MYKOLO ROMERIO UNIVERSITETO
VIEŠOJO SAUGUMO AKADEMIJOS
TEISĖS IR POLICIJOS VEIKLOS KATEDRA

RASA PAŽĖRIENĖ

TEISĖS IR IKITEISMINIO PROCESO TYRIMO PROGRAMA

NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE ATSKLEIDIMO TEISINIAI IR PRAKTINIAI YPATUMAI

Magistro baigiamasis darbas

Darbo vadovė: prof. dr. Žaneta Navickienė

Kaunas, 2021

TURINYS

ĮVADAS

Tiriama problema. Šio darbo problema yra susijusi su nusikaltimų elektroninėje erdvėje atskleidimo teoriniais ir praktiniais ypatumais analizuojant nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso (toliau – BK)[1] 198, 198[1], 198[2] straipsniuose. XXX skyriuje yra įtvirtintos teisės normos, reglamentuojančios elektroninių duomenų ir informacinių sistemų saugumą, numatyta atsakomybė už jų pažeidimą. Tačiau teisinėje veikloje užkardomi ne visi nusikaltimai, siejami su elektronine erdve. Nusikaltimų elektroninėje erdvėje bruožas yra jų kvalifikavimas pagal nusikaltimų sutaptį su kitais tradiciniais nusikaltimais (pvz., vaiko išnaudojimas pornografijai (BK 162 straipsnis), netikros mokėjimo priemonės gaminimas (BK 214 straipsnis), autorystės pasisavinimas (BK 191 straipsnis), neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas (BK 215 straipsnis), sukčiavimas (BK 182 straipsnis) ir kt.).

Darbe analizuojamos BK 198, 198[1], 198[2] straipsniuose įtvirtintos teisės normos ir šių nusikaltimų atskleidimo ypatumai. Kitaip nei likusieji BK XXX skyriaus straipsniai, minėti straipsniai tarpusavyje susiję formalia nusikaltimų sudėtimi (šių nusikaltimų padarymo vieta laikoma ta, kurioje veikė nusikaltimą daręs asmuo), skiriasi jų tyrimų metodikos ir t. t. Taip pat dėl dažnai keliamo šių straipsnių tarpusavio santykio klausimo, kuris šių normų taikymą daro sudėtingesnį[2], darbe pasirenkami analizuoti būtent BK 198, 198[1], 198[2] straipsnių probleminiai aspektai.

Nusikaltimų elektroninėje erdvėje tyrimui būdingas sistemiškumas. Tokio pobūdžio veikų tyrimai yra labai sudėtingi, nes, norint tinkamai juos identifikuoti ir ištirti, turi būti naudojama daug skirtingų technologinių išteklių, reikalingos specialios žinios, tyrimo metodikos ir t. t. Kaip atskleidžia 2020 m. valstybinio audito ataskaita, 2016–2019 m. net 11 procentų elektroninių nusikaltimų ikiteisminių tyrimų atliko nespecializuoti pareigūnai, nors tyrimai yra priskirti specializuotų padalinių kompetencijai[3].

Taigi, galima teigti, kad šios srities specialistų trūksta, o nusikaltimų elektroninėje erdvėje ikiteisminius tyrimus atlieka neturintys pakankamai specialių žinių pareigūnai. Taip pat pažymėtina, kad 2020 m. Lietuvos ikiteisminio tyrimo įstaigose nusikaltimų, susijusių su elektroninių duomenų ir informacinių sistemų saugumu, užregistruota 431, tačiau iš jų ištirta tik 181[4], o tai reiškia, kad net daugiau nei pusė tokių nusikaltimų lieka neišaiškinti. Šie skaičiai parodo, kad elektroninių nusikaltimų tyrimo metu yra padaroma esminių klaidų, dėl kurių vėliau ištirti nusikaltimus yra sudėtinga. Viena iš tokių problemų yra reikšmingų tyrimui duomenų surinkimas ir jų ištyrimas, taip pat jų visumos

[1] Lietuvos Respublikos baudžiamasis kodeksas, TAR, žiūrėta 2021 m. sausio 5 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr.
[2] Renata Marcinauskaitė, *Nusikalstamos veikos elektroninėje erdvėje* (Vilnius: Registrų centras, 2019), 242.
[3] *Valstybinio audito ataskaita: ar veiksmingai kovojama su elektroniniais nusikaltimais, 2020 m. Nr. VAE-7,* 4.
[4] *Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos: Duomenys apie nusikalstamumą Lietuvos Respublikoje per 2020 m. sausio-gruodžio mėn.2020 m*. Nr. 24 St.-52.

įvertinimas. Svarbu kaip įmanoma greičiau apklausti liudytojus, nustatyti ir apklausti įtariamuosius, atlikti kratas ir ištirti reikšmingus tyrimui duomenis bei daiktus[5]. Jais laikomi kompiuteriai, serverių įrangos, mobilieji telefonai, laikmenos, atminties kortelės, išoriniai kietieji diskai ir kt. To laiku neatlikus ir nepasirinkus tinkamų taktinių ikiteisminio tyrimo veiksmų, pavėluotai gauta informacija gali būti netiksli ir nenaudinga[6].

Dar viena problema, su kuria susiduriama tiriant tokio pobūdžio nusikaltimus, yra nusikaltimo vietos nustatymas. Nusikaltimai elektroninėje erdvėje yra išskirtiniai tuo, kad gali būti padaryti kaltininkui esant dideliu atstumu nuo įrenginių, kuriems padaroma žala, o nusikaltimo padarymo vieta bei žalingų padarinių kilimo vieta dažnai nesutampa[7]. Visa tai tik dar labiau apsunkina kaltininko nusikalstamų veiksmų kvalifikavimą.

Darbe siekiama išnagrinėti problemas, su kuriomis susiduria ikiteisminio tyrimo institucijos, tirdamos nusikaltimus elektroninėje erdvėje, t. y. BK 198, 198[1], 198[2] straipsniuose numatytus nusikaltimus: kas lemia tokį mažą šių nusikaltimų ištyrimo lygį? Ar tiriant tokio pobūdžio nusikaltimus tinkamai identifikuojami duomenys, reikšmingi bylos tyrimui? Kokių pagrindinių sunkumų ir problemų rinkdami informaciją patiria ikiteisminio tyrimo pareigūnai? Ar turima šių nusikaltimų tyrimų metodika yra pakankama ir gali padėti tiriantiems šiuos nusikaltimus?

Baigiamojo darbo aktualumas. Kiekvienas laikotarpis ir karta turi tam tikrų savitų bruožų ir išskirtinumų, lyginant su ankstesniaisiais. Kalbant apie Y ir Z kartas neabejotinai išskirtume tobulėjančią technologijų raidą ir prisitaikymą prie naujųjų technologijų. Turbūt nė vienas šiuometiniame pasaulyje neįsivaizduojame savo gyvenimo be kompiuterių, telefonų ar interneto. Internetu galime dirbti, užsisakyti prekių ir paslaugų, plėtoti verslą, atlikti mokėjimus ar tiesiog bendrauti. Kiekvienas technologinis patobulėjimas turi ir savo „tamsiąją pusę“, kuri atveria galimybes ir nišas asmenims padaryti nusikaltimus, t. y. įgyvendinti savo neteisėtus tikslus. Kaip sparčiai tobulėja ir auga technologijos, taip pat sparčiai auga ir nusikaltimų elektroninėje erdvėje skaičius. Nusikaltimai elektroninėje erdvėje – tai nuolat auganti visuomenės saugumo problema. Žmonės turi skirtingas tapatybes realiame pasaulyje ir kibernetinėje erdvėje[8]. Asmenys, darantys tokius nusikaltimus, tikisi likti neidentifikuoti, nes gali lengvai pakeisti savo virtualią asmenybę.

Tokiems nusikaltimams būdingas itin didelis latentiškumas: dauguma nusikaltimų, padarytų elektroninėje erdvėje, taip ir lieka neišaiškinti[9]. Skaitmeninės ekonomikos ir visuomenės indeksas

[5] *Supra note* 3, 39.
[6] Lietuvos Aukščiausiojo Teismo 2018 m. lapkričio 6 d. nutartis, priimta baudžiamojoje byloje Nr. 2K-293-788/2018, eteismai, žiūrėta 2021 m. sausio 30 d., https://eteismai.lt/byla/278248162686377/2K-293-788/2018?word=vilius%20sutkus.
[7] Albertas Milinis, Edita Gruodytė, Aurelijus Gutauskas ir kt., *Lietuvos baudžiamoji teisė specialioji dalis, pirmoji knyga* (Vilnius: 2013), 456.
[8] Darius Štitilis, *Elektroniniai nusikaltimai* (Vilnius: Mykolo Romerio universitetas, 2011), 23.
[9] *Supra note* 3, 8-9.

(DESI) rodo, kad didelė dalis Lietuvos gyventojų naudojasi internetu, o kiekvienais metais šie skaičiai auga, t. y. 2017 m. internetu naudojosi 75 proc. šalies gyventojų, 2018 m. – 78 proc., o 2019 m. – 81 proc.[10]

Dalijimasis nuotraukomis internete atveria galimybes klestėti vaikų pornografijai, kaip ir elektroninė bankininkystė yra patogi, tačiau ji sudaro palankias sąlygas sukčiauti. Taip pat telefonas ar el. paštas gali būti naudojami priekabiavimui ar persekiojimui. 2020 m. pandemijos laikotarpiu dėl koronaviruso žmonės daugiau laiko praleidžia namuose, dirba nuotoliniu būdu, tad daugumai verslų persikeliant į elektroninę erdvę tokio pobūdžio nusikaltimų skaičius tik dar labiau išaugo[11]. Karantino metu daugiau nei penktadalis Lietuvos gyventojų pradėjo daugiau pirkti internetu nei iki tol[12].

Kaip rodo naujausia Europolo ataskaita, asmenys elektroninėje erdvėje pandemijos laikotarpiu pritaiko žinomas sukčiavimo schemas, kurios apima įvairių tipų pritaikytas sukčiavimų schemų versijas[13]. Šios pandemijos metu vienas ryškiausių nusikaltimų elektroninėje erdvėje per pastaruosius 10 metų buvo įvykdyta neteisėta prieiga prie „CityBee“ bendrovės duomenų. Daugiau nei 110 tūkstančių klientų asmens duomenų buvo nutekinti[14]. Taigi, akivaizdu, kad nusikaltimai elektroninėje erdvėje yra opi visuomenės problema. Elektroninė erdvė suteikia naujų galimybių daryti nusikaltimus, sudaro sąlygas naujiems nusikaltimo būdams atsirasti ir vykdyti naujus, iki tol nežinomus teisinėje praktikoje nusikaltimus[15].

Todėl svarbu ištirti problemas, susijusias su nusikaltimų elektroninėje erdvėje samprata, išanalizuoti šių nusikaltimų tyrimo ypatumus bei tokių nusikaltimų rūšių užkardymą ateityje. Taip pat aktualu išsiaiškinti, kokie pagrindiniai tyrimo veiksmai yra atliekami tiriant tokio pobūdžio nusikaltimus. Išanalizavus ir susisteminus informaciją darbas padėtų lengviau atskirti ir suprasti nusikaltimų, padarytų elektroninėje erdvėje, ypatumus ir svarbą, tuo pačiu palengvinant teisėsaugos institucijų darbą tiriant tokio pobūdžio nusikaltimus. Taigi, šiuo požiūriu darbe galime identifikuoti naujausios kriminalistikos metodikos tiriant minėtus nusikaltimus dimensiją. Darbo autorė kartu su prof. dr. Ž. Navickiene MRU VSA organizuotoje metinėje tarptautinėje mokslinėje konferencijoje pristatė mokslinį pranešimą tema „Lyderystės svarba tiriant kibernetinius nusikaltimus (angl. „Importance of leadership in investigating cybercrime“).

---

[10] *Supra note* 3, 17.

[11] *Internet organized crime threat assessment* (OCTA 2020, Europol, European Union Agency for Law Enforcement Cooperation: 2020), 13.

[12] „Karantinas pakeitė vartotojų įpročius: beveik penktadalis internetu pirks daugiau“, Verslo žinios, žiūrėta 2021 m. vasario 15 d., https://www.vz.lt/versli-lietuva/2020/06/22/karantinas-pakeite-vartotoju-iprocius-beveik-penktadalis-internetu-pirks-daugiau.

[13] „How criminals profit from the covid-19 pandemic“, Europol, žiūrėta 2021 m. vasario 4 d., https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic.

