matyti, kad tiriami sukčiavimo atvejai yra padaryti elektroninėje erdvėje, melagingai išsiunčiant trumpąsias žinutes, kuriose apsimetama dvejais Lietuvos Respublikoje esančiais bankais. Tokiu būdu apgaule buvo gauti elektroninės bankininkystės prisijungimo duomenys, pakankami neteisėtai vykdyti finansines operacijas. Atsižvelgiant į sukčiavimo mąstą, yra pagrindo manyti, kad tiriamas veikas galėjo padaryti tarpusavyje susiję asmenys. Įvykdytos nusikalstamos veikos pasižymi panašiu padarymo mechanizmu, vykdant pakankamai sudėtingą schemą, naudojant įvairias sąskaitas, kurių savininkai yra Airijos piliečiai, ar asmenys gyvenantys Airijoje, naudojant suklastotus telefonų numerius, IP adresus.

Išanalizavus nukentėjusiesiems siųstas nuorodas bei apibendrinant gautus duomenis, galima išskirti kelis esminius aspektus. Nukentėjusiesiems siųstos nuorodos tekstai yra susiję su bankų pavadinimais, tačiau akivaizdu, kad tai nėra oficialios nuorodos. Dauguma interneto svetainių domenų užregistruota per kompaniją „*pavadinimas*“ arba jos partnerius. Interneto svetainių domenai dažniausiai buvo registruoti naudojant interneto svetainę „*pavadinimas*“, suteikiančią registruotojo privatumo paslaugą. Tai reiškia, kad tikrasis domeno savininkas lieka anonimas. Visi interneto svetainių domenai apžiūrų metu buvo neaktyvūs. Darytina pagrįsta prielaida, kad nuorodos, turinčios bankų pavadinimus, buvo naudojamos fišingo (smišingo) atakoms, siekiant suklaidinti vartotojus, imituojant oficialius bankų puslapius. Domenų registracijos ir privatumo paslaugos buvo teikiamos įmonių, registruotų Malaizijoje ir Singapūre.

Siekiant nustatyti trumpųjų SMS žinučių siuntėjus buvo išanalizuotos nukentėjusiųjų telefono numerių išklotinės, kuriuose matomos įeinančios žinutės tiriamuoju laikotarpiu, kurių siuntėjai: „*banko Nr. 1 pavadinimas didžiosiomis raidėmis*“, „736562“, „Facebook“, „0E3D2A0D5C6A30“, „534542“ „0E3D2A01“ „0E6C0F8BC2E7FB7D“, „*banko Nr. 1 pavadinimas su t a r p a i s*“, „*banko Nr. 1 pavadinimas su . (taškas)*“, „*banko Nr. 1 pavadinimas mažosiomis raidėmis*“, „*banko Nr. 2 pavadinimas*“. Taip pat nustatyta ir tokių atvejų, kuomet telefonų numerių išklotinėse tiriamuoju laikotarpiu nebuvo užfiksuota jokių įeinančių SMS žinučių. Apžiūrų protokoluose nurodyta, jog informacijos turinčios reikšmės tyrimui nenustatyta, taip pat nenustatyti žinučių siuntėjai.

Analizuojant bankų pateiktus duomenis apie IP prisijungimus prie nukentėjusiųjų banko sąskaitų, buvo nustatyta, kad dažnu atveju jie priskirti Lietuvos Respublikoje gyvenantiems asmenis. Pažymėtina, kad tiriant tokio pobūdžio nusikalstamas veikas išryškėjo naudojamos priemonės anonimiškumui užsitikrinti. Prisijungti prie nukentėjusiųjų internetinės bankininkystės, atlikti finansines operacijas ir taip užsitikrinti anonimiškumą naudojami kompiuteriai „zombiai“. Kompiuteris „zombis“ tai kenkėjiška programine įranga paveiktas kompiuteris, kuris trečiųjų asmenų valdomas per pasaulinį interneto tinklą (iš bet kurios pasaulio vietos kur yra interneto ryšys) tokio kompiuterio savininkui net nežinant apie tai. Kompiuteriai „zombiai“ apjungiami į kompiuterių „zombių“ tinklus, vadinamus „botnet“[268]. Tokie tinklai naudojami įvairioms, dažniausiai paskirstyto atsisakymo aptarnauti (DDoS), atakoms vykdyti. TOR ar „DarkNet“ interneto tinkluose už gan nedidelį mokestį (apie 10-50 JAV dolerių) galima įsigyti apie 100 „zombių“ tinklą. Kaip paminėta aukščiau, kompiuteriai „zombiai“ naudojami užsitikrinti anonimiškumą. Tai yra jungiantis prie nukentėjusiojo internetinės bankininkystės per kompiuterį „zombį“ bankas fiksuoja prisijungusio kompiuterio „zombio“ IP adresą bei slapukus (angl. cookies, tai „duomenų rinkinys arba informacija, kurią sukuria svetainė ir įrašo į lankytojo kompiuterį, taip paspartindama arba supaprastindama darbą vėl kreipiantis į tą pačią svetainę[269]“). Jei nusikaltėliai jungiasi per keletą ar keliasdešimt įvairiose šalyse esančių „zombių“, nustatyti pradinį IP (nusikaltėlio) adresą praktiškai nėra galimybės. Be to, tokias nusikalstamas veikas darantys asmenys, kaip taisyklė, prie kompiuterio „zombio“ jungiasi naudodami papildomas anonimiškumą garantuojančias priemones, tokias kaip jau ankščiau minėtas VPN paslaugas, TOR tinklus ir pan.

Tyrimų metu gauta informacija apie IP adresus, iš kurių sukčiai jungiasi prie nukentėjusiųjų interneto banko, rodo kompiuterių „zombių“ savininkų/naudotojų tiesioginę sąsają su padaryta nusikalstama veika, tačiau praktiškai taip niekada nebūna. Tai būtų nelogiška, kadangi nusikaltimą darantis asmuo nors ir siekdamas kuo didesnio anonimiškumo, tokiu atveju jungtųsi iš tikro vartotojo galutinio IP adreso ir taip faktiškai paliktų savo „piršto antspaudą“. Netgi elementarių IT žinių neturintis nusikalsti linkęs asmuo, darydamas nusikalstamą veiką, siekia paslėpti savo tikrąjį IP adresą, naudoja „TOR“ naršyklę, VPN ir kitas IP paslėpimo priemones. Todėl nėra pagrindo manyti, kad sukčių „paliktas“ duomuo (įrodymas) (IP adresas) atves pas nusikaltimą padariusį asmenį. Atsižvelgiant į tai kas išdėstyta, kompiuterių „zombių“ valdytojų (savininkų) nėra pagrindo įtarti padarius tiriamą nusikalstamą veiką. Tai tiesiog menką kompiuterinį raštingumą turintys arba nesirūpinantys savo informacijos saugumu asmenys ar jų

[268] Guzman, T. Luis de. 2010. "Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges." *Catholic University Law Review* 59(2): 529 p., https://scholarship.law.edu/cgi/viewcontent.cgi?article=3201&context=lawreview

[269] „Slapukas.“ *Vikipedija*, žiūrėta 2025 m. gruodžio 17 d., https://lt.wikipedia.org/wiki/Slapukas

(nepilnamečiai) šeimos nariai, kurie nepaiso elementarių saugaus elgesio internete taisyklių, nenaudoja antivirusinės programinės įrangos. Dėl to jų naudojama kompiuterinė įranga yra pažeidžiama ir dažnu atveju, užvaldoma bei įtraukiama į vadinamus „botnet“ tinklus.

Taip pat atsižvelgiant ir į tai, kad sukčiavimų metų jungiantis prie nukentėjusiųjų banko sąskaitų naudojamos visišką anonimiškumą garantuojančios priemonės (paslaugos) bei techniniai sprendimai, darytina pagrįsta išvada, kad netgi ir atlikus visus baudžiamojo proceso kodekse numatytus proceso veiksmus, siekiant surasti ir užfiksuoti duomenis, susijusius su kompiuteriu „zombiu“, nebus gauta tyrimui reikšminga informacija, t. y. nebus nustatytas konkretus asmuo, jungęsis prie nukentėjusiojo interneto banko. Todėl nutarime sustabdyti ikiteisminį tyrimą pagrįstai nurodoma, jog netikslinga ir neracionalu imtis priemonių tokių kompiuterių „zombių“ apžiūrai/tyrimui bei jų savininkų/ naudotojų galimam baudžiamajam persekiojimui.

Ikiteisminio tyrimo metu, siekiant nustatyti nusikalstamas veikas padariusius asmenis, tiriamuoju laikotarpiu buvo išanalizuoti nukentėjusiųjų banko sąskaitų išrašai. Iš apžiūros protokolų matyti, kad nukentėjusiųjų piniginės lėšos buvo pervedamos į skirtingų Airijos Respublikos piliečių ar ten gyvenančių asmenų vardu atidarytas sąskaitas Lietuvoje veikiančiose finansų įstaigose - UAB „*pavadinimas*“ (absoliuti dauguma atvejų), taip pat UAB „*pavadinimas*“ ir UAB „*pavadinimas*“. Pažymėtina, kad Airijos piliečių ar Airijoje reziduojančių asmenų sąskaitos Lietuvos minėtose finansinėse įstaigose buvo atsidaromos be fizinio tokių asmenų dalyvavimo, per nuotolį, atsiunčiant tokių asmenų bei jų dokumentų nuotraukas. Taip pat nėra duomenų, leidžiančių tvirtinti, kad būtent minėti asmenys (sąskaitų savininkai) faktiškai jungėsi prie jų ir valdė tas sąskaitas. Iš minėtų sąskaitų piniginės lėšos dažnu atveju nedelsiant buvo pervedamos į tų pačių piliečių vardu atidarytas sąskaitas kitose Lietuvos finansų įstaigose (UAB „*pavadinimas*“, UAB „*pavadinimas*“) ar į užsienio bankus, o vėliau dalis pinginių lėšų per kriptovaliutų keityklas iškeičiama į kriptovaliutą, o dalis išgryninamos. Galutinių tokių lėšų gavėjų tyrimo metu identifikuoti nepavyko.

Siekiant gauti duomenis apie piniginių lėšų judėjimą bei apklausti asmenis, į kurių sąskaitas buvo pervesti nukentėjusiųjų pinigai, buvo siųsti paklausimai į Lietuvos kriminalinės policijos biuro Tarptautinių ryšių valdybą, buvo parengti ir išsiųsti Europos tyrimo orderiai bei teisinės pagalbos prašymai į užsienio valstybes. Įvertinus gautus duomenis, tarnybiniuose pranešimuose iš esmės nurodoma, kad gauti atsakymai neinformatyvūs, nepadėję nustatyti galutinius lėšų gavėjus bei nusikaltimus vykdžiusius asmenis.

Gavus vieno Airijos piliečio T. T. G., gim. 2002 m. vardu atidarytos banko sąskaitos, į kurią buvo pervestos vieno iš nukentėjusiųjų asmens piniginės lėšos, duomenis, buvo nustatyta, kad pastarasis asmuo laikotarpyje nuo 2022-05-22 11:37 val. iki 2022-05-23 01:11 val., gautas

pinigines lėšas iš savo UAB „*pavadinimas*“ sąskaitos įvairiomis sumomis pervedė į Vokietijos banke „*pavadinimas*“ savo vardu atidarytą sąskaitą. Tyrimo metu buvo parengtas ir išsiųstas Europos tyrimo orderis į Vokietiją. Gautas atsakymas ir atlikta jo apžiūra. Pastaroji sąskaita (Nr. DE**********) priklausė minėtam T. T. G., buvo atidaryta 2020-10-13, uždaryta 2022-06-15 (netrukus nuo tiriamų nusikalstamų veikų padarymo) į šią sąskaitą 2022-05-22 – 2022-05-23 dienomis be pavedimų iš jo sąskaitos UAB „*pavadinimas*“, taip buvo atliekami pavedimai iš kito Airijos piliečio vardu atidarytos sąskaitos Lietuvos finansinėje įstaigoje. Be to, iš šios sąskaitos buvo atliekami pavedimai į kito Airijos piliečio vardu atidarytą sąskaitą taip pat Lietuvos finansinėje įstaigoje, dalis piniginių lėšų išgryninta, dalis pervesta į „*pavadinimas*“ (banko sąskaitą), dalis - į „*pavadinimas*“ (kriptovaliutų birža). Tokiu būdu per minėtą sąskaitą per dvi dienas „perėjo“ apie 6000 eurų, pradinis likutis buvo 18 eurų, pabaigos likuti - 0, 79 eurų. Prie minėtos T. T. G. sąskaitos Vokietijos banke „*pavadinimas*“ (Nr. DE**********) minėtomis dienomis buvo jungiamasi iš IP adresų, Dubline, Airijoje. Pagal Europos tyrimo orderį apklaustas liudytoju T. T. G. nurodė, kad jis UAB „*pavadinimas*“ (Lietuvoje registruota elektroninių pinigų įstaiga) paslaugomis nesinaudoja, niekada nebuvo prisijungęs. 2022 m. jo draugas Samuelis, jam pasakė, kad rado būdą kaip užsidirbti pinigų. Manė, kad tai susiję su kriptovaliutos prekyba. Samuelis jam liepė atsidaryti sąskaitą. Manė, kad tai panašu į „Revolut“, kur galėtų prekiauti. Jis taip pat paprašė atidaryti sąskaitas „*pavadinimas*“ (Airijoje veikianti pašto paslaugų ir finansų bendrovė, tiekianti dabartines sąskaitas), „*pavadinimas*“ (mobili bankininkystė, leidžianti atidaryti sąskaitą internetu mobiliuoju telefonu), „*pavadinimas*“ (kriptovaliutų birža). T. T. G. teigia, kad jam trūko pinigų besimokant kolegijoje ir norėjo jų užsidirbti. Jis susidomėjo, nemanė, kad tai būtų neteisėta. Galvojo, kad atidarys sąskaitas, jose prekiaus ir tada uždirbs pinigų. Jam nebuvo sumokėta už sąskaitų atidarymą. Kai atidarė „*pavadinimas*“ sąskaitą (Lietuvoje registruota elektroninių pinigų įstaiga), visus duomenis perdavė Samueliui. Jis niekada jokių pinigų į šią sąskaitą nepervedė ir nepaėmė. Kai gaudavo kodą iš „*pavadinimas*“ (Lietuvoje registruota elektroninių pinigų įstaiga), perduodavo jį Samueliui. Jis galėjo prisijungti, sąskaitą patikrinti, bet jis retai tai darė. Samuelis žinojo prisijungimo duomenis, jis sakė, kad perdavė visus duomenis kitiems pažįstamiems žmonėms, todėl jie taip pat turi prieigą. T. T. G. teigė, kad nežino kas tie žmonės. Apie tai, kad iš jo vardu atidarytos „*pavadinimas*“ sąskaitos (Lietuvoje registruota elektroninių pinigų įstaiga) Nr. LT********** pinigai buvo pervesti į sąskaitą Nr. DE**********, esančią „*pavadinimas*“ (Vokietijos mobiliojo banko sąskaita), nieko nežino, neturi supratimo. Parašė SMS žinutę Samueliui paklausė, ką šis padarė. Samuelis atsiuntė atsakymus, juose nurodydamas, kad nieko nedarė, niekada nežinojo nieko, jis tiesiog perdavė savo žmogui.

Taip pat buvo nustatyta, kad vieno iš nukentėjusiųjų piniginės lėšos buvo pervestos į

„*pavadinimas*“ (Lietuvoje registruota elektroninių pinigų įstaiga) sąskaitą Nr. LT**********, priklausančią Airijos pilietei L. O. gim. 2001 m.. Siekiant apklausti piniginių lėšų gavėją L. O., parengtas ir išsiųstas teisinės pagalbos prašymas į Airijos Respubliką. Gautoje iš Airijos Respublikos teisinės pagalbos prašymo vykdymo medžiagoje nurodoma, jog būtina patvirtinti L. O. gyvenamąją vietą, nes Airijos institucija negali patvirtinti L. O. gyvenamosios vietos, tai turi būti atlikta Interpolo kanalais. Atsižvelgiant į tai, nutarime sustabdyti ikiteisminį tyrimą pažymėta, jog: „*iš tokio atsakymo akivaizdu, kad vykdantys teisinę pagalbą Airijos pareigūnai nesiekia atlikti prašomų asmenų gyvenamosios vietos paieškos, perkeldami šią pareigą prašančiajai valstybei. Airijos piliečių ar Airijoje reziduojančių asmenų sąskaitos Lietuvos minėtose finansinėse įstaigose buvo atsidaromos be fizinio tokių asmenų dalyvavimo, per nuotolį, atsiunčiant tokių asmenų bei jų dokumentų nuotraukas, taip pat tokiu būdu pateikiant duomenis ir apie tokių asmenų gyvenamąją vietą bei kitus kontaktus (nebūtinai teisingus ar tebegaliojančius).Taip pat iš teisinės pagalbos vykdymo su Airijos Respublika praktikos yra žinoma, kad asmenys, į kurių sąskaitas pervedamos piniginės lėšos, pagal Airijos įstatymus gali būti apklausiami policijos įstaigose tik jiems sutinkant. Kitais atvejais, tokie asmenys turėtų būti apklausiami teisme, kur turi teisę turėti gynėją. Be to, tokios apklausos metu gauti duomenys, tikėtina, nesuteiktų reikšmingų rezultatų, kurie padėtų nustatyti nusikaltimą padariusius asmenis bei piniginių lėšų buvimo vietą, taip pat akivaizdu, kad tokios sąlygotų žymiai didesnius proceso kaštus, o taip pat keltų teisėtumo klausimų dėl tokių asmenų procesinio statuso bei parodymų davimo apie save ir kt*. „

Apibendrinant teisinės pagalbos taikymo šiame ikiteisminiame tyrime racionalumą bei perspektyvas, konstatuotina, kad minėti asmenys, į kurių sąskaitas pervesti nukentėjusiųjų pinigai, akivaizdžiai nėra galutiniai lėšų gavėjai. Tokie asmenys, už atlygį ar be jo, tikėtina, tik atsidaro savo vardu banko sąskaitas, o sąskaitų valdymą perduoda kitiems asmenims, kurie, savo ruožtu, valdo tokias sąskaitas, arba perleidžia jų valdymą tokiems asmenims, kurių banko sąskaitos savininkas nepažįsta. Dėl šių priežasčių, o taip pat atsižvelgiant į nurodytą tokių asmenų apklausų galimybės specifiką, bei į tai, kad nukentėjusiųjų piniginės lėšos buvo užvaldytos ir perkeltos iš tokių asmenų sąskaitų dar tą pačią nusikalstamų veikų padarymo dieną, nutarime sustabdyti ikiteisminį tyrimą konstatuota, jog „*nėra pagrįsta, proporcinga ir racionalu kreiptis į Airijos Respubliką su teisinės pagalbos prašymu dėl tokių asmenų apklausų*.“

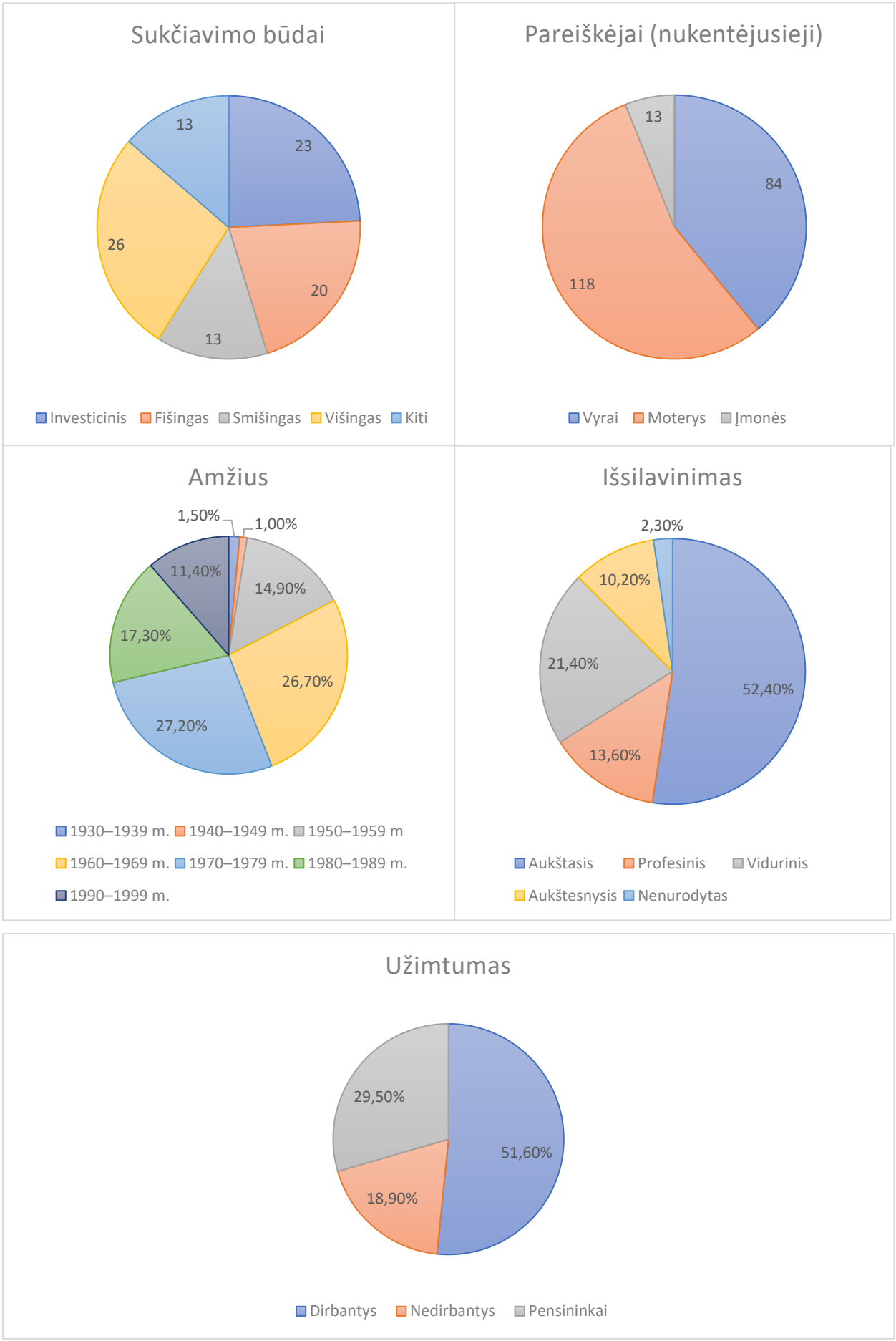
Pažymėtina, kad ikiteisminio tyrimo metu buvo kreiptasi į finansų įstaigas, į kurias buvo pervestos nukentėjusiesiems priklausančios piniginės lėšos, atlikti visi galimi proceso veiksmai, kad nukentėjusiesiems būtų grąžinti pinigai. Piniginės lėšos buvo grąžintos kai tik sąskaitose buvo pakankamas pinigų likutis, tačiau kai kuriais atvejais dėl nepakankamų pinigų likučių sąskaitose grąžinimas buvo neįmanomas. Taigi atsižvelgiant į tyrimo aplinkybes, konstatuota,

kad „*yra atlikti visi būtini ir racionalūs veiksmai, siekiant nustatyti tiriamas nusikalstamas veikas įvykdžiusius asmenis, tačiau tokie asmenys nenustatyti*“. Dėl šių priežasčių, šis ikiteisminis tyrimas buvo sustabdytas.