[14] „Policija pradėjo ikiteisminį tyrimą dėl bendrovės citybee klientų pavogtų duomenų“, Policija, žiūrėta 2021 m. vasario 16 d., https://policija.lrv.lt/lt/naujienos/policija-pradejo-ikiteismini-tyrima-del-bendroves-city-bee-klientu-pavogtu-duomenu.

[15] Darius Štitilis ir kt., *Interneto ir technologijų teisė* (Vilnius: Registrų centras, 2016), 402.

Baigiamojo darbo mokslinis naujumas ir tiriamos problemos ištyrimo lygis. Šiame darbe analizuojama Lietuvos teisės mokslinė doktrina ir įstatymai, aktualūs būtent Lietuvai, tačiau skiriamas nemažas dėmesys ir užsienio bei nacionalinės teisės ir mokslo šaltiniams. Temos naujumą lemia tai, kad vis daugėja tokio pobūdžio nusikaltimų, proporcingai didėja ir kovos priemonių su jomis bei naujų nusikaltimų padarymo būdų[16]. 2020 m. liepos 16 d. pateikta valstybinio audito ataskaita, kurioje nagrinėti nusikaltimų elektroninėje erdvėje prevencijos ir ištyrimo sistemos klausimai. Audito ataskaita atskleidė daug teisinės sistemos spragų, taip pat nustatyta, kad skiriamas per mažas dėmesys nusikaltimams elektroninėje erdvėje ir šių nusikaltimų skaičius vis auga[17]. Taigi, akivaizdu, kad dabartinė situacija netenkina nei vartotojo, nei valstybės ar įgaliotų jos asmenų veikti užkardant tokius nusikaltimus, vis dar ieškoma tinkamų priemonių ir sprendimo būdų kovai prieš juos. Nusikaltimų, padarytų elektroninėje erdvėje, tyrimo problematika Lietuvoje yra gan plačiai nagrinėjama. Tačiau, lyginant su kai kuriomis kitomis temomis, laikams keičiantis, ieškant naujų taktinių tyrimo veiksmų ir būdų kai kurie šaltiniai praranda svarbą. Be to, naujumą lemia ir tai, kad, tiriant nusikaltimus elektroninėje erdvėje, labai svarbi tyrėjo lyderystė: gebėjimas įvertinti situaciją dėl žinių poreikio, motyvacija domėtis šių nusikaltimų tyrimo tendencijomis, tinkamas tyrimo planavimas bei veiksmų koordinavimas.

Šią temą tam tikrais aspektais Lietuvoje nagrinėjo šie autoriai: D. Štitilis[18], M. Kiškis[19], R. Marcinauskaitė[20], P. Pakutinskas[21] ir kt. R. Marcinauskaitė yra parašiusi disertaciją, monografiją ir kelis mokslinius straipsnius apie nusikaltimus elektroninėje erdvėje, kuriuose bandė spręsti BK XXX skyriaus straipsnių normų konkurencijos klausimus. D. Štitilio 2002 m. disertacijoje „Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos“ ir kituose jo leidiniuose daugiausiai dėmesio skiriama bendriems tokių nusikaltimų atsakomybės problematikos aspektams. P. Pakutinskas, D. Štitilis, M. Laurinaitis ir I. Dauparaitė 2011 m. išleido vadovėlį „Tapatybės vagystė elektroninėje erdvėje“, kuriame pagrindinis dėmesys skiriamas teisinio reguliavimo ir prevencijos klausimams, susijusiems su tapatybės vagyste elektroninėje erdvėje. M.

[16] Jonathan Clough, *Data Theft? Cybercrime and the Increasing Criminalization of Access to Data* (Criminal Law Forum: 2011), 150.
[17] *Supra note* 3, 7.
[18] Darius Štitilis, *Supra note* 8.
[19] Darius Štitilis, ir kt. *Supra note* 15.
[20] Pagrindinis šaltinis: Renata Marcinauskaitė, „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai)“ (daktaro disertacija, Mykolo Romerio universitetas, 2013), žiūrėta 2021 m. sausio 5 d., https://repository.mruni.eu/bitstream/handle/007/15957/Disertacija_Marcinauskait%c4%97.pdf?sequence=2&isAllowed=y. Darbe buvo analizuojami ir kiti šios autorės darbai, kurie susiję su nagrinėjama tema: Renata Marcinauskaitė, *Nusikalstamos veikos elektroninėje erdvėje* (Vilnius: Registrų centras, 2019).
[21] Darius Štitilis ir kt., *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai* (Vilnius: Justitia, 2011).

Kiškis, T. Limba ir kiti autoriai 2016 m. vadovėlyje „Interneto ir technologijų teisė“ pagrindinį dėmesį skyrė asmens duomenų apsaugai, asmens identifikavimui ir kibernetiniam saugumui.

Užsienio autoriai atskirais aspektais taip pat yra nagrinėję nusikaltimus elektroninėje erdvėje. Nusikaltimų elektroninėje erdvėje, jų reguliavimo bei ikiteisminio tyrimo klausimus darbuose nagrinėjo J. Clough[22], Todd G. Shipley, Art Browker[23], M. Sheward [24], John Ashcroft[25] ir kiti. Terorizmo problematiką kibernetinėje erdvėje ir pagrindinius nusikaltimų elektroninėje erdvėje ikiteisminio tyrimo metodikos ypatumus nagrinėjo R. Moore[26], M. Talib, V. Sekgwathe [27] ir kiti. Šiame darbe daugiausiai analizuojama Lietuvos Respublikos nusikaltimų elektroninėje erdvėje tyrimo bei teismų praktikos ypatumai. Tačiau atsižvelgiant į tai, kad šie nusikaltimai yra išskirtiniai savo globaliu veikimu (kai asmuo daro nusikaltimą vienoje valstybėje, tačiau žalingi padariniai atsiranda kitoje), daug dėmesio skiriama ir užsienio šaltiniams bei jų tyrimo metodikai.

Nėra parašyto mokslinio darbo, kuris apimtų tiek teorinius, tiek praktinius nusikaltimų elektroninėje erdvėje tyrimo ypatumus. Darbe surinkta naujausia literatūra ir teismų praktika, susijusi su nusikaltimų elektroninėje erdvėje samprata, teisiniu reglamentavimu ir tyrimo metodika.

Baigiamojo darbo reikšmė. Darbas reikšmingas tuo, kad Lietuvoje mažai autorių nagrinėjo šią temą praktiniu aspektu, skirdami dėmesio tiek teoriniams, tiek pagrindiniams kriminalistikos aspektams, susijusiems su nusikaltimais elektroninėje erdvėje detaliau nagrinėjant BK 198, 198^1, 198^2 straipsnių taikymo sritį. O tai yra aktualu, nes tik pasirinkus tinkamus taktinius tyrimo veiksmus galima pasiekti sėkmingą ir teisingą bylos baigtį. Taigi, atliktas tyrimas gali būti naudingas tiek studentams, studijuojantiems kriminalistiką ir atskiras nusikaltimų rūšis bei jų tyrimą, tiek ikiteisminio tyrimo tyrėjams, tiek mokslininkams pasinaudojant susisteminta informacija apie nusikaltimus, susijusius su elektroninių duomenų ir informacinių sistemų saugumu. Šis baigiamasis darbas taip pat galėtų padėti teisę taikantiems subjektams geriau pažvelgti į tokio pobūdžio nusikaltimų tyrimo spragas ir tiriant nusikaltimus elektroninėje erdvėje vengti pagrindinių šiame darbe identifikuotų problemų bei klaidų.

Tyrimo tikslas – atskleisti nusikaltimų, padarytų elektroninėje erdvėje, tyrimo metodikos probleminius aspektus ir pateikti siūlymus dėl tyrimo tobulinimo.

---

[22] Jonathan Clough, *Principles of cybercrime* (Cambridge university press: 2011).
[23] Art Browker, Todd G. Shipley, *Investigating internet crimes* (Wyman Street, Waltham, MA 02451,USA, 2014), žiūrėta 2021 m. sausio 15 d., http://web.a.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/ZTAwMHh3d19fNTAzNTkyX19BTg2?sid=bc8e17ea-299d-4fbe-ab49-98f8508ced2a@sessionmgr4008&vid=6&format=EB&rid=1.
[24] Mike Sheward, *Hands-on incident responce and digital forensic* (United Kingdom, 2018).
[25] John Ashcroft, *Electronic crime scene investigation: a guide for first responders* (Washington, 2001).
[26] Robert Moore, *Search and seizure of digital evidence,* (New York, 2005).
[27] Mohammad Talib, Virginiah Sekgwathe, „Cyber forensics: computer security and incident response“, ISSN: 2220-9085, International journal, žiūrėta 2021 m. sausio 26 d., https://www.academia.edu/8332048/CYBER_FORENSICS_COMPUTER_SECURITY_AND_INCIDENTRESPONSE?auto=download&email_work_card=download-paper.

Uždaviniai.

1. Išsiaiškinti nusikaltimų elektroninėje erdvėje sampratą, rūšis bei atsakomybės už juos teisinį reglamentavimą.
2. Atskleisti pagrindinius nusikaltimų elektroninėje erdvėje, numatytų BK 198, 198^1, 198^2 straipsniuose, tyrimo aspektus per kriminalistinės charakteristikos prizmę.
3. Išanalizuoti nusikaltimų elektroninėje erdvėje BK 198, 198^1, 198^2 straipsnių ikiteisminio tyrimo ypatumus.
4. Išanalizuoti BK 198, 198^1, 198^2 straipsnių probleminius aspektus, kylančius teismų praktikoje, ir pateikti problemų sprendimo būdus ir rekomendacijas.

Tyrimo objektas. Nusikaltimų elektroninėje erdvėje, numatytų BK 198, 198^1, 198^2 straipsniuose, atskleidimo teoriniai ir praktiniai ypatumai Lietuvos bei užsienio baudžiamojoje teisėje.

Tyrimo metodika. Šiame darbe naudojami teoriniai ir empirinis metodai.

Teoriniai metodai: *analizės* metodas, kuris skirtas mokslinės, metodinės literatūros bei teismų praktikos analizei. Naudojant *abstrakcijos* metodą nagrinėti nusikaltimų elektroninėje erdvėje kriminalistiniai ir praktiniai aspektai. Lyginamasis metodas buvo naudojamas atskleidžiant BK 198, 198^1, 198^2 straipsnių ir kitų BK numatytų straipsnių sąsajas. *Apibendrinimo* metodu susisteminta, išanalizuota informacija ir pateiktos išvados.

Empirinis metodas: *dokumentų analizė* naudojama teismų praktikai ištirti.

Baigiamojo darbo struktūra. Magistro baigiamąjį darbą sudaro 4 skyriai. Pirmas skyrius skirtas atskleisti nusikaltimų elektroninėje erdvėje sampratą, rūšis ir teisinį reglamentavimą. Šiame skyriuje pateikiama išsami elektroninių nusikaltimų sampratos analizė, lyginami įvairių mokslininkų šaltiniai, išskiriamos nusikaltimų elektroninėje erdvėje rūšys, įtvirtintos BK XXX skyriuje ir 2001 m. Europos Sąjungos konvencijoje, bei teisinis reglamentavimas Lietuvoje. Antrame skyriuje kalbama apie nusikaltimų, padarytų elektroninėje erdvėje, kriminalistinius aspektus ir kriminalistinę charakteristiką. Išskiriami BK 198, 198^1, 198^2 straipsniai ir analizuojama šių nusikaltimų kriminalistinė charakteristika. Trečias skyrius skirtas nusikaltimų elektroninėje erdvėje praktiniams ypatumams atskleisti. Ketvirtame skyriuje analizuojami teismų praktikos ypatumai taikant BK 198, 198^1, 198^2 straipsnius.

Ginamieji teiginiai. Nusikaltimai elektroninėje erdvėje yra pavojingi ir keliantys daug iššūkių teisėsaugos institucijoms, tačiau esama šių nusikaltimų tyrimo metodika ir ištekliai nėra pakankami norint atskleisti ir ištirti tokio pobūdžio nusikaltimus.

1. NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE SAMPRATA, RŪŠYS IR TEISINIS REGLAMENTAVIMAS

1.1. Nusikaltimų elektroninėje erdvėje samprata

Analizuojant nusikaltimų elektroninėje erdvėje (angl. *cybercrime*) sampratą svarbu paminėti, kad teisinėje doktrinoje nėra bendro apibrėžimo ir bendros nuomonės, kas konkrečiai laikoma nusikaltimais elektroninėje erdvėje. Nusikaltimų elektroninėje erdvėje samprata susideda iš dviejų junginių: tai *elektroninė erdvė* ir *nusikaltimai*. Kalbant apie elektroninę erdvę būtina atkreipti dėmesį į tai, kad „elektroninė erdvė iš esmės neturi nei fizinių, nei teisinių sienų, nėra jokios „centrinės valdžios“, kuri valdytų informacijos kaitą internete. Elektroninės informacijos erdvė (angl. *cyber space*) – „globaliai, integruota, viešai ir visuotinai prieinama kompiuterių tinklų sistema, kuria naudojantis keičiamasi informacija (forumai, tinklaraščiai, finansiniai atsiskaitymai, sudaromi sandoriai)“[28]. Teisės mokslų doktrinoje nurodyta, kad „elektroninė erdvė – tai ne kas kita, kaip mūsų visuomenės atspindys; tai puiki terpė ne tik teisėtiems tikslams pasiekti, bet ir pavojingiems, priešingiems teisės normoms veiksmams atlikti bei juos atliekančių subjektų išradingumui parodyti: efektyvūs veiksmai (informacijos siuntimas, gavimas, saugojimas, apdorojimas), atliekami elektroninėje terpėje naudojantis informacinėmis technologijomis pačiais įvairiausiais paprastam elektroninės erdvės naudotojui dažniausiai ne visada suprantamais ir pastebimais būdais“[29]. Atsižvelgiant į tai, kad sunku nustatyti elektroninės erdvės ribas, jos negalima apčiuopti ar pamatyti, apibrėžti nusikaltimų elektroninėje erdvėje sampratą yra sudėtinga.

2001 m. priėmus Europos Tarybos Budapešto konvenciją dėl elektroninių nusikaltimų[30] (toliau – ir Konvencija) praktikoje pradėtas vartoti nusikaltimų elektroninėje erdvėje terminas, nors iki tol dažniau buvo minima kompiuterinio nusikaltimo sąvoka. Analogiškai kaip ir su nusikaltimų elektroninėje erdvėje atveju kompiuterinio nusikaltimo terminas sudarytas iš dviejų junginių (t. y. *kompiuteris* ir *nusikaltimas*). Literatūroje[31] kompiuteris apibrėžiamas kaip automatinis, elektroninis prietaisas, skirtas atlikti matematines ar logines operacijas ir vadinamas aukštųjų technologijų įrenginiu. 1960 m. pradžioje JAV spaudoje pirmą kartą pasirodė terminas „kompiuterinis nusikaltimas“, kai buvo išaiškinti pirmieji nusikaltimai, atlikti pasitelkus elektroninius automatizuoto skaičiavimo įrenginius[32]. Vienas iš pirmųjų, susidomėjęs šia problema JAV, buvo Donnas Parkeris, kuris pateikė kompiuterinio nusikaltimo sąvoką: „Visos tyčinės veikos, vienu ar kitu būdu susijusios

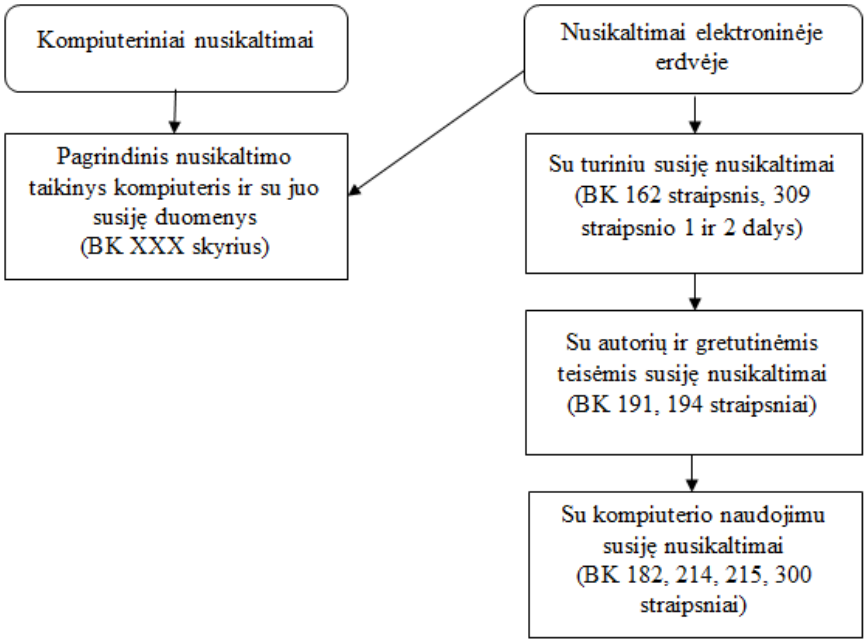
[28]Darius Štitilis, ir kt. *Supra note* 15, 20.
[29] Darius Štitilis ir kt., *Supra note*, 21, 34.
[30] Konvencija dėl elektroninių nusikaltimų, TAR, žiūrėta 2021 m. sausio 10 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195.
[31] Anthony Reyes, Richard Brittson, James Steel ir kt., *Cyber Crime Investigations : Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, (*Syngress publishing Rocland: 2007), 33.
[32] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Kriminalistika: taktika ir metodika* (Vilnius: 2013), 629.

su kompiuteriais, dėl kurių nukentėjusysis patyrė ar galėjo patirti žalą, o nusikaltimo subjektas turėjo ar galėjo gauti iš to naudos.“ Tačiau šis apibrėžimas neapima nusikaltimų, padarytų dėl neatsargumo arba nesiekiant naudos[33]. Manoma, kad kompiuterinio nusikaltimo sąvoka (angl. *computer crime*) yra siauresnė, lyginant su elektroniniais nusikaltimais, nes nusikaltimai elektroninėje erdvėje yra siejami ir su kompiuterine ar programine įranga, internetu, turiniu, skaitmenine įranga ar duomenimis, kai tuo tarpu kompiuterinių nusikaltimų sampratos turinio prasme svarbiausią vaidmenį nusikaltime vaidina kompiuterinė sistema ir su ja susiję įrenginiai. Svarbu paminėti, kad kelis dešimtmečius aktyviai buvo naudojamos ne tik kompiuterinių ar elektroninių nusikaltimų, bet ir su kompiuteriais susijusių nusikaltimų (angl. *computer-related crime*), aukštų technologijų (angl. *high-tech crime*) ir kitos sąvokos. Tačiau atsižvelgiant į tai, kad kompiuterinių nusikaltimų ir nusikaltimų elektroninėje erdvėje sąvokos labiausiai paplitusios literatūroje ir turi daugiausiai panašumų, plačiau bus aptariamos tik jos.

Nusikaltimams elektroninėje erdvėje priskiriami nusikaltimai, padaryti naudojant kompiuterius ar išmaniuosius elektroninius įrenginius, siekiant neteisėtai perimti, sugadinti, sunaikinti, pašalinti duomenis, sutrikdyti ar nutraukti informacinės sistemos darbą, kai kompiuterinė ar programinė įranga yra nusikaltimo objektas arba įrankis, ir kitos neteisėtos veikos, susijusios su skaitmenine informacija ir jos apdorojimu[34]. Kaip pavyzdį autoriai išskyrė situaciją, kai kompiuteris ar kitas elektroninis įrenginys gali būti ir nusikaltimo objektas, t. y. jis gali būti pavogtas ar piktybiškai sugadintas ir juo gali būti įsilaužiama į informacinę sistemą ar internetinį portalą, ištrinami ar sugadinami naudotojų duomenys.

Nusikaltimai elektroninėje erdvėje – tai ir pornografijos platinimas, informacijos ar asmeninės informacijos vagystė, autorinių teisių pažeidimus ir taip toliau[35]. Kai tuo tarpu kompiuterinio nusikaltimo samprata apima tik nusikaltimus, kuriais tiesiogiai kėsinamasi į kompiuterį ir su juo susijusius įrenginius. Darbo autorė atkreipia dėmesį, kad sudarydama kompiuterinių ir nusikaltimų elektroninėje erdvėje sampratų palyginamąją schemą (žiūrėti 1 pav.) rėmėsi siaurąja kompiuterinių nusikaltimų apibrėžtimi.

[33] Anthony Reyes, Richard Brittson, James Steel ir kt., *Supra note*, 31, 25.
[34] Nikolaj Goranin, Dalius Mažeika, *Nusikaltimai elektroninėje erdvėje ir jų tyrimų metodikos*, (Kaunas: 2011), 16, žiūrėta 2021 m. sausio 20 d., http://www.esparama.lt/documents/10157/490675/Nusikaltimai_elektronineje_erdveje_ir_ju_tyrimo_metodikos.pdf.
[35] Nikolaj Goranin, Dalius Mažeika, Ibid, 9.



1 pav. Kompiuterinių nusikaltimų ir nusikaltimų elektroninėje erdvėje sampratų lyginamoji schema (sudaryta autorės).

Svarbu pažymėti, kad daugelio autorių kompiuterinio nusikaltimo samprata suvokiama plačiai ir išskiriama į kategorijas. Tyrinėtojas Majid Yar[36] ir mokslininkas G. E. Higgins[37] taip pat išskiria kompiuterinius nusikaltimus ir nusikaltimus, padarytus elektroninėje erdvėje. G. E. Higgins kompiuterinius nusikaltimus apibūdina kaip veikas, kurioms įvykdyti naudojamas kompiuteris ir kurios uždraustos baudžiamųjų įstatymų. Kompiuteriniai nusikaltimai gali būti skirstomi į tris grupes:

1. kai kompiuteris panaudojamas kaip nusikaltimo įvykdymo įrankis (pvz., neteisėtas garso failų siuntimasis);
2. kai kompiuteris yra nusikaltimo objektas (pvz., neteisėtos prieigos atveju);
3. kai kompiuteris naudojamas kaip nelegalaus turinio saugykla (pvz., saugoti medžiagai su vaikų pornografija)[38].

Mokslininko nuomone, kompiuteris gali būti naudojamas ir kaip įrankis tokio pobūdžio nusikaltimams įvykdyti, ir kaip nusikaltimo objektas, ir kaip saugykla. Toks skirstymas atveria platesnį požiūrį į kompiuterinių nusikaltimų sampratą ir yra panašiausias į nusikaltimų elektroninėje erdvėje sampratos turinį. Pavyzdžiui, D. Štitilis, savo disertacijoje išanalizavęs daugelio mokslininkų darbus, rašė, kad iš esmės kompiuteriniai nusikaltimai ir nusikaltimai elektroninėje erdvėje beveik nesiskiria. Tačiau šis autorius pažymi, kad „kai kurios veikos, priskiriamos nusikaltimams

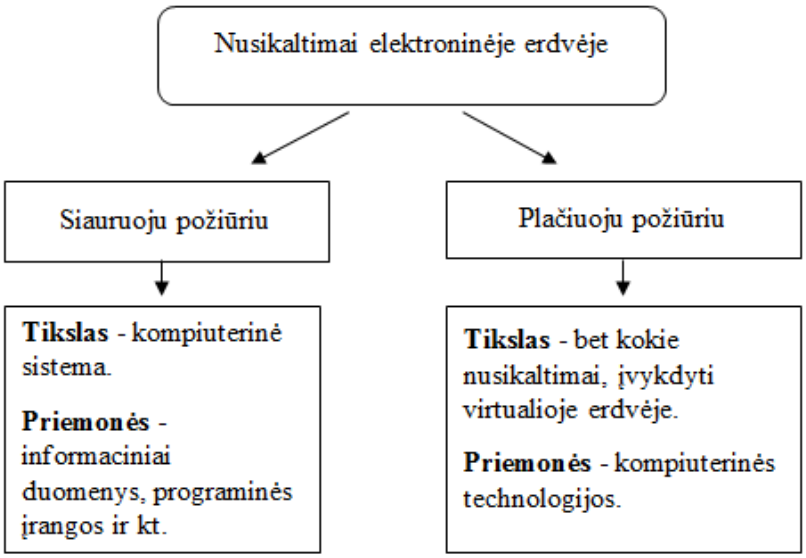
[36] Majid Yar „Cybercrime and society “, žiūrėta 2021 m. sausio 11 d., https://books.google.lt/books/about/Cybercrime_and_Society.html?id=Ye4QAAAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false.
[37] G. E. Higgins, *Cybercrime: An Introduction to an Emerging Phenomen. Library of Congress Cataloging* (2010), 2.
[38] Darius Štitilis, *Supra note*, 8, 7.

elektroninėje erdvėje, tokios kaip vandalizmas ar terorizmas, literatūroje nelaikomos nusikaltimais, susijusiais su kompiuteriais“[39]. Trumpai tariant, kompiuteriniai nusikaltimai ir nusikaltimai elektroninėje erdvėje turėtų būti sujungti į bendrą visumą ir įvardijami kaip nusikaltimai elektroninėje erdvėje. Toks aiškinimas yra paprastesnis ir apima didesnį tokio pobūdžio nusikaltimų spektrą.

Tokios pat nuomonės yra ir kai kurie kiti mokslininkai. Pasak J. Clough[40], nusikaltimų elektroninėje erdvėje sąvoka yra teisingiausia ir išskiriamos kelios to priežastys. Pirmiausia, šių nusikaltimų sąvoka dažniausiai vartojama literatūroje. Be to, tapo įprasta ir lengva ją vartoti ir pritaikyti ne vien tik prie nusikaltimų, padarytų naudojantis kompiuteriu. Taip pat nusikaltimų elektroninėje erdvėje sąvokoje pabrėžiama tinklų svarba – kompiuteriai. Be to, anot autoriaus, svarbiausia, kad tai terminas, priimtas Europos tarybos konvencijoje dėl elektroninių nusikaltimų. Galima sutikti su profesoriaus nuomone, kad labai svarbi Europos Konvencija, kurioje ši sąvoka įtvirtinta kaip tinkamiausia, nes ši Konvencija laikoma pamatine tarp nusikaltimų elektroninėje erdvėje teisės aktų. Ir, be to, Konvencijoje išskiriamos kai kurios nusikaltimų elektroninėje erdvėje rūšys labai diskutuotinos: pavyzdžiui, ar jos galėtų būti kompiuterinių nusikaltimų sampratos turinio dalimi?

Nusikaltimai elektroninėje erdvėje gali būti suvokiami ir siauruoju, ir plačiuoju požiūriu. Tokia apibrėžtis yra plačiai paplitusi mokslinėje literatūroje: siauruoju požiūriu – kai kompiuterinė sistema yra nusikaltimo tikslas, o joje esantiems duomenims daroma įtaka tikslui pasiekti[41]. O štai plačiuoju požiūriu nusikaltimai elektroninėje erdvėje suprantami kaip „bet kokie nusikaltimai, kuriems įvykdyti vienaip ar kitaip buvo panaudotos kompiuterinės technologijos, o nusikaltimo faktui įrodyti turi būti taikomos specifinės elektroninių nusikaltimų tyrimo priemonės“[42]. Tad galima teigti, kad siaurasis požiūris yra artimesnis kompiuterinio nusikaltimo sampratai, o plačiuoju nusikaltimų elektroninėje erdvėje požiūriu kompiuteris gali būti naudojamas kaip tikslas ir kaip įrankis tam tikslui pasiekti (žiūrėti 2 pav.).

[39] Darius Štitilis, „Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos“ (daktaro disertacija, Lietuvos teisės universitetas, 2002), 39.
[40] Jonathan Clough, *Supra note*, 22, 9.
[41] Nikolaj Goranin, Dalius Mažeika, *Supra note*, 34, 9.
[42] Nikolaj Goranin, Dalius Mažeika *Supra note*, 34, 9.



2 pav. Nusikaltimų elektroninėje erdvėje sąvokos apibrėžtis remiantis siauruoju ir plačiuoju požiūriais (sudaryta autorės).

Dar išsamesnį nusikaltimų elektroninėje erdvėje grupavimą yra pateikęs JAV teisingumo departamentas[43], apibrėžęs trijų etapų klasifikaciją, kuri sėkmingai naudojama Australijoje, Kanadoje ir Jungtinėje Karalystėje. Nusikaltimai elektroninėje erdvėje – tai:

1. Nusikaltimai, kurių objektas yra kompiuteris ar kompiuterių tinklas, (pvz., įsilaužimai, kenkėjiškos programos, „DoS“ atakos).
2. Nusikaltimai, kai kompiuteris yra įrankis padarant nusikalstamą veiką, (pvz., vaikų pornografija, persekiojimas, sukčiavimas, autorių teisių pažeidimas).
3. Nusikaltimai, kai kompiuterio naudojimas yra atsitiktinis nusikaltimo įvykdymui, tačiau jame paliekami įkalčiai ir galima rasti įrodymų. Pavyzdžiui, nužudymu įtariamo asmens kompiuteryje rasti adresai ar telefono įrašai. Tokiais atvejais kompiuteris nėra reikšmingai susijęs su nusikaltimu, tačiau jame galima rasti bylai reikšmingų duomenų.

Galima teigti, kad Teisingumo departamento atstovų nuomonė ir klasifikacija labai panaši į mokslininko Goerge E. Higgins ir atskleidžia nusikaltimų elektroninėje erdvėje sampratos turinį, kuris apima kompiuterio ir kaip nusikaltimo objekto, ir kaip įrankio kitam nusikaltimui atlikti, ir kaip įkalčių saugyklos panaudojimą. Tačiau svarbu pažymėti, kad kiekviena valstybė turi teisę spręsti ir naudoti jai priimtiniausią terminologiją. Kai kurios organizacijos net nebando apibrėžti nusikaltimų elektroninėje erdvėje sampratos, nes, jų nuomone, nuolat keičiantis ir tobulėjant technologijoms tokie apibrėžimai greitai taptų neaktualūs. Todėl nebūtų įmanoma pateikti ir bendro apibrėžimo, o tik

[43] Gosh Sumit, Elliot Turini, *Cybercrimes: a multidisciplinary analysis* (Springer Heidelberg Dordrecht London New York: 2010) 8, žiūrėta 2021 m. vasario 10 d., https://link-springer-com.skaitykla.mruni.eu/book/10.1007%2F978-3-642-13547-7.

numatyti bendras gaires, kurios padėtų praplėsti bendrą suvokimą ir lemtų paprastesnį vartojimą kalbant apie tokio pobūdžio nusikaltimus.

Taigi, išanalizavus mokslinę doktriną ir teisės aktus galima daryti išvadą, jog būtų teisinga vartoti nusikaltimų elektroninėje erdvėje terminą, nes jis yra platesnis ir tikslesnis, apimantis didesnį nusikaltimų, kurie įvykdomi virtualioje erdvėje, spektrą. Tačiau tuo pačiu šio darbo autorė pritaria D. Štitilio nuomonei, kad nusikaltimus elektroninėje erdvėje didžiąja dalimi galima būtų tapatinti su nusikaltimais, susijusiais su kompiuteriais, nes jie beveik nesiskiria, tarp jų skirtumas – tik toks, kad „nusikaltimai elektroninėje erdvėje susiję su kompiuteriais, vykdomi elektroninėje erdvėje“[44]. Atsižvelgiant į tai ir apibendrinus visas analizuotas sampratas manoma, kad nusikaltimai elektroninėje erdvėje yra pavojingi virtualioje erdvėje padaryti nusikaltimai, kurie gali pažeisti pagrindines žmogaus teises, sukelti pavojų visuomenės saugumui ir nuosavybei. Šių nusikaltimų pagrindinis veikimo mechanizmas yra kompiuterinė informacija, kuri gali būti naudojama ir kaip priemonė daryti tokius nusikaltimus, ir būti nusikaltimų objektu. Todėl ir šiame darbe pasirinkta naudoti nusikaltimų elektroninėje erdvėje sąvoką, tačiau kompiuteriniai nusikaltimai ir nusikaltimai elektroninėje erdvėje suprantami kaip turintys tą pačią reikšmę, todėl kartais, atsižvelgiant į skirtingas pozicijas ir požiūrius, bus naudojami kaip sinonimai.

1.2. Pagrindinės nusikaltimų elektroninėje erdvėje rūšys

Kiekviena valstybė turi savo jurisdikciją ir ją taiko savo šalyje pagal vidaus baudžiamąja teisę. Tačiau norint užkirsti kelią nusikalstamumui ir efektyviai su juo kovoti, organizuojant jo prevenciją svarbų vaidmenį atlieka tarptautinis bendradarbiavimas. Nusikaltimai elektroninėje erdvėje yra išskirtiniai tuo, kad tuo pačiu metu gali nukentėti daug asmenų skirtingose pasaulio vietose. Nusikaltimai elektroninėje erdvėje yra visuotinė problema ir norint parengti veiksmingą teisinį reguliavimą būtina tam tikra šalių veiksmų harmonizacija. Kaip jau buvo minėta anksčiau, 2001 m. pasirašyta Konvencija dėl nusikaltimų elektroninėje erdvėje[45], Lietuvoje buvo ratifikuota 2004 m., buvo pirmoji tarptautinė sutartis dėl tokio pobūdžio nusikaltimų. Šioje Konvencijoje „materialioji baudžiamoji teisė susideda iš tokių kriminalizuotinų veikų, kurios priskirtinos nusikaltimams kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui, kompiuteriniams nusikaltimams, turinio nusikaltimams, nusikaltimams, susijusiems su autorių teisių ir gretutinių teisių pažeidimais, bei atitinkamai taikoma papildoma atsakomybė ir sankcijos“[46]. Po šios Konvencijos Lietuvos BK XXX skyriuje buvo papildytos arba pakeistos iš esmės visos šio skyriaus normų sudėtys.

[44] Darius Štitilis, *Supra note*, 39, 38.
[45] Supra note, 29.
[46] Ugnė Grigaitytė, Miglė Mackevičiūtė, „Nusikaltimai virtualioje erdvėje – šiuolaikiniai iššūkiai ir prevencijos galimybės“, 279, iš *Teisės mokslo pavasaris 2020*.

Konvencijoje išskiriamos keturios nusikaltimų elektroninėje erdvėje rūšys. Toliau trumpai aptariama kiekviena iš jų.

Pirma rūšis – tai nusikaltimai, pažeidžiantys kompiuterinės informacijos ir kompiuterinių sistemų konfidencialumą, vientisumą ir prieinamumą (BK 196–198[2] straipsniai). Konvencijos 1 antraštinėje dalyje nurodoma, kad tai tokie nusikaltimai, kai kompiuteris laikomas kaip taikinys, dar kitaip išskiriamas kaip porūšis, arba nusikaltimo padarymo būdas – įsilaužimas. Svarbu pabrėžti, kad „elektroninių duomenų ir informacinių sistemų saugumo turinį atskleisti ir sustruktūrinti BK XXX skyriuje numatytas nusikalstamas veikas padeda CIA triados modelis: elektroninių duomenų ir informacinių sistemų konfidencialumas (angl. *confidentiality*), užtikrinantis, kad reikiama informacija bus prieinama tik tiems vartotojams, kuriems yra suteikta prieigos teisė, integralumas (angl. *integrity*), užtikrinantis, jog duomenų apdorojimo funkcijas atliekančios sistemos nebuvo neteisėtai keičiamos ar modifikuojamos ir prieinamumas (angl. *availability*), sukuriantis galimybę reikiamą informaciją be trukdžių pasiekti reikiamu metu“[47]. Šiais nusikaltimais siekiama pašalinti, pažeisti arba perimti kompiuterinius duomenis. Naudojimasis internetu yra viena iš pagrindinių priežasčių, leidžiančių atlikti tokius prisijungimus. Tipiškos neteisėtos prieigos prie duomenų priežastys apima konfidencialios informacijos gavimą, sukčiavimą ar trikdžių sukėlimą.

Antroji rūšis – tai su kompiuterių naudojimu susiję nusikaltimai (BK 182 straipsnis, 214 straipsnis, 215 straipsnis, 300 straipsnis). 2 antraštinėje dalyje „Su kompiuteriais susiję nusikaltimai“ pateikiama klasifikacija, kai kompiuteris naudojamas palengvinti nusikaltimo padarymą. Konvencijoje išskiriami tik du nusikaltimai: kompiuterio klastojimas (7 straipsnis) ir sukčiavimas kompiuteriu (8 straipsnis). Sukčiavimas yra viena labiausiai paplitusių nusikaltimų elektroninėje erdvėje formų. Pavyzdžiui, apgaulingas internetinis pardavimas, apgaulingas elektroninių lėšų pervedimas ir t. t.[48] Pagal BK 182 straipsnį už sukčiavimą baudžiamojon atsakomybėn traukiamas tas, kuris apgaule savo ar kitų naudai įgijo svetimą turtą ar turtinę teisę, išvengė turtinės prievolės arba ją panaikino. Tokių nusikaltimų pagrindinė įstatymo saugoma vertybė yra asmens nuosavybė, turtinės teisės ir turtiniai interesai. BK XXX skyrius neapibrėžia visų įmanomų nusikaltimų, padarytų elektroninėje erdvėje. Šie nusikaltimai gali būti atliekami daug didesniu mastu, apimdami ir kitus baudžiamajame įstatyme apibrėžtus nusikaltimus. Kompiuterinis klastojimas – tai neteisėtas kompiuterinės informacijos sukūrimas arba pakeitimas. Dažniausiai sukčiavimu yra suklastojama asmens tapatybė. Konvencijoje nebuvo aptariama „tapatybės vagystės“ problema. Tapatybės vagystė apima sukčiavimą, kai auka gauna informaciją iš jam galimai žinomos ir teisėtos institucijos (pvz., AB „Swedbank“) į savo kompiuterį ar el. paštą, kur prašoma pateikti sąskaitos numerius ir slaptažodžius.