Analizuojant 2020-2024 m. Vilniaus apygardos prokuratūros veiklos teritorijoje sustabdytus ikiteisminius tyrimus dėl sukčiavimo elektroninėje erdvėje, nepaisant skirtingų sukčiavimo mechanizmų, šių tyrimų eiga iš esmės pasižymi tomis pačiomis tipinėmis situacijomis. Beveik visi ikiteisminiai tyrimai buvo pradėti gavus pareiškimus jau po to, kai piniginės lėšos buvo prarastos. Kai kuriais atvejais, dėka nukentėjusiųjų, ikiteisminio tyrimo įstaigų ir bankų savalaikių veiksmų, aukoms pavyko susigrąžinti prarastas lėšas. Visi sukčiavimo subjektai veikė nuotoliniu būdu, naudodami technologinius įrankius tapatybei maskuoti arba išsidėstė keliuose jurisdikcijose (lėšų pervedimas mažomis sumomis į skirtingas jurisdikcijas), kas įtakojo tyrimų sėkmei. Nepriklausomai nuo konkretaus sukčiavimo scenarijaus, tyrimas paprastai orientuojamas į skaitmeninių pėdsakų, finansinių srautų analizę bei tarpinstitucinio ir tarptautinio bendradarbiavimo galimybių išnaudojimą. Vis dėlto praktika rodo, jog naudojamos anonimiškumą užtikrinančios technologijos, trumpalaikiai skaitmeniniai duomenys, tarpinės banko sąskaitos ir tarpvalstybinis piniginių lėšų judėjimas lemia tai, jog nustatyti galutinius sukčiavimų organizatorius ar kitus bendrininkus dažniausiai nepavyksta. Šiais atvejais tyrimų rezultatyvumą ribojo ne proceso šalių pasyvumas, o technologiniai ir tarptautiniai veiksniai, kurie lėmė tai, kad net ir atlikus visus racionalius bei proporcingus procesinius veiksmus, ikiteisminiai tyrimai turėjo būti sustabdyti, nenustačius konkrečių, nusikalstamas veikas padariusių asmenų.

3.3 Sukčiavimo elektroninėje erdvėje aukos portretas kaip kriminalistinės charakteristikos elementas

Nagrinėjant sustabdytus ikiteisminius tyrimus, buvo atlikta nukentėjusiųjų analizė pagal IBPS esančius charakterizuojančius (demografinius) duomenis, o būtent pagal lytį, amžių, išsilavinimą bei užimtumą:



Diagramos Nr. 2-6, 95 ikiteisminių tyrimų aukų demografiniai duomenys, autorius – V. Golovko.

1. Iš statistinių duomenų matyti, kad dėl investicinio pobūdžio sukčiavimų elektroninėje erdvėje buvo pradėti 23 ikiteisminiai tyrimai, dėl fišingo (siųstu nuorodų el. paštu, įsilaužimo į el. susirašinėjimą įterpiant fišingo turinį, naršymo internete metu) – 20 ikiteisminių tyrimų, dėl smišingo – 13 (SMS su nuorodomis), o dėl višingo (apgaulė telefonu) – 26 ikiteisminiai tyrimai. Dar 13 ikiteisminių tyrimų pradėta dėl kitų sukčiavimo būdų, susijusių su kriptovaliutomis, tinklalapių, serverių ar vidinių ryšių tinklų įsilaužimais ir pan.
2. Vertinant nukentėjusiųjų lytį skirtingų sukčiavimo būdų kontekste, didžiausią nukentėjusiųjų dalį sudaro moterys. Tai ypač ryškų analizuojant smišingo (SMS) atvejus, kuriose iš 113 nustatytų nukentėjusiųjų 67 buvo moterys, o 46 vyrai.
3. Analizuojant pareiškėjų (nukentėjusiųjų) amžiaus duomenis nustatyta, kad vyriausias asmuo gimęs 1934 m., o jauniausias 1999 m. Didžiausia nukentėjusiųjų rodikliai pastebimi dviejuose amžiaus grupėse, t. y. 1960-1969 m. (26,7%) ir 1970-1979 m. (27,2%), kurios bendrai sudaro daugiau nei pusę visų nukentėjusiųjų. Iš šių duomenų matyti, jog 1960-1979 m. intervalas yra labiausiai pažeidžiamas įvairioms sukčiavimo formoms. Kiek mažesnė, tačiau vis vien reikšminga dalis tenka 1980-1989 m. gimimo asmenims (17,3%), o jauniausi, gimę 1990-1999 m. sudaro 11,4%. Taigi šie rodikliai leidžia daryti išvadas, jog tipinėmis sukčių aukomis tampa ne tik vyresnio amžiaus žmonės, bet ir ekonomiškai aktyvūs įvairaus amžiaus asmenys.
4. Vertinant nukentėjusiųjų išsilavinimo duomenis matyti, kad didžiausią dalį sudaro aukštąjį išsilavinimą turintys asmenys – jie apima 52,4%. Tokie rodikliai paneigia stereotipą, kad sukčių aukomis labiau tampa mažiaus išsilavinę asmenys bei rodo, jog išsilavinimo kriterijus nėra papildoma atsparumo priemonė. Antroje pagal dydį grupėje yra vidurinį išsilavinimą turintys nukentėjusieji – 21,4%. Profesinį išsilavinimą turintys asmenys sudaro 13,6%, o aukštesnįjį 10,2%. Tokie duomenys leidžia teigti, kad sukčiavimo elektroninėje erdvėje aukomis iš esmės tampa įvairių socialinių ir išsilavinimo grupių atstovai.
5. Sustabdytų ikiteisminių tyrimų dėl sukčiavimo elektroninėje erdvėje analizė rodo, jog didžiausią nukentėjusiųjų dalį sudaro dirbantis asmenys 51,6%, pensininkai sudaro 29,5% visų nukentėjusiųjų, nedirbantys asmenys 18,9% (tarp jų bedarbiai, studentai, vaiko priežiūros atostogose ar registruoti Užimtumo tarnyboje). Tokių duomenų rezultatai rodo, jog aukomis dažniau tampa ekonomiškai aktyvūs asmenys, turintys nuolatines pajamas.

Analizuojant gautus rodiklius matyti, kad nukentėjusiųjų spektras yra labai įvairūs. Aukomis tampa skirtingo amžiaus, socialinės padėties ir išsilavinimo asmenys. Tokie rezultatai

kelia natūralų klausimą, dėl kokių priežasčių nėra apibrėžto vieno ar kelių tipinių nukentėjusiųjų portretų bei kodėl į sukčių spąstus patenka iš esmės visi. Tam tikro aiškumo šiuo klausimu suteikia mokslininkės Nataljos Revenko įžvalgos[270]. Nagrinėdama tipinį sukčiavimo elektroninėje erdvėje aukos portretą kaip kriminalistinės charakteristikos elementą, ji pažymi, kad dėl tiesioginio vizualinio kontakto tarp aukos ir sukčiaus nebuvimo, šiuo atveju tam tikros aukų asmenybės savybės įgauna ypatingą reikšmę, kurią sukčius išnaudoja savo nusikalstamam sumanymui įgyvendinti. Mokslininkė išskiria dvi pagrindines tokių aukų grupes – „patiklias“ ir „gobšias“ aukas. Kalbant apie pirmąją grupę, N. Revenko praktika rodo, jog paprastai, elektroninėje erdvėje į kontaktą su sukčiumi dažniau linkę eiti asmenys, pasižymintys emocinių jautrumu, patiklumu, polinkiu impulsyviai ir neapgalvotai veikti bei menkas kritiškas požiūris į gaunamą informaciją. Šiai grupei galima priskirti telefoninio, iš dalies tam tikrų investicinio sukčiavimo formų aukas, tam tikrais atvejais net fiktyvių elektroninių parduotuvių, siūlančių neįprastai palankias kainas, aukas. Antroji grupė apibūdinama tokiais bruožais kaip polinkis rizikuoti, siekis greitos ir lengvos finansinės naudos, bei jau minėti bruožai, tokie kaip žemas kritiškas mąstymas bei impulsyvus, neapgalvotas elgesys. Šiam apibūdinimui visa apimtimi priskirtinos investicinio sukčiavimo aukos. Taigi šios N. Revenko įžvalgos dalyje leidžia kriminalistiškai pagrįsti šioje analizėje nustatytą aukų įvairovę pagal išskirtus kriterijus, tačiau, šis vertinimas labiau apima tas apgaulės elektroninėje erdvėje formas, kur tarp aukos ir sukčiaus yra tam tikras, nors ir virtualus sąlytis (žodinis pokalbis, susirašinėjimas), pavyzdžiui – investicinio, romantinio pobūdžio sukčiavimuose, telefoninio (višingo) sukčiavimo atvejais ir pan.

Vertinant sustabdytų ikiteisminių tyrimų statistinius duomenis, matyti, kad telefoninio sukčiavimo aukų amžius aiškiai svyruoja 60-75 m. ribose. Viešai prieinamuose šaltiniuose[271], taip pat galima įžvelgti, jog telefoninio sukčiavimo atvejais, labiau pažeidžiama grupė yra vyresnio amžiaus žmonės. I. Jaroslavcevos ir S. Dorochinos darbe[272] pateikiami tyrimo rezultatai, rodantys, kad vyresnio amžiaus žmonių, tapusių sukčiavimo aukomis, mąstymui būdingas žemas arba vidutinis kritiškumo lygis. Tai lemia jų patiklumo lygį ir nepasirengimą

[270] Н. И. Ревенко, „Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий“, Вестник Омского университета, Серия „Право 21“, № 2, 2024 m., 88 p. https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-moshennichestva-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy

[271] 15min. „Sukčiai skambina ir rašo jūsų tėvams bei seneliams: kaip juos apsaugoti?“ *15min.lt*, 2024 m. Žiūrėta 2025 m. gruodžio 17 d., https://www.15min.lt/verslas/naujiena/finansai/sukciai-skambina-ir-raso-jusu-tevams-bei-seneliams-kaip-juos-apsaugoti-662-2504672

[272] Ярославцева, И. В., и С. А. Дорохина. 2016. „Критическое мышление пожилых людей – жертв мошеннических действий: теоретический и прикладной аспекты исследования.“ *Известия Иркутского государственного университета*. Серия „Психология“. 69, 70 p. https://cyberleninka.ru/article/n/kriticheskoe-myshlenie-pozhilyh-lyudey-zhertv-moshennicheskih-deystviy-teoreticheskiy-i-prikladnoy-aspekty-issledovaniya/viewer

ieškoti atsakymų. Lyginant su jaunais ar vidutinio amžiaus žmonėmis, vyresnio amžiaus asmenims dažniau būdingas situacinis mąstymas. Toks mąstymas charakterizuojamas tuo, jog aukai yra problematiška atskirti pagrindinius ir antraeilius dalykus bei reiškinius, o tai ne visuomet leidžia tinkamai įvertinti situaciją apgaulės metu. Be to pažymima, kad neturintys aukštojo išsilavinimo senjorai yra dar labiau pažeidžiami. Darbo autoriaus nuomone, be individualių asmenybės bruožų ir kaltininko psichologinio spaudimo, svarbų vaidmenį lemia ir socialinė vyresnio amžiaus žmonių padėtis. Dažnai šie asmenys yra arba jaučiasi vieniši, jų bendravimo ratas bei „kiekis“ yra ribotas, o galimybės pasitarti su artimaisiais ar pasitikrinti gautos informacijos patikimumą pokalbio metu yra menkos. Tokios aplinkybės iš esmės padidina aukos pažeidžiamumą ir sustiprina poreikį bendrauti su kitais asmenimis. Tuo tarpu, remiantis sustabdytų tyrimų statistiniais duomenimis, investicinio pobūdžio sukčiavimo atvejais nukentėjusių asmenų amžiaus vidurkis siekia 50-60 metų. Darbo autoriaus vertinimu, toks amžiaus pasiskirstymas iš dalies gali būti siejamas su tuo, kad šio amžiaus žmonės dažnai jau yra sukaupę didesnes santaupas, turi daugiau laisvų lėšų. Be to, domėjimasis investavimo galimybėmis, gali būti siejamas su siekiu sustiprinti finansinę padėtį prieš išeinant į pensiją arba kompensuoti būsimą pajamų sumažėjimą. Dėl ko, šiame gyvenimo etape kylantis finansinis nerimas dėl ateities gali mažinti kritinį požiūrį į patraukliai reklamuojamus „greito uždarbio“ pasiūlymus ir paskatinti prisiimti finansinę riziką.

Kalbant apie sukčiavimo atvejus kai auka ir sukčius neturi tiesioginio kontakto (pvz. apgaulingos nuorodos, fiktyvios svetainės), darbo autoriaus nuomone, aukomis iš esmės gali tapti bet kuris žmogus, kuriam internetas, socialiniai tinklai, el. paslaugos yra kasdienybės dalis. Šiandieninis gyvenimo tempas, informacijos gausa ir skubėjimas lemia, kad sprendimai internete priimami greitai, beveik automatiškai, neįsigilinant į galimas pasekmes – paspaudžiant nuorodą, atidarant svetainę ir atlikus veiksmus joje, nesusimąstant, kas slypi už to veiksmo. Tokie situaciniai veiksniai būdingi fišingo bei jo atmainoms ir farmingo atvejams, kai reikia atnaujinti duomenis, patvirtinti prisijungimą, autorizuotis el. paslaugų svetainėje ir pan. Tuo tarpu, kai fišingo turinyje ar reklamose pateikiami viliojantys pretekstai, kaip laimėjimai loterijose, žemos kainos „naujoje“ el. parduotuvėje, čia reikšmę įgyją N. Revenko minėti aukų bruožai. Be to, turint omenyje, kad tokio pobūdžio veikos vyksta skaitmeninėje aplinkoje, darbo autoriaus vertinimu, vienu reikšmingiausiu veiksnių laikytinas aukos informacinių technologijų raštingumo lygis. Būtent šis kriterijus, kartu su pastabumu, praktiškai yra lemiamas, ar auka sugebės atpažinti įtartinus pranešimus, nuorodas ar svetaines ir atitinkamai įvertinti galimą grėsmę. Šiame kontekste aktuali mokslininkės J. Charinos pozicija, kuri, analizuodama

sukčiavimą informacinių ir telekomunikacijų technologijų srityje[273], vieną iš pagrindinių aukos savybių įvardija pasitikėjimą savo saugumu ir polinkį ignoruoti informacijos saugumo priemones arba nežinojimą apie būtinybę tokias priemones taikyti. Remdamasi D. Šuryginos ir V. Poljakovo įžvalgomis[274], mokslininkė pažymi, kad lengvabūdiškas, neatsargus ar aplaidus požiūris į informacijos saugumą iš nukentėjusiųjų pusės sudaro palankias sąlygas sukčiavimui ir faktiškai tampa vienu iš jo priežasčių. Tačiau esminiu tokių aukų požymių ji laiko tai, jog tokios aukos disponuoja materialinėmis gėrybėmis, prie kurių nusikaltėliai gali gauti prieigą, jiems įveikus atitinkamas programines ir technines apsaugos priemones. Iš šios įžvalgos suprantama, jog sukčiavimo elektroninėje erdvėje aukos portretas neatsiejamas nuo pinigu, t. y. šios veikos dalyko, turėjimo. Taigi tai logiškai pagrindžia, jog sukčiavimo elektroninėje erdvėje auka iš esmės gali tapti kiekvienas asmuo, turintis tokio pobūdžio turtą ir jo valdymui naudojantis informacinėmis technologijomis.

Taigi, dėl didelės ir nuolat kintančios sukčiavimo schemų įvairovės kiekvienas jų orientuojamas į skirtingą pažeidžiamumą ir tikslinę aukų grupę. Dėl to asmuo, gebantis atpažinti ir išvengti vienos apgaulės formos, gali būti pažeidžiamas kito, labiau jo poreikius ar interesų, atitinkančio sukčiavimo modelio. Papildoma vaidmenį viktimizacijos procese, be individualių aukos bruožų, atlieka ir išoriniai veiksniai, pavyzdžiui – vienišumas, materialinė padėtis, sveikatos problemos[275], patirta netektis ir pan. Tokiomis aplinkybėmis net ir kritiškiau informaciją vertinantis asmuo gali tapti labiau pažeidžiamas ir lengviau įtraukiamas į sukčiavimo schemą.

3.4 Sukčiavimo elektroninėje erdvėje kaltininko portretas kaip kriminalistinės charakteristikos elementas

Kiekvieno žmogaus mąstymo būdas iš dalies yra užkoduotas jo genetikoje ir kinta viso gyvenimo eigoje. Asmenybės formavimasis prasideda jau vaikystėje, per tėvų bei jį supančių žmonių elgesio modeliavimą, atsižvelgiant į jų veiksmų moralines ir etnines nuostatas. Teisės pažeidimą iš esmės gali padaryti kiekvienas žmogus, tačiau skirtingas asmenų sąmoningumo

[273] Харина, Елена Алексеевна. 2024. *Особенности методики расследования мошенничества в сфере компьютерной информации*. Диссертация на соискание ученой степени кандидата юридических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования „Красноярский государственный аграрный университет“. 107 p., chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://kubsau.ru/upload/iblock/500/m0oh4gpjtj0xoc5qcwm213n43ghqy23d.pdf

[274] Шурыгина Д. С., Поляков В. В. „Особенности криминалистической характеристики потерпевших по компьютерным преступлениям“ // „Проблемы правовой и технической защиты информации“. 2018 m. 162-166 p., cituota iš ibid, 107, 108 p.

[275] Yang, Y., Hackett, K., Katta, S., Ludwig, R. M., Jarcho, J., Giovannetti, T., Fareri, D. S., & Smith, D. V. (2025). Psychological, social, and health-related factors predict risk for financial exploitation. *Communications Psychology, 3*, Article 88, 12 p., https://www.nature.com/articles/s44271-025-00266-x

lygis lemia skirtingą požiūrį į tuos pačius neteisėto elgesio pareiškimus arba į jų galimybę. Pavyzdžiui, vienas asmuo, įsivaizdavęs galimybę padaryti tam tikrą teisės pažeidimą ar nusikaltimą, remdamasis savo vidiniais moraliniais įsitikinimais, tokį elgesį laikys visiškai nepriimtinu jokiomis aplinkybėmis. Kitas, nors teoriškai ir svarstytų neteisėto veiksmo galimybę, nuo jo susilaikys dėl baimės būti patrauktam atsakomybėn. Trečiasis, kartą padaręs teisės pažeidimą ir sulaukęs tam tikros „bausmės“, tinkamai įvertinęs asmeninę patirtį, gali atsisakyti tokio elgesio ateityje. Tuo tarpu ketvirtasis, priešingai, net ir menkiausios galimybės kontekste, gali imtis neteisėtų veiksmų, parodydamas iniciatyvą ir netgi tam tikrą entuziazmą jų įgyvendinimui.