[47] Ugnė Grigaitytė, Miglė Mackevičiūtė, *Supra note*, 46, 279.
[48] Jonathan Clough, *Supra note,* 22, 27.

BK 300 straipsnyje numatyta atsakomybė už netikro dokumento pagaminimą, klastojimą, jo laikymą, gabenimą, siuntimą, panaudojimą ar realizavimą. Taip pat svarbu paminėti, kad tokio pobūdžio nusikaltimai dažniausiai užtraukia kelių baudžiamojo įstatymo straipsnių atsakomybę ir yra neatsiejami vienas nuo kito. Pavyzdžiui, „pasisavinus ar suklastojus elektroninę asmens tapatybę elektroninėje erdvėje, galima įvykdyti ir kitas konvencijoje paminėtas pavojingas veikas – turinio nusikaltimus ar nusikaltimus, susijusius su autorių teisėmis ar gretutinėmis teisėmis (Konvencijos 9–10 straipsniai)“[49].

Trečia rūšis, išskiriama Konvencijoje (BK 162 straipsnis, 309 straipsnio 2 ir 3 dalys), yra skirta su turiniu susijusiems nusikaltimams. Kiekviena šalis gali skirtingai vertinti žodžio laisvę ir neliečiamybę. Su turiniu susijusiems nusikaltimams Konvencija taikoma vaiko pornografijai, smurtui prieš vaikus – šie nusikaltimai smerkiami tarptautiniu mastu. Atsiradus internetui, stebėtinai išaugo nusikaltimų, susijusių su vaikų pornografija, skaičius. Paaugliai naudojasi socialiniais tinklais, įvairiomis bendravimo platformomis, pvz., „Facebook“. Taip jie lengvai pasiekiami ir pažeidžiami internete seksualiniai priekabiaujančių asmenų. Daugybė jurisdikcijų kriminalizuoja tokį elgesį – nuo nepadoraus bendravimo su nepilnamečiu iki seksualinio priekabiavimo. Konvencija taip pat sprendžia klausimus, susijusius su priekabiavimu arba persekiojimu, nors šie gali būti laikomi tik vidaus teisės klausimu[50]. Taip siekiama sustiprinti teisinį reguliavimą ir apsaugoti vaikus nuo tokio pobūdžio nusikaltimų.

Ketvirta rūšis, išskiriama Konvencijoje, yra su autorių ir gretutinėmis teisėmis susiję nusikaltimai (BK 191 straipsnis, 194 straipsnis), intelektualios nuosavybės teisių pažeidimai. Jiems priskiriami autoriaus darbo platinimas, naudojimas be jo sutikimo, kopijavimas, kuris taip pat yra aktualus nusikaltimų elektroninėje erdvėje kontekste. Apsaugos objektais laikomi literatūros darbai, muzikos, fotografijos, autovizualiniai ir kiti kūriniai, kurie gali būti platinami elektroniniais laiškais, per serverius, skelbimų portalus ir pan. Pagrindinis teisės aktas, reglamentuojantis autorių ir gretutinių teisių įgyvendinimą ir gynimą, yra Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas[51]. Šis įstatymas yra suderintas ir su Europos Sąjungos teisės aktais, o už autorių ir gretutinių teisių pažeidimą galima tiek civilinė, tiek administracinė, tiek baudžiamoji atsakomybė[52]. Konvencijos 10 straipsnis reikalauja šalims kriminalizuoti autorių teisių pažeidimus, padarytus tyčia, komerciniu mastu ir naudojant kompiuterinę sistemą. Todėl tokio pobūdžio nusikaltimai numatyti BK XXIX skyriuje, skirtame nusikaltimams intelektinei ir pramoninei nuosavybei.

[49] Darius Štitilis ir kt., *Supra note*, 21, 143.
[50] Jonathan Clough, *Supra note*, 22, 150.
[51] „Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo pakeitimo įstatymas“, Valstybės žinios, žiūrėta 2021 m. sausio 16 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.207019.
[52] Ugnė Grigaitytė, Miglė Mackevičiūtė, *Supra note*, 46, 284.

Šiuo metu galiojančiame BK XXX skyriuje elektroninių duomenų ir informacinių sistemų saugumo nusikaltimai yra skirstomi į tokias veikų rūšis:

1. Neteisėtas poveikis elektroniniams duomenims (BK 196 straipsnis) – tai žalos padarymas dėl elektroninių duomenų arba techninės įrangos, programinės įrangos neteisėto sunaikinimo, sugadinimo, pašalinimo ar pakeitimo ar kitų būdų panaudojimo apribojant naudojimąsi tokiais duomenimis. Pagrindinės tokios rūšies nusikalstamos veikos yra prisijungimas prie tam tikro tinklalapio turinio, įsilaužimas, duomenų pakeitimas ir kt.

2. Neteisėtas poveikis informacinei sistemai (BK 197 straipsnis) – tai žalos padarymas dėl neteisėto sutrikdymo ar nutraukiamo informacinės sistemos darbo. Poveikis informacinei sistemai galėtų būti daromas „DoS“ atakomis.

3. Neteisėtas elektroninių duomenų perėmimas ir panaudojimas (BK 198 straipsnis) – tai neteisėtas neviešų elektroninių duomenų stebėjimas, fiksavimas, perėmimas, įgijimas, laikymas, pasisavinimas, paskleidimas ar kitoks panaudojimas. Pavyzdžiui, „Sodros“ ar banko duomenų perėmimas.

4. Neteisėtas prisijungimas prie informacinės sistemos (BK 198^1 straipsnis) – tai neteisėtas veiksmas, kuriuo pažeidžiamos informacinės sistemos apsaugos priemonės. Populiariausios šiuo metu daromos tokios rūšies nusikalstamos veikos: neteisėtas prisijungimas, (pvz., prie „Facebook“ paskyros ar elektroninio pašto, taip pat neteisėtas prisijungimas prie elektroninės bankininkystės).

5. Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis (BK 198^2 straipsnis). Kaip nurodoma mokslo doktrinoje, šią veiką apima neteisėtas gaminimas, gabenimas, pardavimas ar kitoks įrenginių ar programinės įrangos platinimas, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų, tiesiogiai skirtų daryti nusikalstamas veikas, įgijimas ar laikymas[53]. Tai galėtų būti kenkėjiška programinė įranga, kuri renka informaciją ir duomenis apie kitus asmenis (slaptažodžius ir kt.). Viena iš populiariausių tokių programų yra „Trojos arkliai“.

Kaip jau buvo minėta anksčiau, nusikaltimai elektroninėje erdvėje yra specifiniai ir galintys veikti net keliose jurisdikcijose tuo pačiu metu. Todėl labai svarbu juos apibrėžti kuo įmanoma tiksliau išskiriant ir vis papildant elektroninių nusikaltimų rūšis, atsižvelgiant į kaltininkų veikimo lygį, mastą ir padarinius. Iš esmės galima daryti išvadą, kad Konvencijoje ir BK išskiriamos elektroninių nusikaltimų rūšys yra apibrėžtos tapačiai. Tokia sutaptis lemia efektyvesnį ir paprastesnį nusikaltimų elektroninėje erdvėje atskleidimą ir tarptautinį bendradarbiavimą tiriant šiuos nusikaltimus.

1.3. Atsakomybė už nusikaltimus, padarytus elektroninėje erdvėje, ir jos raida Lietuvos Respublikos bei tarptautiniuose teisės aktuose

[53] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 632-633.

Nusikaltimų elektroninėje erdvėje raida siejama su technologijų atsiradimu. Terminas kompiuterinis nusikaltimas buvo pavartotas jau 6–7 dešimtmečiuose. Kaip jau minėta anksčiau, kompiuterinio nusikaltimo terminas pirmą kartą paminėtas JAV spaudoje 1960 m. pradžioje. Alfonsas Konffesore JAV buvo pirmasis žmogus, neteisėtai pasinaudojęs kompiuterine informacija ir taip užvaldęs 620 tūkst. JAV dolerių. Todėl buvo svarbu kuo tiksliau apibrėžti kompiuterinio nusikaltimo sąvoką. Pirmą kartą kompiuterinių nusikaltimų požymiai buvo suformuluoti 1979 m. Dalase vykusioje JAV advokatų asociacijos konferencijoje[54].

1983 m. Ekonominio bendradarbiavimo ir vystymo organizacija (toliau ir – EBPO) sudarė ekspertų komitetą su kompiuteriais susijusių nusikaltimų sampratos problemai spręsti ir apibrėžti[55]. Deja, diskusija baigėsi taip ir nepateisinusi savo lūkesčių ir nebuvo prieita prie vieningos nuomonės. Šiek tiek vėliau EBPO atliko tyrimą, kurio tikslas buvo tarptautinių baudžiamųjų įstatymų dėl kompiuterinių nusikaltimų suvienodinimas. Ekspertų grupė 1992 m. savo 22-oje sesijoje paruošė *Rekomendaciją dėl informacinių saugumo gairių*[56]. Rekomendacijoje apibrėžiami ir suformuluoti pagrindiniai reikalavimai, kurie padėtų užtikrinti saugumą naudojantis informacinėmis sistemomis.

1990 m. Europos Tarybos Komitetas parengė *Rekomendaciją dėl su kompiuteriais susijusių nusikaltimų*, kurioje apibrėžė minimalų 8 ir pasirinktinį 4 kriminalizuotų nusikaltimų sąrašą, susijusį su kompiuteriniais nusikaltimais[57], taip pat pateikė sprendimo būdus ir prevencijos priemones, svarbias norint sumažinti tokių nusikaltimų skaičių. 1995 m. Europos Tarybos Komitetas pateikė dar vieną rekomendaciją *Dėl kriminalistinės procesinės teisės problemų, susijusių su informacinėmis technologijomis*[58]. Šioje rekomendacijoje pagrindinis dėmesys buvo skiriamas tarptautinio bendradarbiavimo stiprinimui baudžiamojo proceso įstatymų srityje, valstybėms narėms išskiriami procedūriniai principai, susiję su nusikaltimų elektroninėje erdvėje tyrimu ir įrodymų rinkimu.

Galima sakyti, kad iki Europos Sąjungos konvencijos dėl nusikaltimų elektroninėje erdvėje Lietuvoje nebuvo skirta pakankamai dėmesio tokiems nusikaltimams. Europos Sąjungos konvencija dėl nusikaltimų elektroninėje erdvėje[59] Lietuvoje buvo ratifikuota 2004 m. Tai pirmoji tarptautinė konvencija prieš tokio pobūdžio nusikaltimus. Šios konvencijos tikslas – sustabdyti neteisėtus veiksmus, nukreiptus prieš informacinių sistemų, tinklų ir duomenų naudojimą. Konvencijoje apibrėžiami tarptautinio bendradarbiavimo aspektai, kai kurios sąvokos, materialioji ir proceso teisė.

[54] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 629.
[55] Darius Štitilis. *Supra note* 8, 6.
[56] OECD Guidelines for the Security of Information Systems, 1992, žiūrėta 2021 m. vasario 10 d., http://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.
[57] OAS, žiūrėta 2021 m. vasario 10 d., http://www.oas.org/juridico/english/89-9&final%20Report.pdf.
[58] „Council of Europe committee of ministres“, žiūrėta 2021 m. vasario 15 d., https://rm.coe.int/16804f6e76.
[59] *Supra note,* 29.

Apie šios konvencijos 1 skyriuje įtvirtintas nusikaltimų elektroninėje erdvėje rūšis ir tokių nusikaltimų kriminalizavimą plačiau rašoma ankstesniame poskyryje.