Nusikaltėlio asmenybė – tai abstrakti sąvoka, reiškianti socialinių ir socialiai svarių, dvasinių, moralinių-valinių, psichofizinių bei intelektinių savybių visumą, kuri formuojasi dėl asmens požiūrių, orientacijų sąveikos su kriminogeniniais išorinės aplinkos veiksniais, įskaitant ir konkrečią kriminalinę situaciją. Šiandien nusikaltėlio asmenybės įtraukimą į kriminalistinės nusikaltimo charakteristikos struktūrą galima laikyti plačiai pripažinta praktika. Tačiau pati „nusikaltėlio asmenybės“ sąvoka nėra vienareikšmė, nes kiekvienas individas išlaiko laisvą valią ir galimybę keistis[276]. Nusikalstamų veikų kriminalistinėje charakteristikoje kaltininko portretas visada užima ypatingą vietą, kaip vienas pagrindinių šios charakteristikos elementų, į kurį nuosekliai dėmesį atkreipia tiek Lietuvos, tiek užsienio kriminalistai. Pasak S. Matulienės, kaltininko portreto, kaip kriminalistinės nusikaltimų charakteristikos elemento turinys yra formuojamas renkant asmenybės požymius, kurie yra specifiniai ir būdingi asmenims, padariusiems konkrečios grupės, rūšies ar porūšio nusikaltimus, svarbius ir esminius, norint sėkmingai atskleisti ir tirti nusikalstamas veikas[277]. Mokslininkės Snieguolė Matulienė ir Lina Novikovienė, analizuodamos nusikaltimų kriminalistinės charakteristikos elementus bei kriminalistikos profilaktinę funkciją, kaltininko portretą siūlo tirti 3 kryptimis:

1. „**Prognostinė kryptis**, numato duomenų apie nežinomo nusikaltėlio asmenybę gavimą pagal paliktus pėdsakus nusikaltimo įvykio vietoje, liudytojų atmintyje ir pagal kitus šaltinius, siekiant nustatyti jo paieškos ir sulaikymo kryptis ir būdus. Dažniausiai tokia informacija leidžia nuspėti tik bendras nežinomų asmenų grupės savybes, tarp kurių galima surasti nusikaltėlį, ir rečiau – kai kurias konkrečias asmenybės savybes. Gauta informacija iš pirmosios tyrimo krypties yra svarbi sudarant kriminalistinę nusikaltimų

[276] Ганиева, Ирада Аллахвердиевна. 2023. „Личность преступника, совершающего дистанционное мошенничество.“ *Актуальные вопросы борьбы с преступлениями 5*. 15 p., https://cyberleninka.ru/article/n/lichnost-prestupnika-sovershayuschego-distantsionnoe-moshennichestvo

[277] Matulienė, Snieguolė. 2004. *Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija*. Daktaro disertacija, Mykolo Romerio universitetas. 88 p.

charakteristiką, kuomet yra nežinomas nusikalstamą veiklą padaręs asmuo, ir pasirenkant tyrimo situacijų būdus ir priemones. Ji yra gaunama iš biologinės kilmės pėdsakų, nusikaltimo būdo bei nusikaltimo situacijos požymių, iš duomenų apie įgūdžius ir specialiąsias žinias, iš manieros, elgesio, kalbos, iš nusikaltimo aplinkos, nusikaltimo pasikėsinimo dalyko ir kitų bylos duomenų. Būtent tokie duomenys ir leidžia daryti išvadas apie asmenų grupę, tarp kurių reikia ieškoti nusikaltėlio, arba apie konkretų nusikaltėlį ir jo asmenines savybes, jo galimą buvimo vietą, pėdsakus, kurie gali būti ant jo kūno bei drabužių ir pan.;

2. **Retrospektyvinė kryptis** – tai įtariamojo asmenybės arba jau žinomo kaltojo asmens analizė, siekiant kriminalistiniu požiūriu įvertinti nusikaltėlio asmenybę. Tokiu atveju tikslinga surinkti informaciją ne tik apie nusikaltėlių vertybinę sistemą, teisinę savimonę, antivisuomeninį požiūrį, gyvenimo būdą, bet ir informaciją apie nusikaltėlio asmenybę, jo ryšius, elgesį, nusikalstamos veikos padarymo metu ir tuoj po jo, padėsiančią užmegzti gerus santykius, kad būtų gauti teisingi parodymai, paneigiant jo melagystes ir kt. Šios rūšies informacija yra svarbi tolesniam konkrečios nusikalstamos veikos kriminalistinei analizei ir sprendžiant iškeltus tyrimo uždavinius. Todėl kriminalistinei nusikalstamų veikų charakteristikai ir nusikalstamų veikų tyrimo metodikai svarbūs duomenys, leidžiantys vertinti rūšinius, tipinius, grupinius ir kitus nusikaltėlio asmenybės požymius, duomenys, liudijantys apie subjektų, darančių skirtingų rūšių nusikalstamas veikas, specifines savybes ir požymius;
3. **Profilaktinė kryptis.** Jos metu renkami, tiriami ir analizuojami duomenys, kuriais naudojantis yra parenkami metodai, būdai ir priemonės, komplikuojančios nusikalstamų veikų padarymą, nutraukiančios asmenų nusikalstamą veiklą arba užtikrinančios palankias sąlygas aptikti ir demaskuoti nusikaltėlį“[278].

S. Matulienės ir L. Novikovienės išskirtos šios trys tyrimo kryptys leidžia sistemiškai pažvelgti į kaltininko portreto analizę ir jos reikšmę nusikalstamos veikos tyrime. Vis dėlto, analizuojant sukčiavimą elektroninėje erdvėje šios kryptys įgyja tam tikrų ypatumų. Dėl specifinių šios veikos bruožų, tokių kaip veikimas virtualioje, neapibrėžtoje erdvėje, dažnas tiesioginio kontakto su auka nebuvimas, įvairių techninių priemonių (pvz., nuorodų, fiktyvių

[278] Snieguolė Matulienė „*Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: Teorinių ir praktinių problemų šiuolaikinė interpretacija*“, Mykolo Romerio universitetas 2004 m., Vilnius. 88, 89 p. // Lina Novikovienė, „Kriminalistikos profilaktinė funkcija: kai kurie teoriniai aspektai,“ Lietuvos teisės universitetas, 2001 m., 183-188 p., cituota iš: Snieguolė Matulienė ir Lina Novikovienė, „Kriminalistinės nusikalstamų veikų charakteristikos ir kriminalistinės profilaktikos vieta šiuolaikinės kriminalistikos koncepcijoje“, Teisės mokslas, Mykolo Romerio universitetas, 2022 m., 94, 95 p., https://cris.mruni.eu/cris/entities/publication/1eab09d3-4b92-40e8-aa22-7729e800ab2e

svetainių, dirbtinio intelekto generuotų vaizdų ir pan.) panaudojimas, kaltininko portreto nustatymas reikalauja ne tik tradicinių, bet ir papildomų vertinimo aspektų. Be technologinio pasirengimo, tokio pobūdžio veikose didelę reikšmę turi ir kaltininko gebėjimas manipuliuoti auka, išnaudoti jos psichologines silpnybes bei susiklosčiusias aplinkybes. Todėl, taikant šias tris tyrimo kryptis praktikoje, būtinas gebėjimas jas interpretuoti lanksčiai, atsižvelgiant į kintančius šiuolaikinių elektroninėje erdvėje esamų nusikaltimų bruožus. Tolesnėje analizėje dėmesys bus sutelkiamas būtent į šio tipo kaltininko portreto formavimo specifiką, remiantis tiek bendrais kriminologiniais aspektais, tiek praktikoje stebimais pokyčiais.

Iš aptarto matyti, jog sukčiavimo elektroninėje erdvėje atveju kaltininko portreto reikšmė ir tyrimo krypties ypatumai dar labiau išryškėja dėl veikimo netradicinėje aplinkoje ir technologinių priemonių vaidmens. Šią kryptingą analizę papildo ir kriminologinis požiūris, jog greta bendro nusikaltėlio portreto, priklausomai nuo konkrečios nusikalstamos veikos krypties, išryškėja ir specifiniai kaltininko bruožai[279]. Vertinant asmenį, kuris sistemingai vykdo sukčiavimus elektroninėje erdvėje, J. Charina vienu iš jo išskirtinių požymių laiko tai, jog kaltininkas dažniausiai nėra pažįstamas su savo auka, o pastarosios asmeninės savybės jam nėra svarbios. Esminiu veiksniu tampa tai, ar auka turi tikslinį turtą, o pagrindiniu tikslu sudaryti galimybę šiam turtui įgyti apgaule. Tačiau, darbo autoriaus vertinimu, tokia mokslininkės pozicija gali būti pagrįsta tik tais atvejais, kai apgaulės mechanizmas nukreiptas į plačią visuomenės dalį, t. y. kai nėra orientuojamasi į konkrečius asmenis (pvz., vykdant fišingo ar smišingo atakas). Tais atvejais, kai aukomis tampa pavieniai, nors ir kaltininkui nepažįstami, bet tikslingai parinkti asmenys, aukos charakteristikos įgyja ganėtinai tvirtą vaidmenį. Tokiais atvejais (pvz., vykdant angl. spear phishing atakas prieš įmonių vadovus ar finansus tvarkančius darbuotojus), informacijos apie auką turėjimas tampa būtina sąlyga nusikalstamos veikos pasiruošimui ir įgyvendinimui. Panaši tendencija pastebima ir telefoninio sukčiavimo atvejais, t. y. kai apgaulė orientuota į neapibrėžtą asmenų ratą (pvz., apsimetant nelaimės ištiktu giminaičiu), aukos individualūs duomenys gali būti mažiau reikšmingi. Tačiau, kai apsimetama banko darbuotoju ar kitos institucijos atstovu, siekiant įtikinti konkretų asmenį perduoti turtą ar prisijungimo duomenis, kaltininkui yra būtina susipažinti su asmens duomenimis, elgsenos ypatumais ar kita informacija.

Analizuojant skirtingus sukčiavimo padarymo būdus elektroninėje erdvėje, darbo autoriaus nuomone, tikslinga išskirti du kaltininko portretų tipus. Pirmasis tipas apima

[279] Харина, Елена Алексеевна. 2024. *Особенности методики расследования мошенничества в сфере компьютерной информации*. Диссертация на соискание ученой степени кандидата юридических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования „Красноярский государственный аграрный университет“. 86 p., https://kubsau.ru/upload/iblock/500/m0oh4gpjtj0xoc5qcwm213n43ghqy23d.pdf

kaltininkus, kurie tiesiogiai arba netiesiogiai (telefoniniai ar vaizdo pokalbiai, susirašinėjimai), pasitelkdami apgaulę, daro poveikį aukai siekdami įgyti turtą. Antrajam tipui priskiriami kaltininkai, kurie neturi jokio kontakto su auka, tačiau pasitelkia specifines apgaulės priemones ir sukuria aplinkybes, dėl kurių pati auka, to nesuvokdama, atlieka veiksmus, lemiančius turto praradimą.

Kaip jau buvo aptarta ankstesniame poskyryje, analizuojant sukčiavimo būdus, kuriems būdingas tiesioginis ar netiesioginis bendravimas tarp aukos ir kaltininko (investiciniai, romantiniai, telefoniniai sukčiavimai), kaltininkai aktyviai naudoja psichologines technikas. Šio pobūdžio nusikalstamų veikų subjektai iš esmės perima dalį klasikiniam sukčiui būdingų bruožų. Tokie subjektai pasižymi psichologiniu lankstumu, pakankamai plačiu akiračiu, išlavintu žodynu, geromis komunikacinėmis kompetencijomis (pavyzdžiui, žiniomis apie bankų klientų aptarnavimo organizavimą), gebėjimu valdyti pokalbį, sužadinti pašnekovo pasitikėjimą ir interesą, paskatinti jį priimti kaltininkui naudingus sprendimus, neretai pasitelkiant manipuliavimą. Kartu pabrėžiama, kad tokie kaltininkai pasižymi ir specifinėmis savybėmis, būdingomis būtent šiam veikų tipui[280]. Papildomai galima pažymėti, jog tokio pobūdžio sukčiai pasižymi atsparumu stresui, išoriškai sukelia pasitikėjimą, yra ryžtingi, drąsūs, linkę rizikuoti, geba išlaikyti šaltakraujiškumą, turi mažą nerimo lygį, sugeba ginti savo interesus ir laisvai elgtis įvairiose situacijose. Jiems būdingas gebėjimas improvizuoti, artistiškumas, greitas sprendimų priėmimas, egoizmas. Tyrimai rodo, kad sukčius į auką žvelgia kaip į negyvybingą objektą, nejaučia empatijos ir net gali patirti emocinį pasitenkinimą, atimdamas iš jos turtą. Jiems taip pat būdingas didelis savo elgesio pateisinimas, pvz. dauguma neigia sąmoningai pasirinkę neteisėtą elgesį, kaltina išorines aplinkybes, bando pateikti savo veiksmus kaip įprastus ar visuotinai paplitusius, o paskirtą bausmę, kaip neteisingą[281]. Sukčiai, visų pirma, siekia sukurti visiško pasitikėjimo atmosferą su potencialia auka, o tik tuomet pereina prie aktyvių apgaulės veiksmų. Neatsitiktinai sukčius kriminalistinėje literatūroje dažnai priskiriamas prie intelektualiai sudėtingesnių nusikaltėlių tipų, kurie puikiai naudojasi žmogiškomis silpnybėmis nusikaltimo tikslais.

Lyties aspektu tokias nusikalstamas veikas dažniau vykdo vyrai – 71,8 %, o 28,2 % – moterys. Vertinant šeimos kaip socialinio veiksnio įtaką, kuri dažnai turi „stabdomąjį“ poveikį

[280] Айвазова, О. В., Г. А. Варданян, и Е. А. Шкуринский. 2022. „Криминалистически значимые особенности субъектов хищений, совершенных с использованием дистанционных технологий.“ *Сибирские уголовно-процессуальные и криминалистические чтения* 2: 44 p., https://cyberleninka.ru/article/n/kriminalisticheski-znachimye-osobennosti-subektov-hischeniy-sovershennyh-s-ispolzovaniem-distantsionnyh-tehnologiy

[281] Ганиева, Ирада Аллахвердиевна. 2023. „Личность преступника, совершающего дистанционное мошенничество.“ *Актуальные вопросы борьбы с преступлениями 5*., 15, 16 p., https://cyberleninka.ru/article/n/lichnost-prestupnika-sovershayuschego-distantsionnoe-moshennichestvo

asmenybei nusikalsti, nustatyta, kad 31,2 % tiriamųjų buvo susituokę, o 14,2 % gyveno partnerystėje. Taigi, 54,6 % asmenų neturėjo šeiminių santykių. Pažymėtina, kad nemaža dalis asmenų, nuteistų už sukčiavimus, naudojant nuotolines technologijas, turėjo įsipareigojimų nepilnamečių vaikų auklėjimui ar senyvo amžiaus tėvų priežiūrai. Analizuojamų asmenų vidiniai poreikiai dažnai nebuvo visiškai realizuoti ir profesinės veiklos srityje. Absoliuti dauguma nuteistųjų neturėjo oficialaus darbo – tokių buvo 41,2 %. Dar 23,1 % vertėsi nekvalifikuotu fiziniu darbu arba atsitiktiniais laikinais uždarbiais. 13,6 % nuotolinių sukčiavimų buvo įvykdyta asmenų, kurių darbas ar kita veikla reikalauja nuolatinio bendravimo su žmonėmis, įskaitant tuos, kurie dėl socialinės pažeidžiamumo ar perdėto pasitikėjimo tampa potencialiomis aukomis. 10,1 % atvejų sukčiavimus įvykdė asmenys, turėję prieigą prie bankų klientų asmens duomenų dėl savo pareigų finansinių paslaugų srityje. Pensininkams priskiriama 5,2 % šių nusikaltimų, o likusiems – 6,8 %. Kalbant apie išsilavinimą, dominuoja asmenys, turintys vidurinį išsilavinimą – tokių buvo 71,2 %[282]. Pažymėtina, kad šis empirinis tyrimas atliktas Rusijos Federacijoje ir pasirinktas apžvalgai neatsitiktinai. Pastarųjų metų praktika Lietuvoje rodo, jog nemaža dalis telefoninio ir investicinio pobūdžio sukčiavimų yra vykdoma asmenų, bendraujančių rusų kalba. Ši aplinkybė vertinama kaip esminė, nes jei tokio pobūdžio sukčiavimus vykdytų Lietuvos Respublikos piliečiai, orientuoti į vietinius gyventojus, natūralu tikėtis, kad būtų bendraujama lietuviškai. Todėl šio tyrimo įžvalgos šiame darbe siejamos pirmiausia su naudojamos kalbos kaip komunikacijos priemonės ypatumais. Atitinkamai tyrimo rezultatai nėra pateikiami kaip teiginiai apie konkrečių kaltininkų pilietybę ar veikimo teritoriją, tačiau bendra rusakalbė komunikacinė terpė leidžia Rusijos Federacijoje gautus duomenis vertinti kaip aktualius analizuojant analogiškas veikas Lietuvos atvejais.

Vertinamas antrasis kaltininko portretas. Šios apgaulės metu kaltininkas neturi jokio kontakto su auka, o pasitelkia specifinę apgaulę (fiktyvios svetainės, nuorodos, apgaulingi laiškai ir pan.), kurios procesas prasideda nuo įrenginių pažeidžiamumu ar duomenų nutekėjimu ir pan. Skirtingai nei aukščiau aptartuose atvejuose, kuriuose kaltininko portrete pagrindu laikyti psichologiniai bei komunikaciniai įgūdžiai, šiuo atveju pagrindinis dėmesys skiriamas techniniam kaltininko pasirengimui, o būtent IT raštingumui ir praktiniams įgūdžiams. J. Charina tokius subjektus išskyrė į 4 grupes:

1. Aukšto lygio specialistai – tam tikra prasme informacinių technologijų srities ekspertai. Šie asmenys pasižymi giliomis ir plačiomis žiniomis savo srityje, kuriai skiria daug

[282] Айвазова, О. В., Г. А. Варданян, и Е. А. Шкуринский. 2022. „Криминалистически значимые особенности субъектов хищений, совершенных с использованием дистанционных технологий.“ *Сибирские уголовно-процессуальные и криминалистические чтения* 2, 45 p., https://cyberleninka.ru/article/n/kriminalisticheski-znachimye-osobennosti-subektov-hischeniy-sovershennyh-s-ispolzovaniem-distantsionnyh-tehnologiy

dėmesio. Jie savarankiškai kuria kompiuterines programas ir dažniausiai palieka itin mažai pėdsakų po nusikalstamos veikos įvykdymo.

2. Patyrę nusikaltėliai informacinių technologijų srityje. Nors jie patys nekuria programinės įrangos, šie asmenys sugeba modifikuoti esamas programas ar techninius įrenginius, pritaikydami juos savo poreikiams.
3. Vidutinio lygio informacinių technologijų žinias turintys asmenys. Jie geba naudotis kompiuterinėmis programomis kaip įgudę vartotojai, tačiau jų nekeičia ir netobulina, kaip tai daro labiau patyrę nusikaltėliai. Tokie asmenys dažniausiai nusikalsta nereguliariai, atsitiktinai, ir jų veiksmai nereikalauja aukšto profesinio pasirengimo.
4. „Buitiniai“ arba „atsitiktiniai“ kompiuteriniai nusikaltėliai. Šiai grupei priklausantys asmenys pasižymi menku, buitiniu kompiuteriniu raštingumu. Nusikalstami veiksmai dažnai kyla iš staiga susiformavusio ketinimo ar aplinkybių, kurioms nereikia specialių žinių ar techninių įgūdžių[283].

Panašią kaltininkų klasifikaciją, tik jau bendrai kibernetinių nusikaltimų kontekste, yra pateikusiosios ir kriminalistės M. Žižina ir D. Zavjalova. Jos išskiria kaltininkus į šias grupes:

- „asmenys, turintys skirtingą informacinių technologijų įgūdžių lygį, tačiau sistemingai nusikalstamas veikas nevykdo;
- asmenys, neturintys išplėtotų informacinių technologijų įgūdžių arba turintys tik vidutinį jų lygį, tačiau vykdantys sistemingą nusikalstamą veiklą, dažnai veikiantys organizuotose nusikalstamose grupuotėse;
- asmenys, pasižymintys aukštu informacinių technologijų įgūdžių lygiu ir sistemingai vykdantys nusikalstamas veikas“[284].

V. Kolominov taip pat siūlo visus sukčiavimo subjektus klasifikuoti atsižvelgiant į jų žinių lygį, gebėjimą valdyti ir naudotis programine įranga bei techniškai sudėtingais įrenginiais, ypač kompiuterine technika. Pirmajai grupei priskiriami profesionalūs sukčiai, vadinamieji „hakeriai“ ar „kompiuteriniai nusikaltėliai“, kurie dažniausiai yra aukštos kvalifikacijos IT specialistai. Paprastai tokie asmenys turi specializuotą išsilavinimą, pasižymi gerai išvystytais techniniais gebėjimais, analitiniu mąstymu bei logika. Tačiau neretai būna uždari, sunkiai bendraujantys realiame gyvenime ir turintys ribotą socialinių ryšių ratą. Jie dirba su jau sukurtais

[283] Харина, Елена Алексеевна. 2024. *Особенности методики расследования мошенничества в сфере компьютерной информации*. Диссертация на соискание ученой степени кандидата юридических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования „Красноярский государственный аграрный университет“. 89-97 p.,

[284] Жижина, Марина Владимировна, и Дарья Владимировна Завьялова. 2022. „Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников).“ *Криминалистика и криминология. Судебная экспертиза* 138 (5):, 154 p., https://cyberleninka.ru/article/n/lichnost-subekta-prestupleniy-v-sfere-kompyuternoy-informatsii-kak-sistemoobrazuyuschiy-element-kriminalisticheskoy-harakteristiki/viewer

programiniais produktais arba patys kuria unikalią, konkrečiai nusikalstamai veiklai pritaikytą programinę įrangą. Antrąją grupę sudaro neprofesionalūs sukčiai, kurie gali turėti IT išsilavinimą arba būti savamoksliai. Šie, savo ruožtu (antroji grupė), skirstomi į pažengusius vartotojus, gebančius kurti paprastas programas ar interneto svetaines ir išmanančius sudėtingesnių techninių įrenginių veikimą, bei į užtikrintus vartotojus, turinčius bendrą supratimą apie kompiuterinių sistemų veikimą ir savarankiškai įdiegiančius programinę įrangą[285]. Mokslininkas taip pat pažymi, jog sukčių profesinės kvalifikacijos lygis turi tiesioginę įtaką pasirenkamų nusikalstamos veiklos metodų bei priemonių sudėtingumui. Tai atskleidžia tiesioginę sąsają tarp kriminalistinės nusikalstamos veikos charakteristikos ir sukčiavimo mechanizmo ypatumų elektroninėje erdvėje.

J. Charina išskiria tam tikrus neigiamus socialinio elgesio išorinius bruožus, būdingus informacinių technologijų srities specialistams, kurie dažniau siejami su asmenimis, turinčiais nusikalstamą polinkį. Nors dauguma šių bruožų, pasak mokslininkės, iš tiesų yra būdingi kibernetiniams nusikaltėliams, vis dėlto kai kurie iš žemiau išvardintų bruožų gali būti būdingi ir kitų nusikalstamoms veikos rūšių subjektams:

- „Paniekinantis požiūris į fizinį darbą, ypač į veiklą, reikalaujančią rimtų fizinių pastangų, taip pat į asmenis, turinčius su tuo susijusias specialybes. Paprastai šie asmenys, patys būdami fiziškai silpnai išsivystę, mano, jog fizinis darbas yra skirtas intelektualiai ribotiems žmonėms;
- Ribotas socialinis ratas, žemas socialinės sąveikos ir adaptacijos lygis, kurį dažniausiai lemia gyvenimo virtualizacija bei realaus bendravimo reikšmės praradimas, kai pirmenybė teikiama skaitmeniniam bendravimui;
- Žemas moralinių principų lygis, abejingumas padarytos žalos pobūdžiui ir mastui, bei visiškas kaltės ar gailesčio nebuvimas;
- Įsitikinimas savo išskirtinumu ir nebaudžiamumu, siekis intelektualinio dominavimo[286]“.

Daugelis kitų mokslininkų siūlo skirtingas kibernetinių nusikaltėlių asmenybės klasifikacijas. Pavyzdžiui, suskirstymas pagal tokius kriterijus kaip kaltininkų patirtis ir įgūdžiai, naudojami techniniai įrenginiai, sukeltų padarinių pavojingumo lygis, motyvai ir tikslai. Tai leidžia daryti prielaidą, kad sukurti vieningą kibernetinių nusikaltėlių klasifikaciją, yra sudėtinga,

[285] Коломинов, Вячеслав Валентинович. 2017. *Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа.* Автореферат диссертации на соискание ученой степени кандидата юридических наук. Иркутск: Байкальский государственный университет. 16, 17 p., https://www.dissercat.com/content/rassledovanie-moshennichestva-v-sfere-kompyuternoi-informatsii-nauchno-teoreticheskaya-osnov

[286] Елена Алексеевна Харина, „Личность типичного преступника, совершившего мошенничество в сфере компьютерной информации“ 2023 m., 54 p., cituota iš Елена Алексеевна Харина, „Особенности методики расследования мошенничества в сфере компьютерной информации“, Красноярский государственный аграрный университет, Красноярск, 2024 m. 86, 87 p.

o gal net neįmanoma. Tai greičiausiai lemia tai, jog kiekvieną dieną atsiranda naujų technologijų, kurios suteikia naujas galimybes tiek eiliniams vartotojams, tiek asmenims, siekiantiems jas panaudoti neteisėtiems tikslams. Ši prielaida leidžia manyti, kad ir asmenys, vykdantys fišingo, farmingo ar kitas specifinės apgaulės formas, iš esmės laikytini kibernetinio sukčiavimo subjektais, todėl jų vertinimas šiame kontekste yra aktualus. Nors iš aptarto kaltininko portreto matyti, kad tokie asmenys ne visada pasižymi aukštu informacinių technologijų išmanymo lygiu, t. y. nelaikytini IT srities specialistais, tačiau jų vykdoma specifinė apgaulė realizuojama būtent per IT įrankius ir skaitmeninę terpę. Dėl šios priežasties jų veikimas pagal pobūdį ir įgyvendinimo mechanizmą, darbo autoriaus vertinimu, atitinka kibernetinių nusikaltimų požymius.

4. SUKČIAVIMO ELEKTRONINĖJE ERDVĖJE TENDENCIJOS IR PAGRINDINĖS PREVENCIJOS KRYPTYS

Remiantis atliktų ekspertų (specializuotų prokurorų) interviu rezultatais, matyti, kad sukčiavimas elektroninėje erdvėje yra iš tiesų apčiuopiama praktinė problema. Specializuotuose prokuratūros padaliniuose tokio pobūdžio ikiteisminiai tyrimai pagrinde sudaro apie pusę visų ikiteisminių tyrimų. Ekspertai pabrėžia, kad šios bylos aiškiai skiriasi nuo „tradicinių“ sukčiavimų, o būtent tuo, kad nukentėjusysis beveik visada nepažįsta kaltininko, tiesioginis kontaktas būna minimalus arba visai jo nebūna, o pačios nusikalstamos veikos turi tarptautinį pobūdį. Ekspertų atsakymuose nuosekliai nurodoma, kad kaltininkai veikia iš užsienio, naudoja užsienio bankų sąskaitas, VPN, kriptovaliutų pinigines, todėl tampa sudėtinga nustatyti tiek nusikaltimo vietą, tiek galutinį lėšų kelią. Tokie sukčiavimo tyrimai, palyginus su kitomis veikomis paprastai trunka ilgiau ir pasižymi mažesniu atskleidžiamumu. Interviu duomenys leidžia daryti išvadą, kad pačios apgaulės schemos ne visada kuriamos iš naujo, tačiau sparčiai tobulėja jų įgyvendinimo mechanizmai. Ekspertai nurodo, kad sukčiavimai vis dažniau vykdomi „pramoniniu būdu“, t. y. pasitelkiant skambučių centrus, realistiškai atrodančias programėles, melagingus prisijungimus (fišingai). Dirbtinis intelektas naudojamas kuriant apgaulingas reklamas, el. laiškus ar skambučius. Taip pat pabrėžiama, kad sukčiavimai tampa vis sunkiau atpažįstami paprastiems vartotojams. Nors žmonės vis plačiau naudoja skaitmenines technologijas, tačiau ne visada geba atskirti patikimą turinį nuo apgaulingų pasiūlymų. Kalbėdami apie dažniausiai pasitaikančius sukčiavimo modelius, ekspertai išskiria telefoninius, investicinius, romantinius bei su kriptovaliutomis susijusius sukčiavimus. Pažymima, kad didžiausią žalą sukelia būtent telefoniniai sukčiavimai, kai aukos įtikinamos „apsisaugoti“ nuo tariamų grėsmių, tačiau iš tiesų pačios tampa sukčiavimo dalyvėmis, t. y. perduoda grynuosius pinigus, banko korteles, jų vardu paimamos paskolos ar net parduodamas turtas. Investiciniai ir romantiniai sukčiavimai dažnai pasižymi ilgesne trukme, todėl pinigų paieška ir jų susigrąžinimas tampa ypač komplikuoti. Ekspertai akcentavo, kad „pasiteisinusios“ schemos dažnai kartojamos, nes nusikaltėliai linkę naudoti tuos modelius, kurie jau buvo sėkmingi. Vertinant nukentėjusiųjų elgesį ir pažeidžiamumą, ekspertų teigimu, dažniau nukenčia vyresnio amžiaus, žemus skaitmeninius įgūdžius turintys asmenys. Taip pat minimas rusakalbių asmenų didesnis pažeidžiamumas bei godumo veiksnys investicinių sukčiavimų atvejais. Tokios įžvalgos, ekspertų nuomone, svarbios planuojant prevencines priemones, kaip švietimo programas, tačiau mažiau naudingos rengiant konkretų tyrimo planą. Vienas iš ekspertų papildomai pabrėžė psichologų vaidmenį analizuojant nukentėjusiųjų elgesį, kartu su teisininkais ir kriminalistais.

Vertinant metodines rekomendacijas dėl elektroninėje erdvėje vykdomo sukčiavimo tyrimų, ekspertai jas apibūdina kaip naudingas pradiniams, neatidėliotiniems veiksmams. Tačiau kartu pažymimas jų ribotumas, t. y. greitai kintančioms ir lengvai modifikuojamoms schemoms sunku pritaikyti vieną universalų tyrimo algoritmą. Iš ekspertų įžvalgų matyti, jog buvo pritartas darbo autoriaus pasiūlymas, dėl detalesnių rekomendacijų pagal atskirus sukčiavimo tipus, su aiškiai apibrėžtais pėdsakų šaltiniais ir veiksmų seka. Taip pat pabrėžiama, kad pirminiai tyrimo veiksmai yra kritiškai svarbūs, kadangi dalis elektroninių duomenų greitai išnyksta, todėl būtina žinoti, ko ieškoti ir ką fiksuoti. Ne kartą interviu atsakymuose išskirta ir technologinių kompetencijų svarba, t. y. trūkstant žinių apie e. bankininkystę, socialinių tinklų veikimą, kriptovaliutas ar ryšio paslaugų tiekėjų saugomus duomenis ir pan., tampa sudėtinga formuluoti tyrimo užduotis ir aptikti elektroninius pėdsakus. Galiausiai, ekspertai išskiria tarptautinio bendradarbiavimo reikšmę. Pasak ekspertų, daugelyje bylų tenka kreiptis į užsienio bankus, platformas, socialinius tinklus ar kitus informacijos valdytojus. Šioje dalyje didžiausia praktinė problema yra ilgi atsakymų terminai. Užsitęsęs teisinės pagalbos procesas apsunkina lėšų paiešką ir mažina galimybes greitai nustatyti kaltininkus. Dėl šių priežasčių, interviu duomenyse greta tyrimo priemonių pabrėžiama ir prevencijos reikšmė, jog yra būtinas finansinių sistemų technologinis tobulinimas, DI įrankių taikymas, duomenų analizė bei „silpnųjų sukčiavimo veiksnių“ nustatymas. Taip pat svarbu nuosekliai stiprinti visuomenės skaitmeninį raštingumą, ypač pažeidžiamiausių grupių atžvilgiu.

Papildomai apklausto IT specialisto įžvalgos leidžia iš technologinės pusės paaiškinti tas sukčiavimo elektroninėje erdvėje tendencijas, kurias praktikoje fiksuoja teisėsaugos pareigūnai. IT specialisto vertinimu, esminis sukčiavimo masto augimas sutapo su COVID-19 pandemijos laikotarpiu, kai žmonės ženkliai daugiau laiko praleido internete ir dažniau naudojosi elektronine prekyba. Pasak specialisto, tuo metu plačiai paplito apgaulės, susijusios su internetiniais skelbimais ir suklastotais internetiniais puslapiais, imituojančiais realias platformas ar bankines sistemas. Taip pat suaktyvėjo fišingo ir smišingo atvejai, kai SMS žinutės ar elektroniniai laiškai buvo pateikiami kaip gauti iš bankų, pašto ar kitų patikimų institucijų. IT specialisto vertinimu, pastaraisiais metais didžiausią įtaką sukčiavimo raidai daro dirbtinio intelekto technologijų plėtra. Dirbtinis intelektas sudaro galimybes ne tik masiškai automatizuoti apgaulingų pranešimų kūrimą, bet ir individualizuoti sukčiavimo metodus, pritaikant juos konkretiems asmenims. Ypač pavojinga laikoma galimybė generuoti netikrus balso įrašus, leidžiančius apsimesti aukų artimaisiais ar pažįstamais, kas iš esmės keičia telefoninio sukčiavimo pobūdį ir dar labiau apsunkina jo atpažinimą. Kalbėdamas apie prevenciją, IT specialistas pabrėžia, kad šiuo metu veiksmingiausios priemonės yra vartotojų informavimas ir technologiniai „filtravimo“ veiksmai, t. y. įtartinų skambučių žymėjimas ar blokavimas, elektroninių laiškų automatinis nukreipimas į

šlamšto aplankus, taip pat bankų ir paslaugų teikėjų siunčiami perspėjimai klientams. Kartu akcentuojama, kad dirbtinis intelektas gali atlikti ir teigiamą vaidmenį, pavyzdžiui analizuodamas vartotojų elgseną, pranešimų turinį ar techninius požymius, jis jau dabar padeda nustatyti galimus sukčiavimo bandymus, atpažinti dirbtiniu intelektu generuotą turinį ar netikras nuorodas. IT specialisto teigimu, papildomą rizikos veiksnį sudaro ir pačių vartotojų elgesys, išskirdamas tokius dalykus kaip – programinės įrangos neatnaujinimas, nepakankamas dėmesys siunčiamų nuorodų ar elektroninio pašto adresų tikrinimui. Tokie veiksmai palieka saugumo spragas, kurios gali būti išnaudojamos nusikalstamai veiklai. Todėl technologinė sukčiavimo prevencija ateityje turėtų būti orientuota į pažangesnių automatizuotų saugumo sprendimų plėtrą bei dirbtinio intelekto taikymą ne tik nusikaltimų aptikimui, bet ir jų užkardymui, kartu nuosekliai didinant visuomenės skaitmeninį raštingumą.

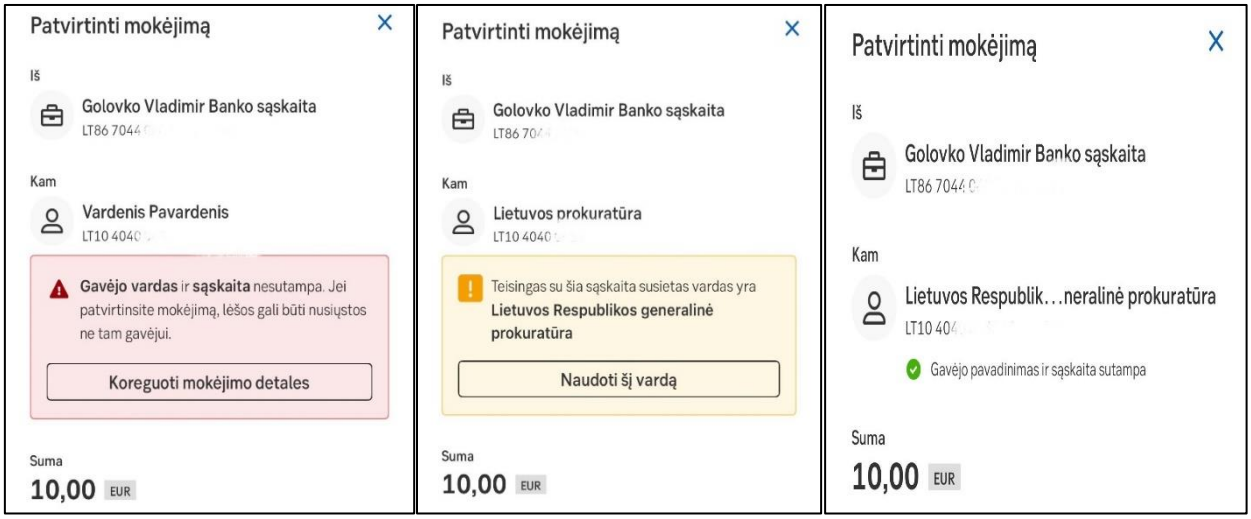
Analizuojant sukčiavimo kriminalistinės charakteristikos pokyčius, šios nusikalstamos veikos integravimą į elektroninę erdvę, interviu išvadas, taip pat statistinius duomenis ir ikiteisminio tyrimo praktiką, akivaizdu, kad toks sukčiavimas tampa vis sudėtingesnis, pasižymintis tarptautinių pobūdžių ir vis dažniau kintantis. Informacinių technologijų raida ne tik išplėtė naujas sukčiavimo galimybes, bet ir iš dalies pakeitė jų veikimo mechanizmą, kaltininkų ir aukų tarpusavio sąveikos pobūdį. Šiuolaikiniai sukčiavimo modeliai vis rečiau pasižymi primityviomis apgaulėmis, kadangi jas keičia kompleksiškos, specifinės formos, kuriose išnaudojamos techninės priemonės, nekalti asmenys bei tarpvalstybinės finansinės įstaigos. Tokie pokyčiai lemia tai, kad paprastam žmogui sudėtinga atskirti rizikingas situacijas, o kartais net apskritai jas aptikti. Tokios aukos vis mažiau siejamos išimtinai su konkrečiomis socialinėmis ar amžiaus grupėmis ir vis labiau priklauso nuo technologinio konteksto, informacinės perkrovos bei momentinių sprendimų priėmimo. Tuo labiau, tradiciniai tyrimo modeliai šiai dienai menkai leidžia operatyviai identifikuoti nusikalstamos veikos subjektus, atsekti galutinį pinigų judėjimą bei užtikrinti efektyvų baudžiamąjį persekiojimą. Dėl šių priežasčių prevencijos klausimai tampa neatsiejama kovos su sukčiavimu elektroninėje erdvėje dalimi ir reikalauja kompleksinio požiūrio, kuris apimtų ne tik teisines priemones, bet ir technologines, organizacines bei švietėjiškas strategijas.

Pirmiausia reikėtų paminėti, kad sukčiavimų problema aiškiai matoma ir valstybės lygmeniu. 2025-03-27 įvyko renginys „Prezidento vienijanti iniciatyva elektroniniams sukčiavimams valstybėje mažinti“, kurio metu buvo pasirašytas memorandumas, prisidėsiantis prie piliečių apsaugos nuo elektroninių sukčiavimų[287]. Jį pasirašė Lietuvos Respublikos

[287] Lietuvos policija. „Pasirašytas memorandumas – reikšmingas žingsnis elektroniniams sukčiavimams valstybėje užkardyti.“ *Policija.lrv.lt*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d.,

generalinė prokuratūra, Lietuvos policija, Nacionalinio kibernetinio saugumo centras, Lietuvos Respublikos ryšių reguliavimo tarnyba, Lietuvos bankas ir Pinigų plovimo prevencijos kompetencijų centras. Šio memorandumo tikslas – užtikrinti veiksmingą institucijų bendradarbiavimą siekiant mažinti sukčiavimo atvejus, keistis informacija realiuoju laiku, stiprinti prevenciją ir mažinti kibernetinių grėsmių riziką. Taip pat siekiama didinti visuomenės informuotumą apie kibernetines grėsmes ir skatinti saugų elgesį internete[288].

Kita prevencijos kryptis – finansų sektoriaus taikomos techninės-prevencinės priemonės, skirtos užkirsti kelią sukčiavimams mokėjimų metu. Nuo 2025-10-09 visoje Europos Sąjungoje įsigaliojo „Momentinių mokėjimų“ reglamento pakeitimai, kurie įpareigoja mokėjimo paslaugų teikėjus prieš atliekant mokėjimą patikrinti, ar mokėjimo nurodyme įrašytas lėšų gavėjo vardas, pavardė ar pavadinimas sutampa su mokėjimo sąskaitos savininku. Ši priemonė skirta apsaugoti mokėtoją tiek nuo sukčiavimo atvejų, kai pateikiamas klaidingas sąskaitos numeris, tiek nuo situacijų, kai pinigai pervedami ne tam adresatui dėl paprastos žmogiškos klaidos. Pradedant mokėjimą elektroninėje bankininkystėje ar mobiliojoje programėlėje mokėtojui parodomas gavėjo tikrinimo rezultatas (neatitikimas arba nepavykęs patikrinimas, dalinis, visiškas atitikimas)[289]. Tokiu būdu sudaroma galimybę įvertinti galimą sukčiavimo riziką ir priimti sprendimą, t. y. tęsti ar nutraukti mokėjimą:



Paveikslai Nr. 5-7, Gavėjo duomenų tikrinimo sistemos pranešimų pavyzdžiai, autorius – V. Golovko.

Tokia prevencinė priemonė stiprina vartotojų apsaugą ir rodo kryptingą finansų sektoriaus vaidmenį užkertant kelią sukčiavimams elektroninėje erdvėje.

---

https://policija.lrv.lt/lt/naujienos/pasirasytas-memorandumas-reiksmingas-zingsnis-elektroniniams-sukciavimams-valstybeje-uzkardyti

[288] Lietuvos Respublikos generalinė prokuratūra. „Sukčiavimui skaitmeninėje erdvėje mažinti – veiksmingas institucijų bendradarbiavimas.“ *Prokuraturos.lt*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d., https://www.prokuraturos.lt/lt/prokuraturos-aktualijos/sukciavimui-skaitmenineje-erdveje-mazinti-veiksmingas-instituciju-bendradarbiavimas/11144

[289] Lietuvos bankas. „Gavėjo tikrinimo paslauga.“ *Lietuvos bankas*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d., https://www.lb.lt/lt/gavejo-tikrinimo-paslauga

Ryšių reguliavimo tarnybos duomenimis, iki 70 proc. visų tarptautinių skambučių gali turėti sukčiavimo požymių. Nuo 2025 m. spalio, mobiliojo ryšio operatoriams pradėjus keistis informacija apie įtartinus numerius, vis dažniau apgaulingi skambučiai sustabdomi dar jiems nepasiekus vartotojų. Vien per kelias savaites blokuojamų skambučių skaičius išaugo nuo 300 tūkst. iki 500 tūkst. per savaitę. Operatoriams suteikta teisė blokuoti, sulaikyti, atsiliepti ar pažymėti, kad skambutis galimai yra apgaulingas. Šios priemonės ženkliai mažina telefoninio sukčiavimo mastą ir apsunkina nusikalstamą veiklą. Ryšių reguliavimo tarnybos duomenimis, 2025 m. lapkričio mėnesį pranešimų apie bandymus sukčiauti sumažėjo beveik perpus. Ryšių reguliavimo tarnybos atstovai pabrėžia, kad technologijos duoda apčiuopiamą rezultatą, tačiau taip pat būtina stiprinti gyventojų budrumą ir skaitmeninius įgūdžius. Ryšių reguliavimo tarnybos metinės diskusijos metu sutarta, jog būtina toliau derinti reguliacines ir technologines priemones, aiškiau reglamentuoti SIM kortelių registravimą ir naudojimą, gerinti duomenų apsikeitimo modelį bei stiprinti techninį ir analitinį bendradarbiavimą su teisėsauga. Pažymėta ir tai, jog glaudus institucijų bendradarbiavimas leido atskleisti ir neutralizuoti profesionaliai įrengtus SIM spiečius – vienoje vietoje aptikta apie 75 tūkst. SIM kortelių iš įvairių šalių. Tai buvo dalis masinės sukčiavimo infrastruktūros, kuri sėkmingai likviduota[290].

Dar viena reikšminga prevencijos kryptis yra griežtesnis kriptoturto paslaugų teikėjų reguliavimas. Finansinių nusikaltimų tyrimo tarnyba nurodo, jog nuo 2026-01-01 Lietuvoje kriptoturto paslaugas galės teikti tik tie subjektai, kurie turės galiojančią kriptoturto paslaugų teikėjo licenciją. Pereinamajam laikotarpiui pasibaigus, licencijos negavusios bendrovės Lietuvoje nebegalės teikti su kriptoturtu susijusių paslaugų. Tokie virtualiųjų valiutų keityklų operatoriai ir depozitinių virtualiųjų valiutų piniginių operatoriai turės priimti sprendimą dėl veiklos keitimo, bendrovės reorganizavimo ar likvidavimo, o neteisėtas vertimasis tokia finansine veikla užtrauks baudžiamąją atsakomybę pagal BK 202 str.[291]. Taigi šie pakeitimai iš esmės skirti mažinti kriptoturto sektoriaus panaudojimą sukčiavimui, pinigų plovimui ir kitoms nusikalstamoms veikoms, taip pat stiprinti finansinių srautų skaidrumą ir institucijų galimybes vykdyti veiksmingą kontrolę. Lietuvos banko duomenimis, šis licencijavimo modelis jau pradedamas taikyti praktikoje ir pirma kriptoturto paslaugų teikėjo licencija išduota bendrovei UAB „Robinhood Europe“. Nuo 2025 m. pavasario ši bendrovė įgijo teisę Lietuvoje ir visoje Europos Sąjungoje teikti kriptoturto saugojimo ir administravimo, pavedimų kriptoturtu

[290] Ryšių reguliavimo tarnyba. „Įjungus naują apsaugą, operatoriai kas savaitę sustabdo apie pusę milijono sukčių skambučių.“ *RRT.lt*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d., https://www.rrt.lt/ijungus-nauja-apsauga-operatoriai-kas-savaite-sustabdo-apie-puse-milijono-sukciu-skambuciu/

[291] Finansinių nusikaltimų tyrimo tarnyba. „Baigiasi pereinamasis laikotarpis VASP: nuo 2026 m. sausio 1 d. privaloma kriptoturto paslaugų teikėjo licencija.“ *FNTT.lrv.lt*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d., https://fntt.lrv.lt/lt/naujienos/baigiasi-pereinamasis-laikotarpis-vasp-nuo-2026-m-sausio-1-d-privaloma-kriptoturto-paslaugu-teikejo-licencija-uww/

vykdymo, pervedimo, priėmimo ir perdavimo paslaugas[292].