1961 m. galiojusiame Baudžiamajame kodekse (toliau – 1961 m. BK) buvo išskiriamos dvi veikos, susijusios su kompiuteriniais nusikaltimais[60]. Pirma – 1961 m. BK 274 straipsnis, kuriame numatyta atsakomybė už svetimo turto užvaldymą arba į teisės į turtą įgijimą apgaulės būdu, taip pat išskiriant sukčiavimą, padarytą pakartotinai, už nusikaltimus nuosavybei arba grupės iš anksto susitarusių asmenų, sudarant žinomai neteisingą kompiuterinę programą, įrašant į kompiuterio atmintį klaidingus duomenis, taip pat kitaip paveikiant kompiuterinę informaciją ar jos apdorojimą.

Antra – 1961 m. BK 277 straipsnyje išskirtas turtinės žalos padarymas apgaule arba piktnaudžiaujant pasitikėjimu. Šiame straipsnyje atsakomybė atsiranda, jei buvo padaryta turtinė žala kitam asmeniui vengiant atsiskaitymų už atliktus darbus ar suteiktas paslaugas, taip pat vengiant kitų mokėjimų, jeigu tai padaryta apgaule ar piktnaudžiaujant pasitikėjimu, arba ta pati veika sudarant žinomai neteisingą kompiuterinę programą, įrašant į kompiuterio atmintį klaidingus duomenis, taip pat kitaip paveikiant kompiuterinę informaciją ar jos apdorojimą. Abiejuose straipsniuose numatytos nusikalstamos veikos buvo priskiriamos prie nusikaltimų nuosavybei, todėl pagrindinė baudžiamojo įstatymo saugoma vertybė buvo asmens nuosavybė, o ne kompiuteriniai ar elektroniniai duomenys.

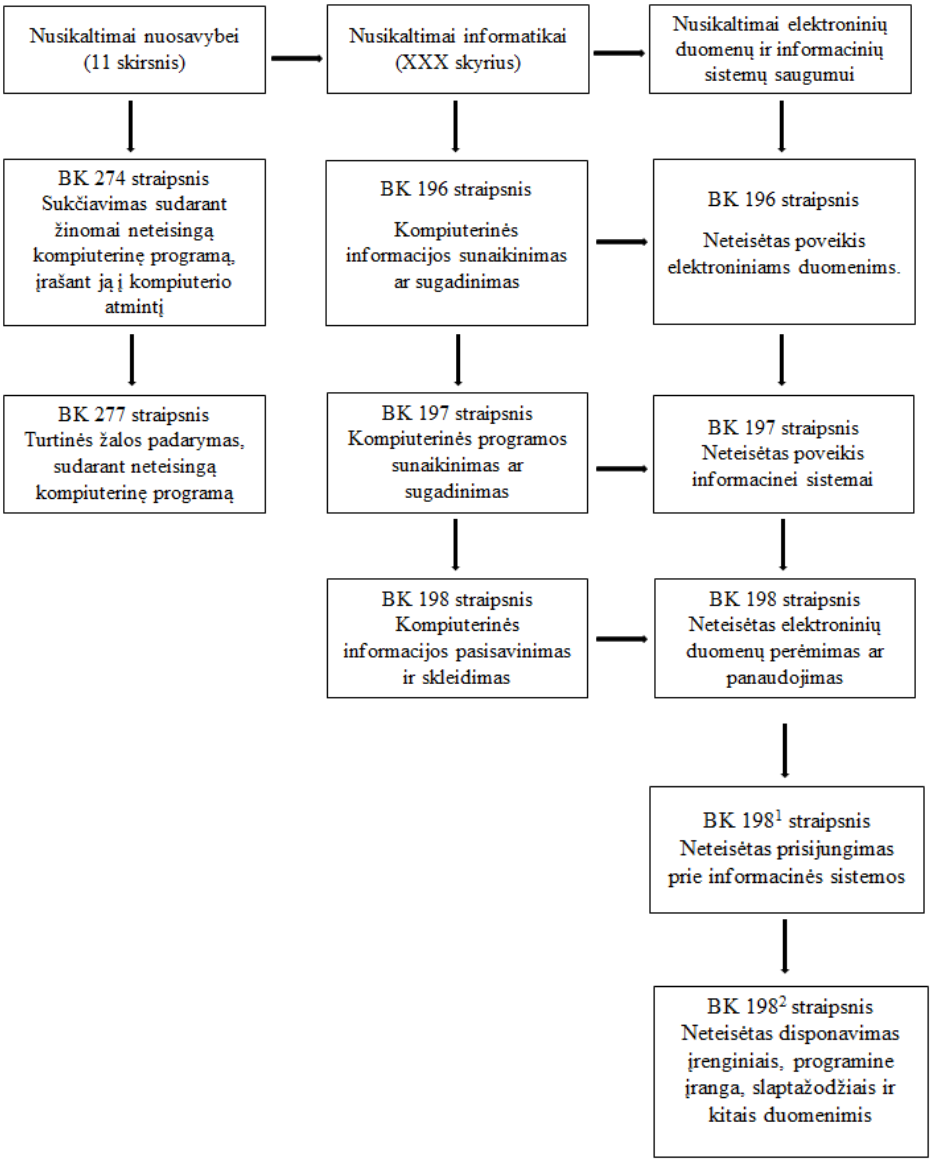
Vėliau, įsigaliojus 2003 m. BK, buvo parengtas naujas XXX skyrius „Nusikaltimai informatikai“. Šiame skyriuje buvo apibrėžtos tokios nusikalstamos veikos: kompiuterinės informacijos sunaikinimas ar pakeitimas (BK 196 straipsnis), kompiuterinės programos sunaikinimas ar pakeitimas (BK 197 straipsnis), kompiuterinės informacijos pasisavinimas ir skleidimas (BK 198 straipsnis). Kaip matyti iš skyriaus pavadinimo, jame yra pavartota sąvoka „informatika“, kurios samprata yra pakankamai plati. Kaip nurodoma mokslo doktrinoje, „informatika – tai mokslo šaka, nagrinėjanti informacijos apdorojimą panaudojant kompiuterinę įrangą. Informatika apima abstrakčių algoritmų, formalių gramatikų tyrimus, programavimo kalbas, programinę ir techninę įrangą. Taigi skaitmeninė informacija ir jos apdorojimas šiuo atveju tampa nusikaltimo objektu, nors informatikos specialistai labiau linkę vartoti konkretesnius terminus, tokius kaip duomenys, informacinė sistema, kompiuterių tinklai, programinė įranga – tai tiksliau apibrėžia patį nusikaltimo objektą“[61]. Todėl akivaizdu, kad nors ir buvo padaryta ganėtinai didelė pažanga reglamentuojant nusikaltimus elektroninėje erdvėje, tačiau nepakankamai tiksliai ir detaliai suformuluotas skyriaus pavadinimas bei nusikaltimų apibrėžimai turėjo daug trūkumų, kurie neleido iki galo atskleisti ir kvalifikuoti visus daromus tokio pobūdžio nusikaltimus. Kaip jau minėta anksčiau, „įstatymų leidėjas naudojo netikslią terminologiją (nebuvo atskirtos sąvokos *duomenys* ir *informacija*), neįvertino kai

[60] Lietuvos Respublikos baudžiamasis kodeksas, Vyriausybės žinios, žiūrėta 2021 m. sausio 25 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.20465/jxfupAglbe.
[61] Nikolaj Goranin, Dalius Mažeika, *Supra note*, 34, 24.

kurių galimų nusikaltimų elektroninėje erdvėje atvejų (pvz., įsibrovimas į kompiuterinę sistemą, bet nepasisavinant ar nekeičiant informacijos, arba neteisėtas disponavimas licencijuotų programų kodais, „nulaužimo“ programomis, slaptažodžiais ir t. t.)“[62].

2004 m. ratifikavus Europos Sąjungos konvenciją dėl elektroninių nusikaltimų buvo padaryti esminiai pakeitimai BK XXX skyriuje. Konvencija buvo pakeistos arba papildytos beveik visų BK XXX skyriuje numatytų nusikaltimų sudėtys[63]. Šie pakeitimai buvo patvirtinti Lietuvos Respublikos Seime 2007 m. birželio mėn. 28 d. įstatymu Nr. X-1233. Pirma, buvo pakeistas XXX skyriaus pavadinimas iš „Nusikaltimai informatikai“ į „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“. Taip pat modifikuoti visi skyriaus straipsniai[64]. Iš esmės pakeisti BK 196–198[2] straipsniai, BK 196 straipsnio pavadinimas keičiamas iš „Kompiuterinės informacijos sunaikinimas“ į „Neteisėtas poveikis elektroniniams duomenims“. Veika papildoma dar vienu alternatyviu kvalifikuojančiu požymiu „kitais būdais“. Taip pat papildomi alternatyvūs nusikaltimo dalykai „elektroniniais duomenimis, technine, programine įranga“. Straipsnis papildytas 2 ir 3 dalimis. BK 196–198 straipsniai papildomi dalimis, numatančiomis griežtesnę atsakomybę padarius veiką strateginę reikšmę turinčiam nacionaliniam saugumui ar valstybės valdymui, ko nebuvo iki tol. Taip pat griežtinama atsakomybė už tokio pobūdžio nusikaltimus. Toliau pateikta lyginamoji schema (žiūrėti 3 pav.), kurioje matyti, kaip keitėsi BK reglamentavimas, susijęs su nusikaltimais elektroninėje erdvėje.

[62] Nikolaj Goranin, Dalius Mažeika, *Supra note*, 34, 24.
[63] Renata Marcinauskaitė, „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai)“ (daktaro disertacija, Mykolo Romerio universitetas, 2013), žiūrėta 2021 m. sausio 5 d., https://repository.mruni.eu/bitstream/handle/007/15957/Disertacija_Marcinauskait%c4%97.pdf?sequence=2&isAllowed=y.
[64] Nikolaj Goranin, Dalius Mažeika, *Supra note*, 34, 24.



3 pav. Nusikaltimų elektroninėje erdvėje reglamentavimas BK (1961–2007 m.) (sudaryta autorės).

2004 m. gegužės 1 d. Lietuvoje įsigaliojo Elektroninių ryšių įstatymas[65]. Šis įstatymas reglamentuoja visuomeninius santykius, susijusius su elektroninių ryšių paslaugomis, tinklais ir su jais susijusiomis priemonėmis bei paslaugomis, elektroninių ryšių išteklių naudojimu, taip pat visuomeninius santykius, susijusius su radijo įrenginiais, galiniais įrenginiais ir elektromagnetiniu suderinamumu.

Vėliau buvo priimtas Europos tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas[66]. Atsižvelgiant į tai, kad valstybių narių įstatymuose yra didelės spragos ir dideli įstatymų skirtumai, galintys trukdyti kovoti su organizuotu nusikalstamumu ir terorizmu,

[65] Lietuvos Respublikoje elektroninių ryšių įstatymas, Valstybės žinios, žiūrėta 2021 m. sausio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232036/SgfuAtlPUO.
[66] Europos tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas, Eur-lex, žiūrėta 2021 m. sausio 25 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32005F0222.

apsunkinti veiksmingą policijos ir teisminį bendradarbiavimą atakų prieš informacines sistemas srityje, siekta suvienodinti sąvokų apibrėžimus, nusikaltimų sudėties požymius numatant, kad neteisėta prieiga prie informacinės sistemos, neteisėtas įsikišimas į sistemą ir neteisėtas įsikišimas į duomenis yra bendrai laikomi nusikaltimais. Taip pat vienas iš siekių – suderinti sklandesnį tarptautinį bendradarbiavimą tarp valstybių narių, numatyti griežtesnę atsakomybę veikiant organizuotai grupei ir t. t.