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos yra pagrindinė institucija, koordinuojanti kibernetinio saugumo užtikrinimą valstybės mastu. Jis stebi kibernetines grėsmes, koordinuoja reagavimą į incidentus, rengia metodikas ir rekomendacijas organizacijoms, organizuoja pratybas bei teikia įrankius gyventojams ir verslui savo skaitmeniniam saugumui įsivertinti, taip tiesiogiai prisidėdamas prie elektroninių sukčiavimų prevencijos[293]. Kaip prevencinį pavyzdį galima paminėti Nacionalinio kibernetinio saugumo centro organizuojamas socialinės inžinerijos pratybas „Kibernetinis skydas PhishEx“. 2025 m. vykusių pratybų metu išsiųsta beveik 120 tūkst. imitacinių fišingo laiškų daugiau nei šimto organizacijų darbuotojams. Organizacijos gavo apie 5,5 tūkst. pranešimų apie gautus apgaulingus laiškus, o jautrius duomenis pateikė apie 4,9 tūkst. darbuotojų, t. y. pirmą kartą daugiau dalyvių atpažino sukčiavimą, nei juo susiviliojo. Tai rodo, kad nuoseklus švietimas ir praktiniai mokymai gali realiai didinti darbuotojų atsparumą elektroniniam sukčiavimui, nors dalis asmenų vis dar išlieka pažeidžiami[294].

Pažymėtina, kad glaudus nacionalinis tarpinstitucinis bendradarbiavimas leidžia operatyviai užkardyti potencialius sukčiavimus dar jų pasirengimo stadijoje. Pavyzdžiui, Vilniaus apskrities vyriausiajame policijos komisariate atliekamame ikiteisminiame tyrime, pradėtame pagal Lietuvos Respublikos Ryšių reguliavimo tarnybos pranešimą, 2025 m. spalio pradžioje buvo organizuota sulaikymo operacija. Šių operacijų metu įvairiose Vilniaus apskrities vietose atliktos kratos ir sulaikyti du asmenys, galimai prisidėję prie šios nusikalstamos veikos vykdymo. Kratų metu rasta beveik 200 „SIM Box“ („įrenginys, kuris naudoja didelį kiekį SIM kortelių tam, kad galėtų nukreipti ar priimti telefono skambučius bei tekstinius pranešimus“[295]), apie 100 kompiuterių, taip pat apie 75 000 įvairių šalių operatorių SIM kortelių[296].

Tarpinstitucinis bendradarbiavimas aktualus ir tarptautiniu mastu. 2025 m. gruodį, kaip nurodoma Lietuvos Respublikos prokuratūros pranešime: „Lietuvos, Čekijos, Latvijos, ir Ukrainos prokuratūrų ir ikiteisminio tyrimo įstaigų atstovai, koordinuojant Eurojustui, išardė organizuotą nusikalstamą tinklą, valdžiusį skambučių centrus Dnipre, Ivano Frankivske ir

---

[292] Lietuvos bankas. „Lietuvos bankas išdavė pirmąją kriptoturto paslaugų teikėjo licenciją.“ *Lietuvos bankas*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d., https://www.lb.lt/lt/naujienos/lietuvos-bankas-isdave-pirmaja-kriptoturto-paslaugu-teikejo-licencija

[293] Nacionalinis kibernetinio saugumo centras. „Veikla.“ *NKSC.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.nksc.lt/veikla.html

[294] LRT. „NKSC per pratybas pirmą kartą fiksavo didesnį e. sukčiavimą supratusių asmenų skaičių.“ *LRT.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.lrt.lt/naujienos/lietuvoje/2/2592135/nksc-per-pratybas-pirma-karta-fiksavo-didesni-e-sukciavima-supratusiu-asmenu-skaiciu?srsltid=AfmBOorTr8GedfASHlE9Ipd-s-RDEctvEWusMle1oygvSzzeLwocFEVZ

[295] Lietuvos policija. „Vilniaus kriminalistų operacija: smogta „SIM box“ tinklui (vaizdo įrašas).“ *Policija.lrv.lt,* žiūrėta 2025 m. gruodžio 17 d https://policija.lrv.lt/lt/naujienos/vilniaus-kriminalistu-operacija-smogta-sim-box-tinklui-video- %200hu5/

[296] Ibid.

Kyjive, Ukraina, kurio nariai, įtariama, apgaudinėjo asmenis Europos šalyse, tarp jų ir Lietuvoje“. Pranešime taip pat nurodoma, kad tarptautinės operacijos metu Ukrainoje buvo atlikta daugiau kaip 70 kratų, išardyta telefoniniam sukčiavimui pritaikyta infrastruktūra, paimta virš 300 kompiuterių, daugiau nei 300 mobiliųjų telefonų, keli serveriai ir dideli kiekiai informacijos laikmenų. Turimais duomenimis, nuo šios nusikalstamos grupuotės nukentėjo daugiau kaip 400 asmenų, bendra padaryta žala viršija 10 mln. eurų[297].

Akcentuotina ir tai, kad nacionalinės ir Europos Sąjungos kompetentingos institucijos, tokios kaip Generalinė prokuratūra, Finansinių nusikaltimų tyrimo tarnyba, Lietuvos bankas, Europos Sąjungos teisėsaugos mokymo agentūra (CEPOL) ir daugelis kitų organizuoja bei koordinuoja kvalifikacijos kėlimo veiklas, skirtas teisėsaugos pareigūnų kompetencijoms sukčiavimų elektroninėje erdvėje, finansinių nusikaltimų ir kibernetinių grėsmių srityse stiprinti. Teisėsaugos institucijos, lygiai taip pat kaip ir finansų sektoriaus bei kiti šioje srityje veikiantys subjektai, nuosekliai plečia savo žinias ir praktinius gebėjimus, siekdamos prisitaikyti prie kintančių sukčiavimo formų. Šios veiklos apima tiek mokymus ir seminarus, tiek tarpinstitucinio bendradarbiavimo iniciatyvas, orientuotas į šiuolaikinių sukčiavimo schemų atpažinimą, elektroninių įrodymų rinkimą ir analizę, taip pat tarptautinio bendradarbiavimo mechanizmų taikymą praktikoje. Be to, prie prevencijos prisideda ir žiniasklaida, naujienų portalai, radijas, socialinių tinklų grupės, kurie nuolat dalijasi su visuomene informacija apie paplitusius sukčiavimus, realių nukentėjusiųjų istorijas ir praktinius patarimus, kaip išvengti apgaulių.

Darbo autoriaus vertinimu, šiandien galima konstatuoti, kad prevencijos ir švietimo priemonių spektras yra itin platus. Jis apima, pagrįstai galima teigti, visas grandis – nuo visuomenės ir potencialių aukų švietimo, teisėsaugos institucijų kompetencijų bei bendradarbiavimo stiprinimo iki nacionalinės ir Europos Sąjungos lygmens sprendimų, kuriais siekiama užkardyti tokio pobūdžio sukčiavimus. Tačiau kartu išlieka klausimas, ar tokios priemonės yra pakankamos, jeigu elektroninio sukčiavimo aukos vis dar nuolat atsiranda. Viena vertus, galima manyti, kad tai laiko ir sistemingo darbo klausimas, kol tokios priemonės duos labiau apčiuopiamus rezultatus. Kartu praktika rodo, kad tiek nacionalinių, tiek tarpvalstybinių institucijų glaudi tarpusavio sąveika ir koordinuoti veiksmai, gali duoti konkretų rezultatą – nustatomi ir sustabdomi organizuoti sukčiavimo tinklai bei užkardomi potencialūs sukčiavimo atvejai pasirengimo stadijoje. Kita vertus, akivaizdu, jog kol teisėsauga, finansų sektorius ir visuomenė mokosi atpažinti esamas apgaulės formas, sukčiai paraleliai kuria naujas, dar sudėtingesnes versijas. Todėl kova su sukčiavimu elektroninėje erdvėje neišvengiamai įgyja

[297] Lietuvos Respublikos prokuratūra. „Lietuvos prokurorai padėjo išardyti telefoninių sukčių tinklą Ukrainoje.“ *Prokuraturos.lt*, žiūrėta 2025 m. gruodžio 17 d., https://prokuraturos.lt/lt/lietuvos-prokurorai-padejo-isardyti-telefoniniu-sukciu-tinkla-ukrainoje/11892

nuolatinės „lenktynių“ su nusikalstamomis inovacijomis formą, o pagrindiniu sėkmės veiksniu tampa gebėjimas laiku prisitaikyti, lanksčiai taikyti kriminalistinius ir technologinius įrankius bei išlaikyti kritišką požiūrį į sparčiai besikeičiančią skaitmeninę aplinką.

IŠVADOS IR PASIŪLYMAI

1. Išnagrinėjus kriminalistikos ir sukčiavimo tyrimo metodikų istorinę raidą, matyti, kad iki XIX a. nusikalstamų veikų tyrimas buvo grindžiamas praktine patirtimi, neturint sistemingo mokslinio pagrindo. Kriminalistikos, kaip savarankiško mokslo, susiformavimas XIX a. pabaigoje sudarė prielaidas kurti nuoseklias tyrimo metodikas. Šiuolaikiniame kontekste istoriškai susiformavęs sukčiavimo priskyrimas vien „nusikaltimams nuosavybei“, nebeatitinka elektroninėje erdvėje vykdomo sukčiavimo pobūdžio, nes technologinė raida iš esmės dalyje pakeitė tiek sukčiavimo mechanizmą, tiek paliekamų pėdsakų vietovę bei jų pobūdį. Dėl šių pokyčių sukčiavimo tyrimas šiuolaikinėje praktikoje nebegali būti atliekamas vien tradiciniais sukčiavimo tyrimo kriminalistikos instrumentais ir turi apimti ir kitų kriminalistikos sričių metodikas;
2. Įvertinus šiuolaikinio sukčiavimo elektroninėje erdvėje baudžiamąją teisinę ir kriminalistinę charakteristiką, nustatyta, kad sukčiavimo sudėties požymiai ir kriminalistinės charakteristikos elementai yra tarpusavyje glaudžiai susiję ir praktikoje veikia kaip vientisa sistema. Baudžiamosios teisės normos apibrėžia veikos kvalifikavimo ribas, tačiau kriminalistinė charakteristika leidžia atskleisti realų apgaulės mechanizmą, pėdsakų susidarymo / slėpimo ypatumus, veikos pasiruošimo / įgyvendinimo / baigiamųjų veiksmų eigą, potencialių aukų bei kaltininkų portretus. Dėl to sukčiavimo elektroninėje erdvėje kvalifikavimas ir tyrimas, neatsižvelgiant į kriminalistinę analizę, tampa nepakankamai išsamus, ypač tais atvejais, kai apgaulė derinama su kitomis nusikalstamomis veikomis;
3. Ištyrus naujausias sukčiavimo elektroninėje erdvėje schemas, matyti, kad technologinė pažanga iš esmės pakeitė sukčiavimo padarymo būdus ir jų specifiką. Šiuolaikiniai sukčiavimo modeliai pasižymi didesniu organizuotumu, anonimiškumu bei galimybe daryti nuotolinį poveikį nukentėjusiajam net ir neturint tarpusavyje kontakto. Dėl to tradicinės sukčiavimo formos, kartu su IT technologijomis keičiasi į sudėtingas, technologiškai pažangias schemas, kurios reikalauja platesnio kriminalistinio vertinimo nei klasikiniai apgaulės modeliai;
4. Išanalizavus sukčiavimo elektroninėje erdvėje ikiteisminių tyrimų praktiką, nustatyta, kad tokie tyrimai pagrinde pradedami gavus nukentėjusiųjų pareiškimus jau po lėšų praradimo. Tokių tyrimų sėkmė labiausiai priklauso nuo operatyvaus skaitmeninių duomenų fiksavimo ir finansinių srautų atsekimo, bei, be abejo, aukos savalaikio reagavimo. Tipiškai tyrimas orientuojamas į virtualių pėdsakų surinkimą, tarpininkaujančių sąskaitų nustatymą ir tarptautinio bendradarbiavimo instrumentų

taikymą. Praktikoje dažniausiai pasitaikančios kliūtys siejamos su kaltininkių tapatybės maskavimo priemonių naudojimu, tarpinių sąskaitų, greitu lėšų „išskaidymu“ per skirtingas valstybes (jurisdikcijas) bei ilgi duomenų gavimo terminai iš užsienio subjektų, dėl ko galutinių kaltininkų tapatybės nustatymas tampa nepasiekiamas net atlikus visus racionalius procesinius veiksmus. Siekiant tobulinti tokių veikų tyrimą, tikslinga taikyti aiškius neatidėliotinų veiksmų algoritmus pagal atskirus sukčiavimo modelius, nustatyti duomenų rinkimo sąrašus ir nuosekliai stiprinti technologines kompetencijas bei operatyvų institucijų ir privataus sektoriaus apsikeitimą informacija;

5. Išnagrinėjus sukčiavimo elektroninėje erdvėje plėtros tendencijas nustatyta, kad šios apgaulės tampa masiškesnės ir vis sunkiau atpažįstamos, nes sukčiavimo subjektai greitai adaptuojasi prie šiuolaikinių technologijų. Prevencijos priemonės šiuo metu formuojasi iš esmės visomis kryptimis. Įvertinus šių prevencinių priemonių sąveiką su kintančiais sukčiavimo modeliais, matyti, kad jos gali duoti apčiuopiamą efektą, tačiau jų veiksmingumas priklauso nuo greito prisitaikymo prie naujų sukčiavimo schemų, realaus duomenų apsikeitimo bei taikomų techninių priemonių nuolatinio tobulinimo. Todėl sukčiavimo elektroninėje erdvėje prevencija praktikoje turi būti organizuojama tuo pačiu principu, kaip ir šiame darbe aptarta sukčiavimo formų adaptacija prie technologijų, t. y. kaip nuolatinis ir dinamiškas procesas, kuriame teisinio reguliavimo, technologinės ir švietėjiškos priemonės taikomos koordinuotai, prevenciją orientuojant ne vien į reagavimą į jau paplitusias schemas, bet ir į jų ankstyvą užkardymą.
6. Darbo autoriaus vertinimu, tikslinga tobulinti galiojančias metodines rekomendacijas dėl sukčiavimo elektroninėje erdvėje tyrimo, integruojant į jas sisteminius kriminalistinės charakteristikos elementus. Rekomendacijose siūlytina neapsiriboti universaliu procesinių veiksmų sąrašu, bet atskirti tyrimo eigą pagal konkrečius sukčiavimo būdus, aiškiai apibrėžiant jiems būdingus veikos mechanizmus, pėdsakų susidarymo ypatumus, rizikos indikatorius (angl. red flags) ir tipines tyrimo kliūtis. Tokios metodinės rekomendacijos sudarytų galimybes jau pirminėje tyrimo stadijoje preliminariai nustatyti sukčiavimo modelį (turint omenyje, jog sukčiavimo subjektai yra linkę pakartotinai naudoti „sėkmingas“ apgaulės schemas), tikslingai pasirinkti atliktinų pirminių procesinių veiksmų apimtį ir kryptį bei greičiau numatyti tolimesnius procesinius veiksmus. Tai leistų ne tik tirti „karštais pėdsakais“, bet ir racionaliau naudoti procesinius ir tarptautinio bendradarbiavimo resursus. Atitinkamai, tai padidintų ikiteisminių tyrimų efektyvumą masinio pobūdžio ir technologiškai sudėtinguose sukčiavimo atvejuose.
7. Papildomai pažymėtina, kad nepaisant taikomų prevencijos priemonių gausos, praktika rodo, jog sukčiavimo elektroninėje erdvėje atvejų vis dar pasitaiko, iš to sprendžiama, jog

esamas prevencijos lygis iki šiol nėra pakankamas. Atlikus šiuolaikinio sukčiavimo tyrimo problematikos, prevencijos analizę, tenka pripažinti, jog šiandien praktiniu požiūriu šias nusikalstamas veikas yra paprasčiau ir efektyviau užkardyti, negu tirti jas jau po to, kai nukentėjusiesiems padaroma turtinė žala. Darbo autoriaus vertinimu, tikslinga toliau plėsti prevencinių priemonių spektrą, įtraukiant labiau matomas visuomenės informavimo formas, pavyzdžiui, nacionalinėje televizijoje, analogiškai komercinei reklamai (pvz., tam tikrų prekių nuolaidų reklamavimo principu), trumpai pristatant dažniausiai pasitaikančius sukčiavimo būdus, jų atpažinimo požymius ir praktinius reagavimo veiksmus.

8. Atlikti tyrimai rodo, jog šiame magistro baigiamajame darbe suformuluoti ginamieji teiginiai (mokslinė hipotezė) pasitvirtino, moksliniai tyrimai šioje problematikoje turi būti tęsiami.

LITERATŪROS SĄRAŠAS

Teisės aktai:

1. „Lietuvos Respublikos baudžiamasis kodeksas“, 2000-09-26, Nr. 1001010ISTAIII-1968. TAR. Žiūrėta 2025 m. sausio 31 d., https://www.infolex.lt/ta/66150
2. Lietuvos Respublikos baudžiamasis kodeksas, 182 straipsnis, „Sukčiavimas,“, Nr. 2023-08475. TAR. Žiūrėta 2025 m. sausio 31 d., https://www.infolex.lt/ta/66150:str182
3. Lietuvos Respublikos Prokuratūra. 2014. *Rekomendacijos dėl ikiteisminio tyrimo organizavimo ir atlikimo tiriant elektroninius sukčiavimus.* Patvirtinta 2014 m. vasario 10 d. generalinio prokuroro raštu Nr. 12.14-40. Žiūrėta 2025 m. gruodžio 17 d. https://www.prokuraturos.lt/data/public/uploads/2015/12/rek-del-el-sukciavimu-2014-02-10.pdf
4. Council of Europe. 2001. *Convention on Cybercrime (Budapest Convention).* Budapest: Council of Europe. Žiūrėta 2025 m. gruodžio 17 d., https://rm.coe.int/1680081561
5. Europos Komisija. 2007. *Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų Komitetui – Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme* KOM(2007) 267 galutinis. Žiūrėta 2025 m. gruodžio 17 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52007DC0267
6. European Commission. 2007. *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a General Policy on the Fight against Cyber Crime* COM(2007) 267 final. Žiūrėta 2025 m. gruodžio 17 d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0267
7. „Lietuvos Respublikos kibernetinio saugumo įstatymas“. 2014. TAR, 2014-12-23, Nr. 2014-20553. Žiūrėta 2025 m. gruodžio 17 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.325977/asr
8. Europos Komisija. 2007. *Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų Komitetui – Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme,* KOM(2007) 267 galutinis, SEK(2007) 641, SEK(2007) 642. Briuselis. Žiūrėta 2025 m. gruodžio 17 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:52007DC0267
9. Europol. 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Luxembourg: Publications Office of the European Union. Žiūrėta 2025 m. gruodžio 17 d., https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf

10. Europos Parlamentas. 2021. *Impact of Cryptocurrency – In-depth Analysis (BRIE 696167).* Žiūrėta 2025 m. gruodžio 17 d., https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS_BRI(2021)696167_EN.pdf
11. Lietuvos Respublikos baudžiamojo proceso kodeksas, 168 str., redakcija nuo 2020-11-20. Teisės aktų registras. Žiūrėta 2025 m. gruodžio 17 d https://www.infolex.lt/ta/10708:str168
12. „Dėl Rekomendacijų dėl ikiteisminio tyrimo pradžios ir jos registravimo tvarkos patvirtinimo“. 2008. *Lietuvos Respublikos generalinio prokuroro įsakymas Nr. I-110, 2008 m. rugpjūčio 11 d.* Teisės aktų registras. Žiūrėta 2025 m. gruodžio 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.325977/asr
13. Lietuvos Respublikos generalinis prokuroras. 2025. Įsakymas Nr. I-123 „*Dėl Rekomendacijų dėl ikiteisminio tyrimo organizavimo ir vadovavimo jam patvirtinimo*“ (2025 m. gegužės 30 d.). Teisės aktų registras. https://www.infolex.lt/ta/1039667

Moksliniai šaltiniai:

1. Ancelis, Petras, Gediminas Bučiūnas, Marijus Šalčius, ir Rolandas Šlepetys. 2016. *Atskirų nusikalstamų veikų tyrimas: vadovėlis*. Vilnius: Registrų centras. 71 p. https://cris.mruni.eu/cris/entities/publication/30014ad7-db66-4490-ba70-082895b74b10
2. Matulienė, Snieguolė. 2004. *Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija*. Daktaro disertacija, Mykolo Romerio universitetas. 4, 50, 51-54, 88, 89 118 p., https://cris.mruni.eu/cris/entities/etd/debef03a-a96a-4aad-b47c-6bf84efc5c12
3. Kuklianskis, Samuelis, ir Snieguolė Matulienė. 2002. „Kriminalistinės nusikaltimų charakteristikos samprata.“ *Jurisprudencija* 29(21). 49-65 p., https://ojs.mruni.eu/ojs/jurisprudence/article/view/3581
4. Kažemikaitienė, Eglė, ir Snieguolė Matulienė. 2005. „Kriminalistinė nusikaltimų charakteristika – vienas iš kriminalinės justicijos informacinės sistemos modelio kūrimo pagrindų Lietuvoje.“ *Jurisprudencija* 65(57). https://ojs.mruni.eu/ojs/jurisprudence/article/view/3108
5. Marcinauskaitė, Renata. 2019. *Nusikalstamos veikos elektroninėje erdvėje: elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje: monografija.* Vilnius: Registrų centras. 37 p., https://cris.mruni.eu/cris/entities/publication/c9e5a17d-3878-4db2-ae66-89f31fb5bbc5
6. Štitilis, Darius. 2002. *Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas*

elektroninėje erdvėje problemos. Daktaro disertacija, Lietuvos teisės universitetas. p. 19