Tačiau šis Europos Tarybos pamatinis sprendimas 2005/222/TVR 2013 m. buvo pakeistas Europos Parlamento ir Tarybos direktyva 2013/40/ES (toliau – Direktyva 2013/40/ES). Direktyva buvo papildyta dar vienu nusikaltimo padarymo būdu elektroninių ir informacinių sistemų saugumui – neteisėtu duomenų perėmimu. Išskiriamos priemonės, naudojamos tokioms nusikalstamoms veikoms atlikti. Įgyvendinant Direktyvą 2013/40/ES, Lietuvos Respublikos įstatymų leidėjas BK (196, 197, 198^1, 198^2 straipsniai) atliko pakeitimus. BK 196 straipsnio 2 dalis papildyta taip: „Tas, kas šio straipsnio 1 dalyje numatytą veiką padarė daugelio informacinių sistemų elektroniniams duomenims arba strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniams duomenims, arba pasinaudodamas svetimais asmens duomenimis, arba padarydamas didelės žalos, baudžiamas bauda arba areštu, arba laisvės atėmimu iki šešerių metų“[67]. Atitinkamai ir BK 197 straipsnio 2 dalis buvo papildyta vienu iš alternatyvių nusikalstamos veikos dalykų „daugeliui informacinių sistemų“. Už nusikaltimus, numatytus BK 198^1 ir 198^2 straipsniuose, sugriežtinta atsakomybė, kaip ir buvo išskirta bei numatyta 2013 m. direktyvoje dėl sankcijų sugriežtinimo. Pagirtina, kad Lietuva jau iki šios Direktyvos savo baudžiamojoje teisėje buvo numačiusi atsakomybę už neteisėtą elektroninių duomenų perėmimą ir panaudojimą (BK 198 straipsnis).

Dar po metų, t. y. 2014 m., buvo priimtas Lietuvos Respublikos kibernetinio saugumo įstatymas (Nr. XII–1428)[68]. Šio įstatymo 1 straipsnio 1 dalis atskleidžia įstatymo paskirtį ir jo taikymą: šis įstatymas nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones.

[67] Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198^1, 198^2 straipsnių ir priedo pakeitimo ir kodekso papildymo 270^3 straipsniu įstatymas, TAR, žiūrėta 2021 m. sausio 21 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ce192022135111e5af81c7d24921dbde.

[68] Lietuvos kibernetinio saugumo įstatymas, TAR, žiūrėta 2021 m. sausio 21 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee.

Taigi, šiame skyriuje išanalizuoti temai reikšmingi teisės aktai, kurie buvo pakeisti ir priimti ne tik tarptautiniu, bet ir nacionaliniu lygmeniu. Iš atliktos analizės galima teigti, kad Europos Sąjungos direktyva dėl elektroninių nusikaltimų bei Direktyva, kuria buvo pakeistas Europos tarybos pamatinis sprendimas dėl atakų prieš informacines sistemas, turėjo itin didelę reikšmę Lietuvos vidaus baudžiamajai teisei. Šios direktyvos itin reikšmingos nusikaltimų, padarytų elektroniniams duomenims ir informacinės sistemos saugumui, reglamentavimui.

2. KAI KURIŲ NUSIKALTIMŲ, PADARYTŲ ELEKTRONINĖJE ERDVĖJE (198, 198[1], 198[2] STRAIPSNIAI), KRIMINALISTINĖ CHARAKTERISTIKA IR BRUOŽAI

2.1. Bendroji nusikaltimų elektroninėje erdvėje charakteristika

Nusikaltimo tyrimo sėkmė priklauso ne tik nuo tyrėjo gebėjimo suprasti baudžiamojo įvykio turinį, bet ir nuo to, kaip jis geba suvokti kriminalistinę nusikaltimo esmę[69]. Nusikaltimų kriminalistinė charakteristika – tai koreliaciniais ryšiais tarpusavyje susijusių ir apibendrintų kriminalistiškai reikšmingų duomenų apie nusikaltimų tipinius požymius ir aplinkybių visuma[70]. Kiekvienas nusikaltimas yra išskirtinis ir palieka savitų, tik jam būdingų, išskirtinai šiam tyrimui reikšmingų duomenų ir pėdsakų. Todėl svarbu, kad ikiteisminio tyrimo pareigūnas būtų kvalifikuotas ir gebėtų suprasti ir pritaikyti šiuos koreliacinius ryšius konkrečiai nusikaltimų rūšiai. V. E. Kurapkos ir H. Malevski nuomone, „kriminalistinė nusikaltimų charakteristika yra ne kas kita, kaip kiekvienos nusikaltimų rūšies ir jos tyrimo metodikos pagrindinis elementas. Tik gerai išmanant jos elementus galima efektyviai, operatyviai ir tikslingai tirti konkretų nusikaltimą, nes priešingu atveju ši veikla yra ne planingas, mokslinėmis rekomendacijomis pagrįstas tyrimas, bet chaotiškas tarpusavyje nesusijusių veiksmų konglomeratas, skirtas siekti labai miglotai suprantamo tikslo“[71]. Kiekvieno ikiteisminio tyrimo pareigūno pagrindinis tikslas turėtų būti per kuo įmanoma trumpesnį laiką išsamiai atskleisti visas nusikaltimo aplinkybes. Todėl gebėjimas analizuoti kriminalistinės charakteristikos elementus yra būtinas šiam tikslui pasiekti, nes vieno elemento atskleidimas suteikia informacijos apie kitą, leidžia susidaryti bendrą tiriamo nusikaltimo vaizdą.

Analizuojant kriminalistinės charakteristikos sampratą pastebėta, kad pirmieji šia koncepcija susidomėję ir pradininkai apibrėžiant ją buvo Rusijos mokslininkai. Vienas iš pirmųjų apibrėžimų – kad kriminalistinė charakteristika suprantama kaip objektyviųjų duomenų apie nusikaltimą sistema[72]. Šis terminas nėra visai tinkamas, nes jis nusako tik objektyviąją nusikaltimo pusę ir tarsi šone palieka subjektyviąją (nusikaltimą padariusį asmenį). Vėliau buvo sukurta ir kitokių teorijų, apibūdinančių kriminalistinę charakteristiką. Pavyzdžiui, V. E. Kozlovo nuomone, tai tam tikra duomenų sistema apie tam tikros rūšies nusikaltimus, kurie tarpusavyje susiję kriminalistiniais charakteringais ryšiais ir požymiais, užtikrinančiais versijų apie nusikaltimo įvykį kėlimą, leidžiančiais tinkamai įvertinti situaciją tiriant nusikaltimus elektroninėje erdvėje[73]. Vieningo apibrėžimo šiuo klausimu nėra ir

[69] Snieguolė Matulienė, „Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimų metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija“ (daktaro disertacija, Lietuvos teisės universitetas, 2014), 4.
[70] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 538.
[71] Vidmantas Egidijus Kurapka, Hendryk Malevski, „Šiuolaikinė nusikaltimų tyrimo koncepcija ir jos kriminalistinis bei procesinis užtikrinimas. Pirmieji rezultatai“, *Jurisprudencija*, 2003, 43 (35)), 81.
[72] Танасевич В. Г., *Образцов В. А. О криминалистической характеристике преступлений* // Вопросы борьбы с преступностью. Вып.25. 1976, 99.
[73] В. Е. Козлов, *Теория и практика борьбы с компьютерной преступностью* (Москва: Горячая линия – Телеком, 2002), 114.

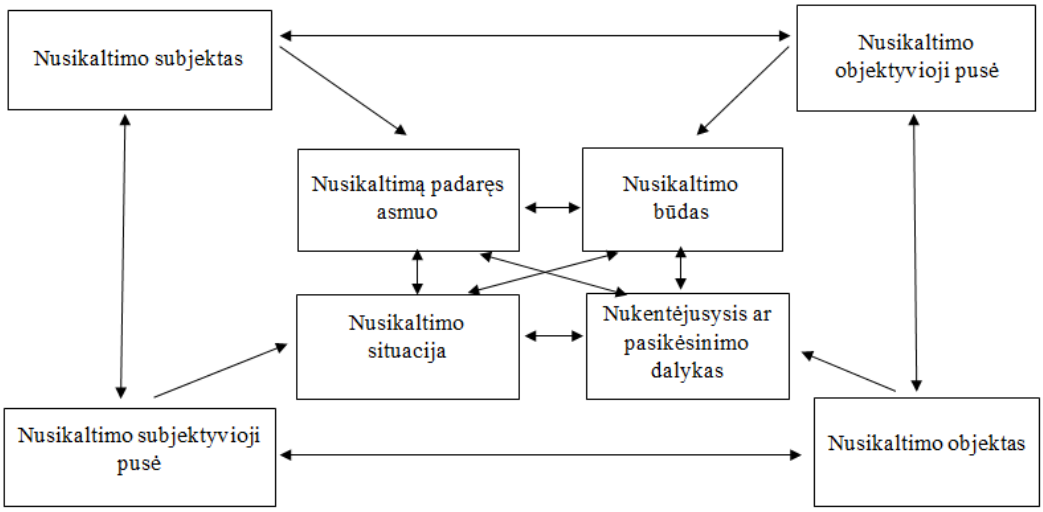
greičiausiai nebus, nes nebūtų tikslinga apibrėžti ir įvardinti konkrečius jos struktūrinius elementus pritaikant visoms nusikaltimų rūšims ir grupėms, nes kriminalistinė charakteristika yra dinamiška, ji gali keistis dėl naujų nusikaltimų mechanizmų, būdų ar atsirandant naujoms kriminalizuotoms veikoms.

Pažymėtina, kad būtų daug tikslingiau atskleisti kriminalistinę charakteristiką per tam tikrą nusikaltimų kategoriją, nes surinkta informacija gali padėti atskleisti tipinius ir pasikartojančius atskirų nusikaltimų rūšių požymius. Pavyzdys galėtų būti toks: Lietuvos kriminalinės policijos biuro (toliau ir – LKPB) tyrėjai sisteminius nusikaltimus elektroninėje erdvėje identifikuoja remdamiesi tokiais požymiais: tapatus padarymo būdas, vienodas pasikėsinimo dalykas, panašus nusikalstamos veikos padarymo braižas, tas pats šią veiką padaręs asmuo[74]. Pateiktas pavyzdys tik patvirtina, kad šių elementų tinkamas surinkimas, ištyrimas ir panaudojimas gali ne tik atskleisti tam tikrą nusikaltimą, tačiau ir padėti greičiau išaiškinti kitus.

S. Matulienė savo disertacijoje rašė, kad būtent nusikaltimo sudėtis yra kriminalistinės nusikaltimų charakteristikos struktūros pagrindas ir teigia, kad šie elementai turi kriminalistiškai reikšmingos informacijos[75]. Nusikaltimo sudėtį, kaip žinia, sudaro nusikaltimo objektyvioji (pažeista įstatymo saugoma vertybė, nusikaltimo padarymo aplinkybės) ir subjektyvioji pusės (kaltė, asmuo, padaręs nusikaltimą). Kriminalistinės charakteristikos turinį sudaro šie tarpusavyje koreliaciniais ryšiais susiję bylai reikšmingi duomenys: nusikaltimo būdas, nusikaltimą padaręs asmuo, nukentėjusysis ar pasikėsinimo dalykas, nusikaltimo situacija. Profesorė savo disertacijoje pateikė schemą (4 pav.), kurioje pavaizduota šių elementų santykių struktūra, puikiai atspindinti elementų koreliacinius ryšius. Mokslininkai, nagrinėjantys elektroninių nusikaltimų kriminalistinę charakteristiką, pažymi, kad tokio pobūdžio nusikaltimai išsiskiria iš tradicinių nusikaltimų savo specifika, ir nurodo tokius elektroninių duomenų ir informacinių sistemų saugumo kriminalistinės charakteristikos elementus: žinios apie nusikaltimo objektą, žinios apie nusikaltimo padarymo būdą ir pėdsakų susidarymo mechanizmą, žinios apie nusikaltimo padarymo aplinkybes (laikas, vieta, aplinka), žinios apie kaltininko asmenybę, tipinius nusikalstamo elgesio motyvus ir tikslus, žinios apie galimą nukentėjusįjį ir ryšiai tarp visų šių elementų[76]. Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui kriminalistinėje charakteristikoje tikslinga įvardyti šiuos elementus: elektroninių duomenų ir informacinių sistemų saugumo nusikaltimų padarymo būdas, nusikaltėlio

[74] *Supra note* 3, 39.
[75] Snieguolė Matulienė, *Supra note*, 69, 47 .
[76] Вехов, В. Б., Попова, В. В., Ильюшин, Д. А., *Тактические особенности расследования преступлений в сфере компьютерной информаций* (Москва: «ЛэксЭст», 2004), 11.

asmenybės charakteristika, nusikalstamo pasikėsinimo objektas, nusikaltimo situacija[77]. Todėl, atsižvelgiant į tai, toliau trumpai apžvelgsime konkrečias šių koreliacinių ryšių sąsajas.