7. Ищенко, Е. П., и А. А. Топорков. 2006. Криминалистика: учебник. 2-е изд. Москва: Юнити-Дана. 3, 14 p. https://ru.scribd.com/document/486830669/%D0%98%D1%89%D0%B5%D0%BD%D0%BA%D0%BE-%D0%95-%D0%9F-%D0%A2%D0%BE%D0%BF%D0%BE%D1%80%D0%BA%D0%BE%D0%B2-%D0%90-%D0%90-%D0%9A%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0-pdf
8. Яблоков, Н. П., ред. 2005. *Криминалистика: учебник*. 3-е изд., перераб. и доп. Москва: Юристъ. 39, 150 p. http://koldin-msu.ru/wp-content/uploads/2015/03/Учебник-классический-2005.pdf
9. Torvaldas, Jonas. 1981. *Kriminalistikos keliai ir klystkeliai*. Vilnius: Mintis.
10. Kurapka, Vidmantas Egidijus, ir Snieguolė Matulienė, red. 2012. *Kriminalistika: teorija ir technika: vadovėlis*. Vilnius: Mykolo Romerio universitetas. 10 p., https://cris.mruni.eu/cris/entities/publication/bf3791d3-497c-465a-8665-db859f50ed8d
11. Г. Гросс. 2002. *Руководство для судебных следователей как система криминалистики*. Москва: Юридическая литература.
12. Kiškis, Alfredas. 2017. *Lietuvos kriminologijos raida, 1918–2017 m.: šimtmečio patirtis. Monografija.* Vilnius: Mykolo Romerio universitetas. 11 p., https://cris.mruni.eu/cris/entities/publication/8ea3640d-4ae4-4843-b84d-7c3cb9a7b104
13. Babachinaitė, Genovaitė, ir Vygandas Paulikas. 2002. „Nedarbas ir nusikalstamumas Lietuvos kaime 1918–1990 m.“ *Jurisprudencija* 26(18): 111 p. https://ojs.mruni.eu/ojs/jurisprudence/article/view/3632
14. Indrišionis, Darius. 2020. „Nelegalių ekonominių veiklų ir kovos su jomis vaizdiniai lietuviškoje spaudoje 1938–1940 metais.“ *Lietuvos istorijos studijos* 46: https://www.zurnalai.vu.lt/lietuvos-istorijos-studijos/article/view/22254
15. Kaminskas, Mindaugas. 2006. Kauno komercinė fotografija 1918–1940. *Panevėžio praeities: fotografijos kontekstas ir paveldas*. Panevėžys: Panevėžio kraštotyros muziejus. 66-67 p., http://www.paneveziomuziejus.lt/files/krasto_istorija/Kaminskas_Kauno_komercin_fotografija_1918_1940.pdf
16. Palskys, Eugenijus. 1995. *Lietuvos kriminalistikos istorijos apybraižos (1918–1940):* monografinė studija. Vilnius: Lietuvos policijos akademija. 4, 5, 9 p., https://cris.mruni.eu/cris/entities/publication/c965eb93-d112-4c4a-972e-44b1d71a65ab

17. Kriminalistikos žinynas / redaktorius A. Povilaitis. - 1935-1940 - 1940-Nr.31, https://www.epaveldas.lt/preview?id=C10000221382-1940-Nr.31
18. Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Российская Е. Р. Криминалистика: учебник для вузов / под ред. Р. С. Белкина. Москва: Издательство, 2001. 1-8 p.
19. Kurapka, Vidmantas Egidijus (atsak. red.), Matulienė, Snieguolė (atsak. red.) ir kt. Kriminalistika: taktika ir metodika: vadovėlis. Vilnius: Mykolo Romerio universitetas, 2013. 3-9 p., https://cris.mruni.eu/cris/entities/publication/e00c162c-8f82-41d5-8ffa-4f3a67742a39
20. *Соотношение уголовно-правовой и криминалистической характеристик умышленных убийств* https://studopedia.ru/28_48021_sootnoshenie-ugolovno-pravovoy-i-kriminalisticheskoy-harakteristik-umishlennih-ubiystv.html
21. Pakštaitis, Laurynas. *Nusikalstamų veikų kvalifikavimas: baudžiamojo įstatymo taikymo teorija ir praktinės gairės: vadovėlis*. Vilnius: Mykolo Romerio universitetas, 2024. 156 p. https://cris.mruni.eu/cris/entities/publication/3b7a4d5c-b3c7-4918-9025-9de31db53c7e
22. Кудрявцев В. Н. *Общая теория квалификации преступлений*. Москва: Юридическая литература, 1972., 352 p. https://www.studmed.ru/kudryavcev-vn-obschaya-teoriya-kvalifikacii-prestupleniy_f7451ec8c9d.html
23. Gruodytė, Edita, Olegas Fedosiukas, Albertas Milinis, Aurelijus Gutauskas, Neringa Palionienė, Marius Kuzminovas, Marijus Šalčius ir Simona Žižienė. 2021. *Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga*. 2-asis leidimas. Kaunas: Vytauto Didžiojo universitetas.392, 394, 395 p., https://ebooks.vdu.lt/einfo/3021/lietuvos-baudziamoji-teise-specialioji-dalis-pirmoji-knyga/
24. Abramavičius, Antanas. 2003. *Baudžiamoji teisė: Bendroji dalis.* Vilnius: Eugrimas. Cituojama pagal: Tomas Dargis, *Sukčiavimo (BK 182 straipsnis) atskyrimas nuo nusikalstamų veikų finansų sistemai,* magistro darbas, Vilniaus universitetas, Teisės fakultetas, 2016:16 p.
25. Fedosiuk, Oleg. 2003. „Sukčiavimo normos koncepcija naujame Lietuvos Respublikos baudžiamajame kodekse ir jos įgyvendinimo problemos“. *Teisė 48*: 79 p. https://www.lituanistika.lt/content/45733
26. Girdenis, Tomas, Aurelijus Gutauskas, ir Pavelas Kujalis. *Baudžiamoji teisė: metodinė priemonė.* Vilnius: Mykolo Romerio universitetas, 2014. 228, 232 p. https://cris.mruni.eu/cris/entities/publication/5bafeae8-80c5-414f-9586-1cb4dedb229b
27. Sinkevičius, Edvardas. 2002. *Neteisėtas banko kredito gavimas arba panaudojimas ir jų kvalifikavimas.* Vilnius: Lietuvos teisės universiteto leidybos centras. 49 p.

28. Винокуров, С. И. 1976. :Криминалистическая характеристика преступления, ее содержание и роль в построении методики расследования:. *Методика расследования преступления (общие положения*), Москва. 101 p.
29. Гликерман, А. П., и Е. А. Скобина. 2020. „Криминалистическая характеристика мошенничества на примере судебной практики Забайкальского края“. *Молодой учёный* 15 (305): 183 p., https://moluch.ru/archive/305/68634
30. Образцов, В. А. 1985. *Теоретические основы раскрытия преступлений, связанных с ненадлежащим исполнением профессиональных функций в сфере производства*. Иркутск., 8 p.
31. Корноухов, В. Е. 2001. Курс криминалистики. *Методики расследования насильственных и корыстно-насильственных преступлений*. Москва: Юристъ. 450 p.
32. Файзуллина, А. А. 2017. „К вопросу о соотношении понятий “криминалистическая характеристика преступлений” и “следственная ситуация”“. *Инновационная наука,* 140-142 p.
33. Киселев, Александр Сергеевич, и Ксения Анатольевна Горбунова. 2023. „Особенности криминалистической характеристики преступлений в сфере компьютерной информации“. *Актуальные проблемы государства и права:* 372, 373 p., https://cyberleninka.ru/article/n/osobennosti-kriminalisticheskoy-harakteristiki-prestupleniy-v-sfere-kompyuternoy-informatsii
34. Shepitko, Valery. 2021. Introduction to Criminalistics. Kharkiv: Apostille Publishing House LLC.,54 p.
35. Sup, Yevhen. 2025. “Forensic Characterization Elements of Criminal Offenses Committed by Professional Participants in Justice.” *Theory and Practice of Forensic Science and Criminalistics*. https://khrife-journal.org/index.php/journal/article/view/650
36. Головин, А. Ю. 2012. *Криминалистическая характеристика преступлений как категория современной криминалистики*. Тула: ТулГУ. 43-46. 47-49 p., https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-prestupleniy-kak-kategoriya-sovremennoy-kriminalistiki
37. Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. 2022. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." Forensic Sciences 2, https://doi.org/10.3390/forensicsci2020028
38. Nikoloska, Svetlana, and Marija Gjosheva. 2021. “Criminal Law, Criminological and Criminalist Aspects of Computer Fraud in the Republic of North Macedonia*.” Security*

Concepts and Policies – New Generation of Risks and Threats: Proceedings of the International Scientific Conference. Skopje: Faculty of Security – Skopje, University "St. Kliment Ohridski" – Bitola. 124-125 p. https://eprints.uklo.edu.mk/id/eprint/6808/

39. Харина, Елена Алексеевна. 2024. *Особенности методики расследования мошенничества в сфере компьютерной информации*. Диссертация на соискание ученой степени кандидата юридических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования „Красноярский государственный аграрный университет". 71, 72, 86, 87, 89-97, 107, 108 p., https://kubsau.ru/upload/iblock/500/m0oh4gpjtj0xoc5qcwm213n43ghqy23d.pdf
Смирнова, Вероника Сергеевна. 2025. „Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий". *Институт публичного права и управления, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА).* 92 p., https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-moshennichestva-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy-1
40. Lance Strate, Ronald L. Jacobson, and Stephanie B. Gibson, eds. *2002. Communication and Cyberspace: Social Interaction in an Electronic Environment.* Cresskill, NJ: Hampton Press.
41. Bučiūnas, Gediminas. 2015. „Terminų vartojimas tiriant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui." *Visuomenės saugumas ir viešoji tvarka* 13:14 p. https://www.lituanistika.lt/content/73376
42. Henthorne T. William Gibson: *A Literary Companion. Jefferson: McFarland & Company*, 2011. 176 p.
43. Štitilis, Darius, Paulius Pakutinskas, Marius Laurinaitis, ir Inga Dauparaitė. 2011. *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai.* Vilnius: Mykolo Romerio universitetas. 32,33 p., https://cris.mruni.eu/cris/bitstreams/a736de82-f1c9-449d-b91a-10401e0b1b4a/download
44. Štitilis, D. 2003. *Prekių ženklų naudojimas elektroninėje erdvėje: teisiniai aspektai*, Jurisprudencija 41(33): https://ojs.mruni.eu/ojs/jurisprudence/article/view/3431/3226
45. Štitilis, Darius. 2011. Elektroniniai nusikaltimai. Vilnius: Mykolo Romerio universitetas. 6 p. https://cris.mruni.eu/cris/bitstreams/ef36e100-b123-46b9-b67f-7631ca9498a5/download
46. Pažėrienė, Rasa. 2021. *Nusikaltimų elektroninėje erdvėje atskleidimo teisiniai ir praktiniai ypatumai.* Magistro darbas, Mykolo Romerio universitetas. 16 p., https://cris.mruni.eu/cris/entities/etd/6ae160d4-a0e5-4b30-a296-af830d993d0b

47. Justickis, Viktoras. 2001. *Kriminologija. 1 dalis: vadovėlis.* Vilnius: Lietuvos teisės universiteto Leidybos centras. 189 p., https://cris.mruni.eu/cris/entities/publication/532f2d65-74b9-4fb1-8158-e22bd4fbc659
48. Kalpokas, Vaidas, ir Renata Marcinauskaitė. 2012. „Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas.“ *Teisės problemos* 3 (77):35, 37 p., https://www.lituanistika.lt/content/42148
49. Carrillo-Mondéjar, Javier, José Luis Martínez, ir Guillermo Suarez-Tangil. 2022. „On how VoIP attacks foster the malicious call ecosystem.“ *Computers & Security.* https://www.sciencedirect.com/science/article/pii/S0167404822001535
50. Buzaitė, Indrė. 2014. *Finansinių piramidžių poveikio valdymas tiesioginio pardavimo įmonių veikloje.* Magistro baigiamasis darbas, Vytauto Didžiojo universitetas. https://portalcris.vdu.lt/server/api/core/bitstreams/ab842dbd-30ba-4939-acba-d1601eb3c783/content
51. Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*., https://bitcoin.org/bitcoin.pdf
52. Badi, Sadi. 2024. *The Digital Evolution of Financial Crime: How Cross-Border Fraud Is Reshaping Cybersecurity*. ResearchGate. Žiūrėta 2025 m. gruodžio 16 d., https://www.researchgate.net/publication/389939761_The_Digital_Evolution_of_Financial_Crime_How_Cross-Border_Fraud_is_Reshaping_Cybersecurity
53. Swartz, Lana. 2017. „Theorizing the 2017 Blockchain ICO Bubble as a Network Scam.“ *New Media & Society*, Special Issue: Scams, Fakes, and Frauds. Preprint. https://llaannaa.com/preprint_swartz_nms_ico.pdf
54. Guzman, T. Luis de. 2010. "Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges." *Catholic University Law Review* 59(2): 529 p., https://scholarship.law.edu/cgi/viewcontent.cgi?article=3201&context=lawreview

Ревенко, Н. И. 2024. „Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий.“ *Вестник Омского университета. Серия „Право“* 21(2): 87,88 p., https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-moshennichestva-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy
55. Ярославцева, И. В., и С. А. Дорохина. 2016. „Критическое мышление пожилых людей – жертв мошеннических действий: теоретический и прикладной аспекты исследования.“ *Известия Иркутского государственного университета*. Серия „Психология“ 15: 69, 70 p. https://cyberleninka.ru/article/n/kriticheskoe-myshlenie-

pozhilyh-lyudey-zhertv-moshennicheskih-deystviy-teoreticheskiy-i-prikladnoy-aspekty-issledovaniya/viewer

56. Шурыгина Д. С., Поляков В. В. „Особенности криминалистической характеристики потерпевших по компьютерным преступлениям“ // „Проблемы правовой и технической защиты информации“. 2018 m. 162-166 p
57. Yang, Y., Hackett, K., Katta, S., Ludwig, R. M., Jarcho, J., Giovannetti, T., Fareri, D. S., & Smith, D. V. (2025). Psychological, social, and health-related factors predict risk for financial exploitation. *Communications Psychology, 3*, Article 88 12 p., https://www.nature.com/articles/s44271-025-00266-x
58. Ганиева, Ирада Аллахвердиевна. 2023. „Личность преступника, совершающего дистанционное мошенничество.“ *Актуальные вопросы борьбы с преступлениями 5*. 15, 16 p., https://cyberleninka.ru/article/n/lichnost-prestupnika-sovershayuschego-distantsionnoe-moshennichestvo
59. Novikovienė, Lina. 2001. *Kriminalistikos profilaktinė funkcija: kai kurie teoriniai aspektai.* Vilnius: Lietuvos teisės universitetas.183-188 p.,
60. Matulienė, Snieguolė, ir Lina Novikovienė. 2022. „Kriminalistinės nusikalstamų veikų charakteristikos ir kriminalistinės profilaktikos vieta šiuolaikinės kriminalistikos koncepcijoje.“ *Kriminalistikos teorijos plėtra ir teismo ekspertologijos ateitis : kolektyvinė monografija. Liber Amicorum Profesoriui Vidmantui Egidijui Kurapkai.* Vilnius: Lietuvos kriminalistų draugija, Mykolo Romerio universitetas. 93-95 p. https://cris.mruni.eu/cris/entities/publication/1eab09d3-4b92-40e8-aa22-7729e800ab2e
61. Айвазова, О. В., Г. А. Варданян, и Е. А. Шкуринский. 2022. „Криминалистически значимые особенности субъектов хищений, совершенных с использованием дистанционных технологий.“ *Сибирские уголовно-процессуальные и криминалистические чтения* 2: 44,45 p., https://cyberleninka.ru/article/n/kriminalisticheski-znachimye-osobennosti-subektov-hischeniy-sovershennyh-s-ispolzovaniem-distantsionnyh-tehnologiy
62. Жижина, Марина Владимировна, и Дарья Владимировна Завьялова. 2022. „Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников).“ *Криминалистика и криминология. Судебная экспертиза* 138 (5): 154 p., https://cyberleninka.ru/article/n/lichnost-subekta-prestupleniy-v-sfere-kompyuternoy-informatsii-kak-sistemoobrazuyuschiy-element-kriminalisticheskoy-harakteristiki/viewer

63. Коломинов, Вячеслав Валентинович. 2017. *Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа.* Автореферат диссертации на соискание ученой степени кандидата юридических наук. Иркутск: Байкальский государственный университет. 16, 17 p., https://www.dissercat.com/content/rassledovanie-moshennichestva-v-sfere-kompyuternoi-informatsii-nauchno-teoreticheskaya-osnov
64. Kaminskaitė, Gertrūda. 2023. „Prekybos žmonėmis nusikaltimų kriminalistinė charakteristika.“ *Mykolo Romerio universiteto Viešojo saugumo akademija*, 824 p., https://cris.mruni.eu/cris/bitstreams/7f8f5221-7327-4c7e-8b1d-477f96f2f6db/download
65. Grigaliūnas, Šarūnas. 2020. *Nusikaltimų elektroninėje erdvėje ekspertinio tyrimo metodas*. Daktaro disertacijos santrauka, Kauno technologijos universitetas; Vilniaus Gedimino technikos universitetas. 3 p., https://epubl.ktu.edu/object/elaba:68107071/68107071.pdf
66. Grigaliūnas, Šarūnas. 2015. Elektroninių nusikaltimų pėdsakų ir įtariamojo įpročių koreliacija. Magistro baigiamasis darbas, Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra. 11, 12 p. https://epubl.ktu.edu/object/elaba:8641422/8641422.pdf

Teismų praktika:

1. Lietuvos Aukščiausiojo Teismo senato 2005 m. birželio 23 d. nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“. Teismų praktika, 2005, Nr. 23.
2. Lietuvos Aukščiausiasis Teismas. *Teismų praktikos sukčiavimo baudžiamosiose bylose (Baudžiamojo kodekso 182 straipsnis) apžvalga*. https://www.lat.lt/data/public/uploads/2018/06/ab-36-1.docx
3. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 20 d. nutartis baudžiamojoje byloje Nr. 2K-108-788/2018“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/1576411
4. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. kovo 16 d. nutartis baudžiamojoje byloje Nr. 2K-71-976/2022“ . *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2068440
5. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2024 m. kovo 6 d. nutartis baudžiamojoje byloje Nr. 2K-43-495/2024“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2230506

6. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2020 m. kovo 24 d. nutartis baudžiamojoje byloje Nr. 2K-76-788/2020“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. 53, p. 565-573, https://www.infolex.lt/tp/1869178
7. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2021 m. kovo 9 d. nutartis baudžiamojoje byloje Nr. 2K-27-788/2021“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/1975659
8. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. lapkričio 14 d. nutartis baudžiamojoje byloje Nr. 2K-215-697/2023“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2204286
9. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. gegužės 24 d. nutartis baudžiamojoje byloje Nr. 2K-262/2011“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/205838
10. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. spalio 20 d. nutartis baudžiamojoje byloje Nr. 2K-P-267/2011“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/228818
11. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2013 m. gegužės 14 d. nutartis baudžiamojoje byloje Nr. 2K-250/2013“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/677654
12. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. balandžio 23 d. nutartis baudžiamojoje byloje Nr. 2K-7-27-746/2015“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. 43, p. 358-368, https://www.infolex.lt/tp/1045319
13. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. sausio 15 d. nutartis baudžiamojoje byloje Nr. 2K-7-47-895/2016“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/1173577
14. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2017 m. vasario 7 d. nutartis baudžiamojoje byloje Nr. 2K-7-41-511/2017“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. 47, p. 457-475, https://www.infolex.lt/tp/1426475
15. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2017 m. lapkričio 16 d. nutartis baudžiamojoje byloje Nr. 2K-7-136-489/2017“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. 48, p. 270-290, https://www.infolex.lt/tp/1538664
16. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2020 m. vasario 11 d. nutartis baudžiamojoje byloje Nr. 2K-17-976/2020“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/1817721

17. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2021 m. birželio 28 d. nutartis baudžiamojoje byloje Nr. 2K-158-303/2021“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2006460
18. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. vasario 2 d. nutartis baudžiamojoje byloje Nr. 2K-6-976/2023“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2140988
19. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2025 m. gegužės 28 d. nutartis baudžiamojoje byloje Nr. 2K-91-891/2025“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2317237
20. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 26 d. nutartis baudžiamojoje byloje Nr. 2K-46-699/2018“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1584302
21. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. lapkričio 22 d. nutartis baudžiamojoje byloje Nr. 2K-241-942/2022“. *Teismų praktika*, 2022, Nr. 58, p. 524–561. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d , https://www.infolex.lt/tp/2123749
22. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. gegužės 8 d. nutartis baudžiamojoje byloje Nr. 2K-138-1073/2023“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2162528
23. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2024 m. gruodžio 12 d. nutartis baudžiamojoje byloje Nr. 2K-261-489/2024“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2284787
24. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 30 d. nutartis baudžiamojoje byloje Nr. 2K-507/2012“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/478922
25. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2014 m. birželio 19 d. nutartis baudžiamojoje byloje Nr. 2K-327/2014“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/831495
26. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. birželio 6 d. nutartis baudžiamojoje byloje Nr. 2K-188-719/2018“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1603326
27. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. birželio 17 d. nutartis baudžiamojoje byloje Nr. 2K-264-895/2016“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1288766
28. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. birželio 6 d. nutartis baudžiamojoje byloje Nr. 2K-188-719/2018“. Infolex. Žiūrėta 2025 m. gruodžio

16 d., https://www.infolex.lt/tp/1603326

29. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. kovo 16 d. nutartis baudžiamojoje byloje Nr. 2K-71-976/2022“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2068440
30. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. vasario 2 d. nutartis baudžiamojoje byloje Nr. 2K-6-976/2023“. Infolex. Žiūrėta 2025 m. gruodžio 16 d., https://www.infolex.lt/tp/2140988
31. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2007 m. spalio 2 d. nutartis baudžiamojoje byloje Nr. 2K-605/2007“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/81406
32. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2008 m. gegužės 6 d. nutartis baudžiamojoje byloje Nr. 2K-211/2008“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/86476
33. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2009 m. birželio 23 d. nutartis baudžiamojoje byloje Nr. 2K-197/2009“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d , https://www.infolex.lt/tp/128269
34. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. kovo 5 d. nutartis baudžiamojoje byloje Nr. 2K-52-511/2019“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1705125
35. „Lietuvos Aukščiausiojo Teismo atrankos kolegijos 2020 m. gruodžio 22 d. nutartis Nr. 2K-278-303/2020“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1954818
36. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. kovo 1 d. nutartis baudžiamojoje byloje Nr. 2K-51-788/2022“. *Teismų praktika*, 2022, Nr. 57, p. 400–411. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2064210
37. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2011 m. gegužės 31 d. nutartis baudžiamojoje byloje Nr. 2K-257/2011“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/211678
38. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2012 m. gegužės 29 d. nutartis baudžiamojoje byloje Nr. 2K-275/2012“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/380545
39. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 2 d. nutartis baudžiamojoje byloje Nr. 2K-453/2012“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/449713

40. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2013 m. sausio 29 d. nutartis baudžiamojoje byloje Nr. 2K-35/2013“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/506623
41. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. gegužės 17 d. nutartis baudžiamojoje byloje Nr. 2K-156-788/2016“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1269445
42. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-103-976/2016“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1241430
43. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2017 m. gegužės 16 d. nutartis baudžiamojoje byloje Nr. 2K-109-746/2017“. *Teismų praktika*, 2017, Nr. 47, p. 572–616. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1475216
44. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. birželio 20 d. nutartis baudžiamojoje byloje Nr. 2K-178-303/2019“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1740432
45. „Lietuvos Aukščiausiojo Teismo atrankos kolegijos 2020 m. vasario 27 d. nutartis Nr. 2K-1-719/2020“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/1852510
46. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. birželio 19 d. nutartis baudžiamojoje byloje Nr. 2K-7-38-1073/2023“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d ., https://www.infolex.lt/tp/2173033
47. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. gruodžio 6 d. nutartis baudžiamojoje byloje Nr. 2K-149-648/2023“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2210026
48. „Lietuvos Aukščiausiasis Teismas, Baudžiamųjų bylų skyrius, 2023 m. birželio 22 d. nutartis baudžiamojoje byloje Nr. 2K-170-495/2023“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2173648
49. „Lietuvos Aukščiausiasis Teismas, Baudžiamųjų bylų skyrius, 2024 m. vasario 13 d. nutartis baudžiamojoje byloje Nr. 2K-13-654/2024“. *Infolex*. Žiūrėta 2025 m. gruodžio 16 d. , https://www.infolex.lt/tp/2225669
50. „Vilniaus apygardos teismas, Baudžiamųjų bylų skyrius, 2025 m. spalio 23 d. nutartis baudžiamoji byla Nr. 1A-235-1036/2025“,. *Infolex*. https://www.infolex.lt/tp/2344316
51. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019.“. *Infolex*. 2019, Nr. 52, p. 387–403 https://www.infolex.lt/tp/1744638

Internetiniai šaltiniai:

1. Ryšių reguliavimo tarnyba, Lietuvos kriminalinės policijos biuras, „Nusikaltėliai elektroninėje erdvėje: kaip sekasi juos stabdyti?“, *pristatymo skaidrės*, 2025 m. gruodžio 17 d., https://www.rrt.lt/wp-content/uploads/2024/10/4_NEE-kaip-sekasi-juos- stabdyti-2024-10-24-2.pdf
2. Informatikos ir ryšių departamentas. „Sukčiavimai.“ *IRD.lt*, žiūrėta 2025 m. gruodžio 17 d. https://ird.lt/lt/atviri-duomenys/sukciavimai
3. Pinigų plovimo prevencijos kompetencijų centras. „2023 m. finansinių sukčių aktyvumas augo trečdaliu, pasitelkė vartotojų pandeminius įpročius.“ *AMLcenter.lt*, žiūrėta 2025 m. gruodžio 17 d., https://amlcenter.lt/2023-m-finansiniu-sukciu-aktyvumas-augo-trecdaliu-pasitelke-vartotoju-pandeminius-iprocius/
4. Nacionalinis kibernetinio saugumo centras. „Fišingas.“ *NKSC.lt*, žiūrėta 2025 m. gruodžio 17 d. https://www.nksc.lt/rekomendacijos/phishing.html
5. Lietuvos bankų asociacija. „Investiciniai sukčiai siautėja toliau: pagrindiniai požymiai ir patarimai, kaip išvengti spąstų.“ *LBA.lt*, žiūrėta 2025 m. gruodžio 17 d. https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/investiciniai-sukciai-siauteja-toliau-pagrindiniai-pozymiai-ir-patarimai-kaip-isvengti-spastu#:~:text=%E2%80%9EInvesticinis%20suk%C4%8Diavimas%20%E2%80%93%20metodas%2C%20kuriam,pelno%20garantija%20ir%20minimalia%20rizika.
6. Nacionalinis kibernetinio saugumo centras. „Nacionalinė kibernetinio saugumo būklės ataskaita 2024.“ *VDAI.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d., https://vdai.lrv.lt/public/canonical/1748429329/942/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf
7. Lietuvos Respublikos prokuratūra. „Nusikaltimai elektroninėje erdvėje.“ Prokuraturos.lt, žiūrėta 2025 m. gruodžio 17 d., https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185
8. Lietuvos policija. „Tarptautinis tyrimas atskleidė organizuotą sukčiavimo schemą.“ *Policija.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d. https://policija.lrv.lt/lt/naujienos/tarptautinis-tyrimas-atskleide-organizuota-sukciavimo-schema/
9. *Международный журнал Молодой ученый*. Часть 3, Казань 2017 m. 210 p. https://moluch.ru/archive/153/43409/

10. Bernardinai.lt. „Tinklalaidė „Ko tyli istorikai?“: nusikaltimai tarpukariu.“ *Bernardinai.lt*, žiūrėta 2025 m. gruodžio 17 d. https://www.bernardinai.lt/tinklalaide-ko-tyli-istorikai-nusikaltimai-tarpukariu/
11. Lietuvos kriminalinės policijos biuras. „Kriminalinės policijos istorija.“ *LKPB.policija.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d. https://lkpb.policija.lrv.lt/lt/apie-mus/kriminalines-policijos-istorija/
12. Stasys Keinys, vyriaus. red., *Dabartinės lietuvių kalbos žodynas*, 8-as patais. ir papild. leid. (Vilnius: Lietuvių kalbos institutas, 2021), XXVI, 973, https://ekalba.lt
13. Lietuvių kalbos žodynas. „Ultima ratio.“ *Lietuviuzodynas.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.lietuviuzodynas.lt/terminai/Ultima_ratio.
14. Fortinet. „Internet Fraud.“ *Fortinet CyberGlossary*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/resources/cyberglossary/internet-fraud
15. 15min. „Naujas sukčiavimo būdas: sukčiai naudojasi E. sveikatos portalo vardu.“ *15min.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.15min.lt/naujiena/aktualu/nusikaltimaiirnelaimes/naujas-sukciavimo-budas-sukciai-naudojasi-e-sveikatos-portalo-vardu-59-2356332
16. Fortinet. „Spyware.“ *Fortinet CyberGlossary*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/resources/cyberglossary/spyware
17. Insights2Techinfo. „The Rise of AI Smishing: Protecting Yourself from Next-Gen Scams.“ *Insights2Techinfo*, žiūrėta 2025 m. gruodžio 17 d., https://insights2techinfo.com/the-rise-of-ai-smishing-protecting-yourself-from-next-gen-scams/
18. Ironscales. „Clone Phishing.“ *Ironscales*, žiūrėta 2025 m. gruodžio 17 d. https://ironscales.com/guides/phishing-prevention/clone-phishing
19. Vilniaus apskrities vyriausiasis policijos komisariatas. „Sukčiavimas apsiperkant internetu.“ *Vilnius.policija.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d., https://vilnius.policija.lrv.lt/lt/policija-pataria/sukciavimu-prevencija/sukciavimas-apsiperkant-internetu/
20. Indeed. „Data Entry Job Scam: How To Spot and Avoid It.“ *Indeed Career Guide*, žiūrėta 2025 m. gruodžio 17 d., https://www.indeed.com/career-advice/finding-a-job/data-entry-job-scam
21. Federal Bureau of Investigation. „Romance Scams.“ *FBI.gov*, žiūrėta 2025 m. gruodžio 17 d., https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams

22. Revolut. „Apie sukčiavimą ir apgavystes.“ *Revolut*, žiūrėta 2025 m. gruodžio 17 d., https://www.revolut.com/lt-LT/about-fraud-and-scam/
23. Lrytas.lt. „Prisidengdami loterija, sukčiai bando išvilioti duomenis – paviešino, kokius laiškus siunčia.“ *Lrytas.lt*, žiūrėta 2025 m. gruodžio 17 d. https://www.lrytas.lt/lietuvosdiena/kriminalai/2022/04/12/news/prisidengdami-loterija-sukciai-bando-isvilioti-duomenis-paviesino-kokius-laiskus-siuncia-23041008
24. Lietuvos policija. „Policija pataria.“ *Policija.lrv.lt*, žiūrėta 2025 m. gruodžio 17 d., https://policija.lrv.lt/lt/policija-pataria/
25. Atvira Klaipėda. „Google“ vardą naudojantiems sukčiams atiteko dar 9200 eurų.“ *AtviraKlaipeda.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.atviraklaipeda.lt/2024/09/21/google-varda-naudojantiems-sukciams-atiteko-dar-9200-euru/
26. Valstybinė mokesčių inspekcija. „Gavau įtartiną pranešimą iš VMI.“ *VMI.lt,* žiūrėta 2025 m. gruodžio 17 d. https://www.vmi.lt/evmi/gavau-itartina-pranesima-is-vmi
27. LRT. „Sukčiai tyko visur: FNTT paaiškina, kaip atpažinti galimą investicinį sukčiavimą.“ *LRT.lt,* žiūrėta 2025 m. gruodžio 17 d. https://www.lrt.lt/naujienos/verslas/4/2047671/sukciai-tyko-visur-fntt-paaiskina-kaip-atpazinti-galima-investicini-sukciavima?srsltid=AfmBOoqsK9dStrhQkG1cAYK-qGlsbjTV4WbohfHj77iA2RLJYAYDC9Z3
28. Lietuvos paštas. „Lietuvos paštas perspėja apie sukčių pinkles – jauku tampa bendrovės vardas.“ *Post.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.post.lt/lt/apie-mus/naujienos/lietuvos-pastas-perspeja-apie-sukciu-pinkles-jauku-tampa-bendroves-vardas
29. Phishing.org. „History of Phishing.“ *Phishing.org,* žiūrėta 2025 m. gruodžio 17 d., https://www.phishing.org/history-of-phishing
30. Fortinet. „Types of Phishing Attacks.“ *Fortinet CyberGlossary*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
31. Esaugumas. „Phishing laiškų pavyzdžiai.“ *Esaugumas.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.esaugumas.lt/phishing-laisku-pavyzdziai
32. Esaugumas. „Kaip vyksta duomenų viliojimas (angl. phishing).“ *Esaugumas.lt,* žiūrėta 2025 m. gruodžio 17 d., https://esaugumas.lt/articles/kaip-vyksta-duomenu-viliojimas-angl-phishing
33. Finansinių nusikaltimų tyrimo tarnyba. „Ataskaita 2024.“ *FNTT.lrv.lt,* žiūrėta 2025 m. gruodžio 17 d. 17 p., https://fntt.lrv.lt/public/canonical/1749447681/1063/Ataskaita_2024%20(1).pdf

34. Canadian Centre for Cyber Security. „Search Engine Optimization (SEO) Poisoning (ITSAP.00.013).“ *Cyber.gc.ca,* žiūrėta 2025 m. gruodžio 17 d., https://www.cyber.gc.ca/en/guidance/search-engine-optimization-poisoning-itsap00013
35. Malwarebytes. „Что такое malvertising?“ *Malwarebytes*, žiūrėta 2025 m. gruodžio 17 d., https://www.malwarebytes.com/ru/malvertising
36. Proofpoint. „Pharming.“ *Proofpoint,* žiūrėta 2025 m. gruodžio 17 d. https://www.proofpoint.com/us/threat-reference/pharming
37. Malwarebytes. „Что такое фарминг (pharming)?“ *Malwarebytes,* žiūrėta 2025 m. gruodžio 17 d., https://www.malwarebytes.com/ru/pharming
38. Proofpoint. „Email Spoofing.“ *Proofpoint,* žiūrėta 2025 m. gruodžio 17 d. https://www.proofpoint.com/us/threat-reference/email-spoofing
39. Proofpoint. „SMTP Relay.“ *Proofpoint,* žiūrėta 2025 m. gruodžio 17 d., https://www.proofpoint.com/us/threat-reference/smtp-relay
40. Get Cyber Safe. „Script Spoofing: Protect Yourself.“ *GetCyberSafe.gc.ca*, žiūrėta 2025 m. gruodžio 17 d., https://www.getcybersafe.gc.ca/en/blogs/script-spoofing-protect-yourself
41. Darktrace. „Thread Hijacking: How Attackers Exploit Trusted Conversations to Infiltrate Networks.“ *Darktrace,* žiūrėta 2025 m. gruodžio 17 d., https://www.darktrace.com/blog/thread-hijacking-how-attackers-exploit-trusted-conversations-to-infiltrate-networks
42. MITRE ATT&CK. „T1566: Phishing.“ *MITRE ATT&CK*, žiūrėta 2025 m. gruodžio 17 d., https://attack.mitre.org/techniques/T1566/
43. Mimecast. „Website Spoofing.“ *Mimecast*, žiūrėta 2025 m. gruodžio 17 d., https://www.mimecast.com/content/website-spoofing/
44. Proofpoint. „Domain Spoofing.“ *Proofpoint*, žiūrėta 2025 m. gruodžio 17 d., https://www.proofpoint.com/us/threat-reference/domain-spoofing
45. Amazon Web Services. „В чём разница между HTTPS и HTTP?“ *AWS*, žiūrėta 2025 m. gruodžio 17 d., https://aws.amazon.com/ru/compare/the-difference-between-https-and-http/
46. IBM. „Web Hosting.“ *IBM*, žiūrėta 2025 m. gruodžio 17 d., https://www.ibm.com/think/topics/web-hosting
47. Interneto vizija. „Domeno registracijos gidas.“ *Domreg.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.domreg.lt/duk/domain_registration_guide.pdf
48. Interneto vizija. „Procedūrinis reglamentas.“ *Domreg.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.domreg.lt/informacija/dokumentai/procedurinis-reglamentas.pdf

49. ICANN. „.com Registry Agreement.“ *ICANN.org*, žiūrėta 2025 m. gruodžio 17 d., https://itp.cdn.icann.org/en/files/registry-agreements/com/com-agreement-pdf-01-12-2024-en.pdf
50. SentinelOne. „Deconstructing PowerShell Obfuscation in Malspam Campaigns.“ *SentinelOne*, žiūrėta 2025 m. gruodžio 17 d., https://www.sentinelone.com/blog/deconstructing-powershell-obfuscation-in-malspam-campaigns/
51. Radware. „Keylogging.“ *Radware DDoSpedia*, žiūrėta 2025 m. gruodžio 17 d., https://www.radware.com/security/ddos-knowledge-center/ddospedia/keylogging/
52. Fortinet. „Latest Remcos RAT Phishing Campaign Uses XWorm to Deliver Malware.“ *Fortinet Blog*, žiūrėta 2025 m. gruodžio 17 d., https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing
53. The Hacker News. „Fileless Remcos RAT Delivered via Weaponized Windows LNK Files.“ *The Hacker News*, žiūrėta 2025 m. gruodžio 17 d., https://thehackernews.com/2025/05/fileless-remcos-rat-delivered-via-lnk.html
54. Microsoft. „What Is Malware?“ *Microsoft Security*, žiūrėta 2025 m. gruodžio 17 d., https://www.microsoft.com/en-us/security/business/security-101/what-is-malware
55. Proofpoint. „Smishing.“ *Proofpoint*, žiūrėta 2025 m. gruodžio 17 d https://www.proofpoint.com/us/threat-reference/smishing
56. „SMS gateway.“ *Wikipedia*, žiūrėta 2025 m. gruodžio 17 d., https://en.wikipedia.org/wiki/SMS_gateway
57. „IP adresas.“ *Vikipedija,* žiūrėta 2025 m. gruodžio 17 d. https://lt.wikipedia.org/wiki/IP_adresas ., https://lt.wikipedia.org/wiki/IP_adresas
58. BioCatch. „Let’s Hack Your Mind.“ *BioCatch Blog*, žiūrėta 2025 m. gruodžio 17 d., https://www.biocatch.com/blog/lets-hack-your-mind
59. CrowdStrike. „What Is a Vishing Attack?“ *CrowdStrike,* žiūrėta 2025 m. gruodžio 17 d., https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/vishing-attack/
60. EC-Council. „Clearing Logs in Ethical Hacking: What You Need to Know.“ *EC-Council,* žiūrėta 2025 m. gruodžio 17 d., https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/clearing-logs/
61. EC-Council. „International Council of E-Commerce Consultants.“ *EC-Council,* žiūrėta 2025 m. gruodžio 17 d., https://www.eccouncil.org/
62. Veriato. „How Cyber Attackers Hide Their Tracks After Committing Digital Fraud.“ *Veriato,* žiūrėta 2025 m. gruodžio 17 d., https://veriato.com/blog/how-cyber-attackers-hide-their-tracks-after-committing-digital-fraud/

63. Nacionalinis kibernetinio saugumo centras. „Tarpinės stoties paslauga (Proxy).“ *NKSC.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.nksc.lt/rekomendacijos/tarpines_stoties_paslauga_proxy.html
64. Esaugumas. „Anoniminis tinklas TOR.“ *Esaugumas.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.esaugumas.lt/articles/anoniminis-tinklas-tor
65. Gupta, Rahul. „Self Deleting Malware: Antivirus Bypass Techniques Using Batch Scripting.“ *LinkedIn,* žiūrėta 2025 m. gruodžio 17 d., https://www.linkedin.com/pulse/self-deleting-malware-antivirus-bypass-techniques-using-gupta--m2dsc
66. Paysera. „Dažnos finansinės apgaulės.“ *Paysera.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.paysera.lt/v2/lt-LT/blog/daznos-finansines-apgaules
67. Mano pinigai. „Gyventojų investavimas: tendencijos teigiamos, bet esminis lūžis dar neįvykęs.“ *Manopinigai.vz.lt,* žiūrėta 2025 m. gruodžio 17 d., https://manopinigai.vz.lt/investavimas/gyventoju-investavimas-tendencijos-teigiamos-bet-esminis-luzis-dar-neivykes/
68. Internet Crime Complaint Center (IC3). „Investment Fraud.“ *IC3.gov*, žiūrėta 2025 m. gruodžio 17 d., https://www.ic3.gov/CrimeInfo/Investment
69. U.S. Securities and Exchange Commission. „Investment Scams Targeting Groups.“ *Investor.gov,* žiūrėta 2025 m. gruodžio 17 d., https://www.investor.gov/protect-your-investments/fraud/types-fraud/investment-scams-targeting-groups
70. Lietuvos policija. „Apgaulės piramidė: kaip nepakliūti į naujausias finansines pinkles.“ *Policija.lrv.lt,* žiūrėta 2025 m. gruodžio 17 d., https://policija.lrv.lt/lt/naujienos/apgaules-piramide-kaip-nepakliuti-i-naujausias-finansines-pinkles/
71. Smithsonian National Postal Museum. „Ponzi Scheme.“ *National Postal Museum,* žiūrėta 2025 m. gruodžio 17 d., https://postalmuseum.si.edu/exhibition/behind-the-badge-case-histories-scams-and-schemes/ponzi-scheme
72. „MMM“, *Vikipedija*, https://lt.wikipedia.org/wiki/MMM
73. TripleA. „Cryptocurrency Ownership Data.“ *TripleA*, žiūrėta 2025 m. gruodžio 17 d, https://www.triple-a.io/cryptocurrency-ownership-data
74. Swedbank. „Kriptovaliutos.“ *Swedbank Blogas,* žiūrėta 2025 m. gruodžio 17 d., https://blog.swedbank.lt/zodynelis/kriptovaliutos
75. Encyclopedia Britannica. „What Is Blockchain?“ *Britannica*, žiūrėta 2025 m. gruodžio 17 d., https://www.britannica.com/money/what-is-blockchain
76. Ethereum Foundation. „Išmaniosios sutartys.“ *Ethereum.org*, žiūrėta 2025 m. gruodžio 17 d., https://ethereum.org/lt/developers/docs/smart-contracts/

77. Encyclopedia Britannica. „Cryptocurrency Wallet.“ *Britannica*, žiūrėta 2025 m. gruodžio 17 d., https://www.britannica.com/money/cryptocurrency-wallet
78. „Централизованная биржа (CEX) против децентрализованной (DEX): полный разбор.“ *Cryptomus,* žiūrėta 2025 m. gruodžio 17 d., https://cryptomus.com/ru/blog/centralized-exchange-cex-vs-decentralized-exchange-dex-complete-comparison
79. Telco. „Kuo skiriasi kriptovaliutos moneta ir žetonas?“ *Telco.in,* žiūrėta 2025 m. gruodžio 17 d., https://www.telco.in/lt/support-center/cryptocurrency-basics/what-is-the-difference-between-a-coin-and-a-token
80. bitFlyer. „What Is an Altcoin?“ *bitFlyer*, žiūrėta 2025 m. gruodžio 17 d., https://bitflyer.com/en-eu/faq/55-7
81. Lietuvos bankas. „Vertybinių popierių požymių turinčių žetonų siūlymo gairės.“ *Lietuvos bankas,* žiūrėta 2025 m. gruodžio 17 d., https://www.lb.lt/uploads/documents/files/STO_gaires_pakartotinai_20190904.pdf?
82. „Verslo angelai,“ *Vikipedija,* https://lt.wikipedia.org/wiki/Verslo_angelai
83. Seth, Shobhit. „What Is a Cryptocurrency Exit Scam? How Do You Spot One?“ *Investopedia*, žiūrėta 2025 m. gruodžio 17 d., https://www.investopedia.com/tech/whats-cryptocurrency-exit-scam-how-spot-one/
84. Volity Team. „What Is a Crypto Exit Scam?“ *Volity.io*, žiūrėta 2025 m. gruodžio 17 d., https://volity.io/crypto/exit-scams/
85. Alfa.lt. „FNTT atlieka kratas su „Bankera“ siejamose įmonėse.“ *Alfa.lt*, žiūrėta 2025 m. gruodžio 17 d., https://www.alfa.lt/aktualijos/lietuva/fntt-atlieka-kratas-su-bankera-siejamose-imonese/377143/
86. Flagship. „How to Protect Yourself from ICO, IEO, and IDO Scams: A Quick Guide.“ *Flagship.fyi,* žiūrėta 2025 m. gruodžio 17 d., https://flagship.fyi/outposts/market-insights/how-to-protect-yourself-from-ico-ieo-and-ido-scams-a-quick-guide/
87. Mpost. „DeFi.“ *Mpost.io,* žiūrėta 2025 m. gruodžio 17 d., https://mpost.io/lt/glossary/defi/
88. RWaltz. „Liquidity Mining in DEX: How It Works and Its Benefits.“ *RWaltz.com,* žiūrėta 2025 m. gruodžio 17 d., https://www.rwaltz.com/blog/liquidity-mining-in-dex-how-it-works-and-its-benefits
89. dYdX. „What Are dApps?“ *dYdX*, žiūrėta 2025 m. gruodžio 17 d., https://www.dydx.xyz/crypto-learning/dapps
90. California Department of Financial Protection and Innovation. „Crypto Scam Tracker.“ *DFPI.ca.gov,* žiūrėta 2025 m. gruodžio 17 d.,

https://dfpi.ca.gov/consumers/crypto/crypto-scam-tracker/#:~:text=In%20a%20liquidity%20mining%2Fyield,victims%20purchase%20additional%20crypto%20assets

91. Internet Crime Complaint Center (IC3). „IC3 Warns of Increase in Use of Remote Desktop Protocol to Facilitate Fraud.“ *IC3.gov,* žiūrėta 2025 m. gruodžio 17 d., https://www.ic3.gov/PSA/2022/PSA220721
92. Investopedia. „A Brief History of Fraud.“ *Investopedia*, žiūrėta 2025 m. gruodžio 17 d., https://www.investopedia.com/articles/financial-theory/09/history-of-fraud.asp
93. „Pool operation”, *Wikipedia,* https://en.wikipedia.org/wiki/Pool_operation
94. „Anaconda Copper,“ *Wikipedia,* https://en.wikipedia.org/wiki/Anaconda_Copper
95. Bitstamp. „What Are Pump and Dump Schemes?“ *Bitstamp.net,* žiūrėta 2025 m. gruodžio 17 d., https://www.bitstamp.net/learn/crypto-trading/what-are-pump-and-dump-schemes/
96. U.S. Commodity Futures Trading Commission. „Customer Advisory: Beware of Pump-and-Dump Schemes.“ *CFTC.gov,* žiūrėta 2025 m. gruodžio 17 d., https://www.cftc.gov/sites/default/files/2019-12/customeradvisory_pumpdump0218.pdf?utm
97. CoinMarketCap. „Rug Pull.“ *CoinMarketCap Academy*, žiūrėta 2025 m. gruodžio 17 d., https://coinmarketcap.com/academy/glossary/rug-pull
98. Business Insider. „NFT Meaning: What Is an NFT and How Does It Work?“ *Business Insider,* žiūrėta 2025 m. gruodžio 17 d., https://www.businessinsider.com/personal-finance/investing/nft-meaning
99. Organization for Security and Co-operation in Europe. „OSCE Supports Uzbekistan’s Efforts to Combat Money Laundering and Terrorism Financing.“ *OSCE.org*, žiūrėta 2025 m. gruodžio 17 d., https://www.osce.org/oceea/587475
100. BBC Newsround. „What Is Cyber Crime?“ *BBC,* žiūrėta 2025 m. gruodžio 17 d. https://www.bbc.co.uk/newsround/69009887
101. Moin, Md Tahmid, Jobayer Hossain, and Selim S. A. Bhuiyan. „Cyber Fraud Detection Using Machine Learning: A Comprehensive Review.“ *arXiv*, žiūrėta 2025 m. gruodžio 17 d. https://arxiv.org/abs/2402.18085
102. LRT. „Įspėjama apie sukčius, kurie dengiasi žinomais LRT vardais.“ *LRT.lt*. 2025 m. rugpjūčio 17 d. Žiūrėta 2025 m. gruodžio 17 d. https://www.lrt.lt/naujienos/lietuvoje/2/2635297/ispejama-apie-sukcius-kurie-dengiasi-zinomais-lrt-vardais?srsltid=AfmBOopvZGs6hS7GP0W0gpy0qgCfVd4gE3S5rqhx1YH-9CQs7x4fd13X

103. California Department of Financial Protection and Innovation (DFPI). *Pig Butchering – How to Spot and Report the Scam.* Žiūrėta 2025 m. gruodžio 17 d., https://dfpi.ca.gov/news/insights/pig-butchering-how-to-spot-and-report-the-scam/

104. Pinigų plovimo prevencijos kompetencijų centras. „Sukčiavimo prevencija gyventojams.“ *AMLcenter.lt.* Žiūrėta 2025 m. gruodžio 17 d., https://amlcenter.lt/sukciavimo-prevencija/sukciavimo-prevencija-gyventojams/

105. Pinigų plovimo prevencijos kompetencijų centras. „AML mokymai: Red Flags.“ *AMLcenter.lt,* žiūrėta 2025 m. gruodžio 17 d., https://amlcenter.lt/wp-content/uploads/2025/10/AML-mokymai-red-flags.pdf

106. „Slapukas.“ *Vikipedija*, žiūrėta 2025 m. gruodžio 17 d. , https://lt.wikipedia.org/wiki/Slapukas

107. 15min. „Sukčiai skambina ir rašo jūsų tėvams bei seneliams: kaip juos apsaugoti?“ *15min.lt*, 2024 m. Žiūrėta 2025 m. gruodžio 17 d. , https://www.15min.lt/verslas/naujiena/finansai/sukciai-skambina-ir-raso-jusu-tevams-bei-seneliams-kaip-juos-apsaugoti-662-2504672

108. Lietuvos policija. „Pasirašytas memorandumas – reikšmingas žingsnis elektroniniams sukčiavimams valstybėje užkardyti.“ *Policija.lrv.lt*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d. , https://policija.lrv.lt/lt/naujienos/pasirasytas-memorandumas-reiksmingas-zingsnis-elektroniniams-sukciavimams-valstybeje-uzkardyti/

109. Lietuvos Respublikos generalinė prokuratūra. „Sukčiavimui skaitmeninėje erdvėje mažinti – veiksmingas institucijų bendradarbiavimas.“ *Prokuraturos.lt*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d., https://www.prokuraturos.lt/lt/prokuraturos-aktualijos/sukciavimui-skaitmenineje-erdveje-mazinti-veiksmingas-instituciju-bendradarbiavimas/11144

110. Lietuvos bankas. „Gavėjo tikrinimo paslauga.“ *Lietuvos bankas*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d. , https://www.lb.lt/lt/gavejo-tikrinimo-paslauga

111. Ryšių reguliavimo tarnyba. „Įjungus naują apsaugą, operatoriai kas savaitę sustabdo apie pusę milijono sukčių skambučių.“ *RRT.lt*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d. , https://www.rrt.lt/ijungus-nauja-apsauga-operatoriai-kas-savaite-sustabdo-apie-puse-milijono-sukciu-skambuciu/

112. Finansinių nusikaltimų tyrimo tarnyba. „Baigiasi pereinamasis laikotarpis VASP: nuo 2026 m. sausio 1 d. privaloma kriptoturto paslaugų teikėjo licencija.“ *FNTT.lrv.lt*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d., https://fntt.lrv.lt/lt/naujienos/baigiasi-pereinamasis-laikotarpis-vasp-nuo-2026-m-sausio-1-d-privaloma-kriptoturto-paslaugu-teikejo-licencija-uww/

113. Lietuvos bankas. „Lietuvos bankas išdavė pirmąją kriptoturto paslaugų teikėjo licenciją.“ *Lietuvos bankas*, 2025 m. Žiūrėta 2025 m. gruodžio 17 d. , https://www.lb.lt/lt/naujienos/lietuvos-bankas-isdave-pirmaja-kriptoturto-paslaugu-teikejo-licencija

114. Nacionalinis kibernetinio saugumo centras. „Veikla.“ *NKSC.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.nksc.lt/veikla.html

115. LRT. „NKSC per pratybas pirmą kartą fiksavo didesnį e. sukčiavimą supratusių asmenų skaičių.“ *LRT.lt,* žiūrėta 2025 m. gruodžio 17 d., https://www.lrt.lt/naujienos/lietuvoje/2/2592135/nksc-per-pratybas-pirma-karta-fiksavo-didesni-e-sukciavima-supratusiu-asmenu-skaiciu?srsltid=AfmBOorTr8GedfASHlE9Ipd-s-RDEctvEWusMle1oygvSzzeLwocFEVZ

116. Reuters. „Key barrier to online fraud can be bypassed for pennies, say researchers.“ *Reuters,* žiūrėta 2025 m. gruodžio 17 d., https://www.reuters.com/business/media-telecom/key-barrier-online-fraud-can-be-bypassed-pennies-say-researchers-2025-12-11/

117. Twingate. „VoIP Spoofing.“ *Twingate Blog*, žiūrėta 2025 m. gruodžio 17 d., https://www.twingate.com/blog/glossary/voip%20spoofing?

118. Borys Musielak @ Warsaw, įrašas socialiniame tinkle *X* (buv. Twitter), https://x.com/michuk/status/1907078798908248478

119. АМИА. „Преступления в информационной сфере.“ *Amia.by*, žiūrėta 2025 m. gruodžio 17 d., 11, 12, 18 p., https://www.amia.by/book/umk/Kaf_rasl_prestypleniy/itsfera/project/DswMedia/tekstlekcii.pdf

120. Unit 42. „The Dilemma of AI: Malicious LLMs.“ *Palo Alto Networks – Unit 42*, žiūrėta 2025 m. gruodžio 17 d., https://unit42.paloaltonetworks.com/dilemma-of-ai-malicious-llms/

121. Abnormal Security. „Combating WormGPT.“ *Abnormal.ai,* žiūrėta 2025 m. gruodžio 17 d., https://abnormal.ai/blog/combating-wormgpt

122. Biometric Update. „Dark news from dark web: Deepfakers are getting their act together.“ *BiometricUpdate.com*, žiūrėta 2025 m. gruodžio 17 d https://www.biometricupdate.com/202105/dark-news-from-dark-web-%20deepfakers-are- getting-their-act-together

123. Lietuvos policija. „Vilniaus kriminalistų operacija: smogta „SIM box“ tinklui (vaizdo įrašas).“ *Policija.lrv.lt,* žiūrėta 2025 m. gruodžio 17 d

https://policija.lrv.lt/lt/naujienos/vilniaus-kriminalistu-operacija-smogta-sim-box-tinklui-video- %200hu5/

124. Lietuvos Respublikos prokuratūra. „Lietuvos prokurorai padėjo išardyti telefoninių sukčių tinklą Ukrainoje.“ *Prokuraturos.lt*, žiūrėta 2025 m. gruodžio 17 d., https://prokuraturos.lt/lt/lietuvos-prokurorai-padejo-isardyti-telefoniniu-sukciu-tinkla-ukrainoje/11892

PRIEDAI

Priedas Nr. 1

Ekspertų (specializuotų padalinių prokurorų) interviu klausimai

1. Kiek dažnai savo darbe susiduriate su sukčiavimu elektroninėje erdvėje? Kuo tokios bylos skiriasi nuo „tradicinių“ sukčiavimo bylų?
2. Kaip, Jūsų akimis, per pastaruosius 5-10 metų pasikeitė sukčiavimo schemos? Ką laikytumėte didžiausiu technologijų „indėliu“ į sukčiavimo mechaniką?
3. Kokius tipinius sukčiavimo elektroninėje erdvėje scenarijus dažniausiai matote? Kokios detalės ar aplinkybės Jums padeda jau pradžioje suprasti, su kokio tipo sukčiavimu turite reikalą (pvz. investicinis, fišingas, smišingas, kriptovaliutų, „romantiniai“ ir pan.)?
4. Ar matote pasikartojančių bruožų nukentėjusiųjų elgesyje ir pasakojimuose (amžius, skaitmeniniai įgūdžiai, tipinės klaidos, reakcija į apgaulę)? Ar, Jūsų nuomone, tai turėtų būti labiau sistemingai fiksuojama ir naudojama planuojant tyrimą?
5. Kaip vertinate dabar galiojančias metodines rekomendacijas dėl sukčiavimo elektroninėje erdvėje tyrimo? Kas jose realiai padeda darbe, o ko, Jūsų manymu, trūksta? Ar Jums užtektinai aiškiai jose atsispindi būtent skirtingi sukčiavimo būdai (fišingas, investicinis, telefoniniai skambučiai ir pan.), ar viskas labiau sudėta „į vieną krūvą“?
6. Ar, Jūsų nuomone, praktikoje būtų naudinga turėti labiau „suskirstytas“ rekomendacijas pagal atskirus sukčiavimo tipus (atskiri blokai fišingui, smišingui, investiciniam, kriptovaliutų sukčiavimui ir pan.)? Jeigu taip – kurioms sritims labiausiai jaustumėte tokio detalesnio išskyrimo poreikį?
7. Kokios informacijos ar duomenų sukčiavimo elektroninėje erdvėje bylose Jums dažniausiai trūksta (pvz., iš bankų, ryšio operatorių, platformų, kriptovaliutų keityklų)? Ar matote galimybę aiškiau apibrėžti, „ką konkrečiai verta rinkti“ pagal atskirą sukčiavimo modelį?
8. Kaip dažnai tokiose bylose tenka kreiptis į užsienio bankus, platformas, socialinius tinklus, kriptovaliutų keityklas ir pan.? Su kokiais didžiausiais sunkumais susiduriate (terminai, atsisakymai, formos, apskritai jokio atsakymo ir pan.)? Ar, Jūsų manymu, būtų prasminga kaupiant praktiką turėti tam tikrą „juodąjį sąrašą“ subjektų/jurisdikcijų, iš kurių realiai duomenų beveik neįmanoma gauti?
9. Kiek, Jūsų požiūriu, svarbu, kad tyrėjai ir prokurorai patys gerai suprastų technologinę pusę (e. bankininkystė, nuotolinė prieiga, kriptovaliutos, dirbtinio intelekto naudojimas)? Kokios kompetencijos Jums atrodo labiausiai reikalingos ir kur jų šiuo metu trūksta?

10. Jeigu reikėtų paprastai paaiškinti, kuo šiuolaikinio sukčiavimo elektroninėje erdvėje tyrimas skiriasi nuo sukčiavimo bylų prieš, tarkime, 10–15 metų, ką pasakytumėte?
11. Jūsų pasiūlymai.

Priedas Nr. 2

Eksperto (IT specialisto-programuotojo) interviu klausimai

1. Kaip, jūsų vertinimu, pastaraisiais metais kinta sukčiavimo elektroninėje erdvėje tendencijos technologiniu požiūriu (naudojami įrankiai, atakų mastas, automatizacija)?
2. Kokias šiuo metu matote ryškiausias technologines kryptis, kurios daro didžiausią įtaką sukčiavimo plitimui elektroninėje erdvėje?
3. Ar pastebite, kad sukčiavimo metodai tampa labiau individualizuoti ir pritaikyti konkretiems vartotojams? Jei taip, kokias technologijas tam pasitelkia sukčiai?
4. Jūsų nuomone, kurios prevencijos kryptys IT srityje šiuo metu yra veiksmingiausios kovojant su sukčiavimu elektroninėje erdvėje?
5. Kokį vaidmenį, jūsų vertinimu, sukčiavimo prevencijoje gali (ar jau pradeda) atlikti dirbtinis intelektas ir automatizuoti saugumo sprendimai?
6. Kokias pagrindines klaidas ar technologinius pažeidžiamumus, sukčiavimo kontekste, dažniausiai daro eiliniai vartotojai?
7. Kaip, jūsų manymu, ateityje turėtų keistis technologinė sukčiavimo prevencija, siekiant mažinti tokių nusikalstamų veikų mastą?

SANTRAUKA LIETUVIŲ KALBA

Atsižvelgiant į tai, kad visuomenės ir paslaugų skaitmenizavimas vis dažniau perkelia kasdienius veiksmus į elektroninę erdvę, technologiniai pokyčiai sudaro sąlygas sukčiavimui įgyti naujas formas. Apgaulės įgyvendinimas tampa greitesnis, masiškesnis ir sunkiau kontroliuojamas, o kartu ir sudėtingesnis tiriant. Sukčiavimo elektroninėje erdvėje tyrimą apsunkina šių nusikalstamų veikų tarptautinis pobūdis, kaltininkų tapatybės slėpimas, skaitmeninių pėdsakų laikinumas ir ribotos galimybės operatyviai gauti esminius duomenis. Dėl šių priežasčių dalis pradėtų tyrimų, atlikus visus įmanomus ir racionalius veiksmus, - sustabdomi, nenustačius įtariamojo asmens. Šiame magistro baigiamajame darbe siekiama atskleisti sukčiavimo kriminalistinės charakteristikos pokyčius technologinės raidos kontekste ir įvertinti jų reikšmę sukčiavimo elektroninėje erdvėje tyrimo organizavimui. Darbe analizuojami šiuolaikiniai sukčiavimo modeliai, jų realizavimo būdai ir su juo susijusi požymiai. Teoriniame lygmenyje nagrinėjama kriminalistikos ir sukčiavimo tyrimo metodikų istorinė raida, sukčiavimo teisinis reguliavimas, kriminalistinė charakteristika, išskiriant veikos dalyką, padarymo būdus, naudojamus įrankius ir priemones. Praktinėje darbo dalyje analizuojami ikiteisminio tyrimo pradėjimo ypatumai, tipinės tyrimo situacijos, tyrimo kryptys ir dažniausiai pasitaikančios kliūtys, vertinamas aukos ir kaltininko portretas kaip kriminalistinės charakteristikos sudedamieji elementai, taip pat aptariamos sukčiavimo elektroninėje erdvėje tendencijos ir prevencijos kryptys. Tyrimas grindžiamas teisės aktų ir teismų praktikos analize, mokslinės literatūros vertinimu, empirinių duomenų analize bei ekspertinių interviu įžvalgomis. Atlikus tyrimą nustatyta, kad technologijų įtakoje sukčiavimo kriminalistinė charakteristika kinta iš esmės: apgaulės mechanizmas ir pėdsakų susidarymo vieta vis dažniau persikelia į skaitmeninę erdvę, o nusikalstamos veikos vykdymas siejamas su nuotoline komunikacija, tarpinėmis paslaugomis ir anonimiškumą užtikrinančiomis priemonėmis. Tyrimas parodė, kad vien formali sukčiavimo sudėties požymių analizė ne visuomet leidžia pakankamai tiksliai suprasti veikos mechanizmą ir tyrimui reikšmingas aplinkybes, todėl kriminalistinės charakteristikos elementų taikymas turi esminę praktinę reikšmę planuojant pirminius procesinius veiksmus, nustatant tikėtinus duomenų šaltinius ir formuojant tyrimo versijas. Taip pat nustatyta, kad sukčiavimo elektroninėje erdvėje tyrimo rezultatyvumą labiausiai riboja ilgi duomenų gavimo terminai, tarptautinio bendradarbiavimo praktiniai barjerai, greitas lėšų judėjimas ir skaitmeninių pėdsakų laikinumas. Atsižvelgiant į tai, darbe pagrįstas poreikis tobulinti metodines rekomendacijas dėl sukčiavimo elektroninėje erdvėje tyrimo, jas labiau pritaikant prie skirtingų sukčiavimo veikimo modelių, aiškiau apibrėžiant reikšmingus duomenų šaltinius ir neatidėliotinų veiksmų seką, taip pat nuosekliai stiprinant prevencines priemones, orientuotas į ankstyvą apgaulės atpažinimą ir savalaikį reagavimą.

SANTRAUKA ANGLŲ KALBA

As the digitalisation of society and public and private services increasingly transfers everyday activities into the electronic environment, technological developments create conditions for fraud to assume new forms. The execution of deception becomes faster, more widespread and more difficult to control, and consequently more complex to investigate. The investigation of fraud committed in the electronic environment is hindered by the transnational nature of such criminal activity, the concealment of offenders' identities, the temporary nature of digital traces and limited possibilities to obtain essential data promptly. For these reasons, some initiated investigations, despite the performance of all possible and reasonable procedural actions, are suspended due to the failure to identify a suspect. This master's thesis aims to reveal changes in the criminalistic characteristics of fraud in the context of technological development and to assess their significance for the organisation of investigations into fraud committed in the electronic environment. The study analyses contemporary fraud models, their methods of implementation and the characteristics relevant to investigation. At the theoretical level, the historical development of criminalistics and fraud investigation methodologies is examined, along with the legal regulation of fraud and its criminalistic characteristics, distinguishing the object of the offence, methods of commission, tools and means employed. The practical part of the thesis analyses the specifics of initiating pre-trial investigations, typical investigative situations, investigative directions and the most common obstacles encountered in practice. The victim's and offender's profiles are assessed as constituent elements of criminalistic characteristics, and trends in fraud committed in the electronic environment as well as key directions of prevention are discussed. The research is based on the analysis of legal acts and case law, the evaluation of academic literature, the analysis of empirical data and insights obtained from expert interviews. The research findings demonstrate that technological development fundamentally alters the criminalistic characteristics of fraud. The mechanism of deception and the location of trace formation increasingly shift into the digital environment, while the commission of criminal acts is commonly associated with remote communication, intermediary services and anonymity-enhancing measures. The study shows that a solely formal analysis of the statutory elements of fraud does not always allow for a sufficiently precise understanding of the actual mechanism of the offence and the circumstances relevant to investigation. Consequently, the application of criminalistic characteristics plays a crucial practical role in planning initial procedural actions, identifying probable sources of data and formulating investigative versions. It was also established that the effectiveness of investigations into fraud in the electronic environment is primarily limited by lengthy data acquisition procedures, practical barriers to international cooperation, rapid movement of funds and the 140

transient nature of digital traces. In view of these findings, the thesis substantiates the need to improve methodological recommendations for investigating fraud in the electronic environment by adapting them more closely to different operational fraud models, more clearly defining relevant data sources and sequences of urgent actions, and consistently strengthening preventive measures focused on early detection of deception and timely response.