4 pav. Nusikaltimų kriminalistinės charakteristikos ir nusikaltimo sudėties elementų santykių struktūra[78]

Iš pateiktos struktūros (4 pav.) labai aiškiai matoma, kad vienas iš kriminalistinės charakteristikos struktūros elementų yra nusikaltimą padaręs asmuo, tarpusavyje susijęs su kitais elementais, tarp kurių yra nusikaltimo būdas, nusikaltimo situacija ir nukentėjusysis arba pasikėsinimo dalykas. Taip pat matoma, kad nukentėjusysis yra tarpusavyje susijęs su nusikaltimo situacija ir nusikaltimo būdu. Jei šiuos elementų santykio ryšius lygintume su nusikaltimais elektroninėje erdvėje (BK 198, 198[1], 198[2] straipsniai), pastebėtume, kad nusikaltimą padaręs asmuo ir nukentėjusysis neretai susiję giminystės ryšiais[79] ar užsimezgusia draugyste[80], taip pat juos gali sieti ir darbo santykiai[81]. Žinoma, gali būti ir taip, kad auka pasirenkama atsitiktinai, tačiau tai ganėtinai reti atvejai. „Tarp nusikaltėlio ir nukentėjusiojo yra kriminalistiškai reikšmingas ryšys: asmenys, darydami nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui, paprastai neatsitiktinai pasirenka savo auką, dažniausiai jie renkasi aukas pagal tai, kaip yra apsaugoti elektroniniai duomenys, ar vartotojai naudojasi kokiomis specialiomis duomenų apsaugos priemonėmis, ar ne, ir kokią programinę įrangą jie naudoja“[82]. Kalbant apie nusikaltimo būdą ir nusikaltimo situaciją, tai elektroninių nusikaltimų padarymo būdas priklausys nuo situacijos aplinkybių (pvz., laikas ir vieta).

[77] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 31, 634.
[78] Snieguolė Matulienė, *Supra note*, 69, 48.
[79] Klaipėdos apygardos teismo 2010 m. kovo 1 d. nutartis, priimta baudžiamojoje byloje Nr. 1S-49-50/2010, eteismai, žiūrėta 2021 m. vasario 15 d., https://eteismai.lt/byla/80718850183473/1S-49-50/2010.
[80] Telšių rajono apylinkės teismo 2016 m. kovo 1 d. baudžiamasis įsakymas, priimtas baudžiamojoje byloje Nr. 1-58-187/2016, eteismai, žiūrėta 2021 m. vasario 15 d., https://e-teismai.lt/byla/134583854524928/1-58-187/2016, „Lietuvos Aukščiausiojo Teismo 2015 m. sausio 6 d. nutartis, priimta baudžiamojoje byloje Nr. 2K-138/2015“, eteismai, žiūrėta 2021 m. vasario 15 d., https://eteismai.lt/byla/148386211638579/2K-138/2015.
[81] Vilniaus apygardos teismo 2014 m. gegužės 15 d. nutartis, priimta baudžiamojoje byloje Nr. 1A-338-312/2014, eteismai, žiūrėta 2021 m. vasario 15 d., https://eteismai.lt/byla/63488840739284/1A-338-312-2014.
[82] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 654.

Pavyzdžiui, asmenys, darydami tokius nusikaltimus netiesioginiu būdu, per atstumą, dažniausiai renkasi nakties metą, kai įmonėje nėra darbuotojų ar aukos miega. Tokiu metu mažesnė tikimybė likti pastebėtiems ir taip galima neskubėti atlikti savo neteisėtus veiksmus (pvz., paskleisti virusą ar perimti tam tikrą konfidencialią informaciją). Taip pat svarbu pažymėti, kad tokiu atveju nusikaltimo padarymo vieta ir padarinių kilimo vieta nesutampa, atvirkščiai, nei veikiant tiesioginiu būdu.

Veikiant tiesioginiu būdu, turint fizinį sąlyti su technika, kurią kaltininkas planuoja perimti, laikyti, gabenti ar pakeisti, dažniausiai pasirenkamas dienos metas, apsimetama kitu asmenim (pvz., informacinių technologijų specialistu), taip apgaule patenkant į patalpas, kuriose yra nusikaltimo dalykas. Nusikaltimą padaręs asmuo ir nusikaltimo situacija susiję tuo, kad nusikaltimai elektroninėje erdvėje dažniausiai yra planuojami iš anksto numatant tam tikras schemas ir veikimo modelius. Taigi, šiuo atveju, kai nusikaltimas yra planuojamas, nusikaltimą darantis asmuo visada pasirinks jam palankiausią situaciją, kuri palengvins jo daromą nusikaltimą. Tai tik keletas šių keturių kriminalistinės charakteristikos elementų pavyzdžių, kurie tarpusavyje koreliuoja. Kiti detaliau analizuojami kitame šio skyriaus poskyryje.

Apibendrinant galima teigti, kad šie keturi elementai ir kiekvienas iš jų atskirai tiriant bylos aplinkybes sudaro tam tikrą rinkinį informacijos, susijusios su konkrečiu nusikaltimu. Šios informacijos požymių visuma bei gebėjimas pritaikyti šių elementų koreliacinius ryšius yra tyrimo metodikos pamatas, be kurio tinkamai ir laiku ištirti nusikaltimą gali būti sudėtinga, o kartais – net ir beveik neįmanoma.

2.2. Nusikaltimų elektroninėje erdvėje padarymo būdai

Nusikaltimo padarymo būdas yra būtinas konkretaus straipsnio objektyvusis sudėties požymis. Kalbant konkrečiai apie kriminalistikoje suprantamą nusikaltimo padarymo būdą galima teigti, kad tai subjekto elgesys iki nusikaltimo padarymo, nusikaltimo padarymo metu ir po nusikaltimo, paliekantis tam tikrus pėdsakus[83]. Nusikaltimų elektroninėje erdvėje padarymo būdai yra išvardinti BK XXX skyriaus baigiamojo darbo analizuojamose 198, 198[1], 198[2] straipsnių dispozicijose. Šiuose straipsniuose numatyti perėmimo ir panaudojimo būdai yra alternatyvūs – tai reiškia, kad, padarius bent vieną iš šių veiksmų, taikoma baudžiamoji atsakomybė[84]. V. E. Kozlovo nuomone, duomenų ir informacinės sistemos perėmimas gali būti tiek kontaktinis, tiek nekontaktinis (tiesioginis ir netiesioginis).

[83] Darius Štitilis, Rimantas Petrauskas, *Kompiuteriniai nusikaltimai ir jų prevencija* (Lietuvos teisės akademija: Vilnius, 2000), 24.
[84] Albertas Milinis, Edita Gruodytė, Aurelijus Gutauskas ir kt., *Supra note,* 7, 472.

Kita mokslininkų grupė duomenų perėmimo būdus skirsto į tiesioginį perėmimą; forsuotą perėmimą; simbolių perėmimą; pranešimų perėmimą[85]. Toks skirstymas yra paremtas asmens, darančio nusikaltimą, buvimo vieta, t. y ar asmuo perėmė tam tikrus duomenis fiziškai dalyvaudamas prie įrenginių, kuriems padaroma žala, ar veikė netiesiogiai, pasinaudodamas internetu ir taip padarydamas žalos per atstumą. Belkino nuomone, dažniausiai literatūroje elektroninių duomenų ir informacinės sistemos skirstomos į šias grupes [86]:

1. Elektroninių duomenų ir informacinės sistemos perėmimo metodai. Elektroninių duomenų ir informacinės sistemos perėmimas – tai veiksmas, kai tam tikri elektroniniai duomenys ar informacinės sistemos yra užfiksuojamos ir persiunčiamos. Kitaip tariant, šiai grupei priskiriami audiovizualiniai ir elektromagnetiniai perėmimo metodai, kuriuos pasitelkus gaunama duomenų ir informacijos apie tam tikrus sistemos duomenis[87]. Perimant elektroninius duomenis ir informacines sistemas dažniausiai naudojami pasiklausymo įrenginiai, video technika, renkami ištrinti failai ir t. t.

2. Neteisėtos prieigos metodai. Neteisėtos prieigos metodas – kai naudojantis tam tikromis programomis yra neteisėtai įsilaužiama į kito asmens kompiuterį ar informacinę sistemą. D. Štitilis savo darbe teigė, kad „neteisėta prieiga prie kompiuterinės informacijos laikytina neteisėta veika, kurios metu įveikiant apsaugos priemones prieinama prie kompiuterinės informacijos ir pažeidžiamas laikomos informacijos slaptumas bei privatumas“[88]. Taip pat šiam metodui priskiriamas ir tam tikrų duomenų stebėjimas. Stebėjimas gali būti suprantamas kaip galimybė šiuos duomenis matyti, suvokti ir įvertinti. Asmuo, darantis nusikaltimą, turi atpažinti, kad tai elektroniniai duomenys. Stebėjimas – tai tam tikrą laiką trunkantis veiksmas, tačiau veikos kvalifikavimui jo trukmė neturi reikšmės[89]. Neteisėta prieiga gali būti įgyvendinama kenkėjiškomis programomis (*paskui kvailį*, *paskui uodegą*, *lėta atranka* ir t. t.).

3. Manipuliacijos duomenimis ir valdymo komandomis metodai. Manipuliacija duomenimis ir valdymo komandomis – vienas labiausiai paplitusių nusikaltimų elektroninėje erdvėje metodų, nes jį gana sunku aptikti. Šie būdai susiję su manipuliavimu duomenimis, kompiuterine informacija ar tam tikromis komandomis. Vienas pagrindinių ir populiariausių šio metodo būdų yra „Trojos arklys“. Kaip rašo Lietuvos Respublikos nacionalinis kibernetinio saugumo centras, „Trojos arklys“ yra kenkėjiškos programos kodas, programa, kuri gali paskleisti kitą kenkėjišką programinę įrangą ir į kompiuterinę sistemą patenka surandant jos spragas naršyklėse. Taip užkrėstoje sistemoje yra atveriamos atgalinės

[85] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 636.
[86] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 635.
[87] Darius Štitilis, Rimantas Petrauskas, *Supra note*, 83, 25.
[88] Darius Štitilis, „Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai“, *Jurisprudencija*, 2003. t. 47 (39), 8.
[89] Albertas Milinis, Edita Gruodytė, Aurelijus Gutauskas ir kt., *Supra note*, 7, 472.

durys, leidžiančios stebėti vartotoją ir kt.[90] Kibernetinio saugumo metinėje ataskaitoje yra pateikiamas vienas iš rezonansinių tokio veikimo pavyzdžių, kai į „TV3“ internetinę svetainę buvo įsilaužta pasinaudojant „galinių durų“ prisijungimo galimybe ir taip gavęs neteisėtą prieigą internete asmuo skelbė melagingas naujienas bei imitavo tikrą siuntėją[91]. Šis būdas yra itin pavojingas ir sunkiai aptinkamas, nes turi specifinių parinkčių, dėl kurių gali pats susinaikinti. Be „Trojos arklio“ yra ir daugiau kenkėjiškų programų (5 pav.), kaip, pavyzdžiui, įvairūs virusai ar makrovirusai, duomenų ar kodų pakeitimo programos ir t. t. Sąrašas nėra baigtinis, kadangi tokių programų yra daugybė, o laikui bėgant atsiranda ir vis naujų.

4. Kompleksiniai metodai. Kompleksiniai metodai – tai veikimas, kai asmuo, darantis tokius nusikaltimus, pasinaudoja keliais anksčiau minėtų metodų būdais. Dažniausiai pasirenkamas vienos grupės metodas, kuris naudojamas kaip pagrindinis, o kitas – kaip pagalba savo funkcijomis slėpti darant neteisėtus veiksmus.

Azorult	*Pykspa*	*Conficker*	*Downadup*	*He-andromeda*	*Sality-p2q*	*Wrokni*	*Wannacrypt*	*Lokibot*
9 %	7 %	6 %	5 %	3 %	2 %	2 %	2 %	1 %

5 pav. 9 labiausiai paplitusios kenkimo programinės įrangos, susijusios su lietuviškais IP adresais [92]

Lietuvos Respublikos nacionalinis kibernetinio saugumo centras[93] yra atsakingas už kibernetinių incidentų valdymą. Jis stebi ir kontroliuoja incidentus, susijusius su kibernetiniu saugumu, taip pat kiekvienais metais teikia akreditacijas. 2019 metais savo kasmetinėje ataskaitoje šis centras yra pateikęs gautą informaciją iš trečiųjų šalių dėl 9 labiausiai paplitusių programinių įrangų tarp lietuviškų IP adresų. Labiausiai paplitusios buvo *Azorut*, *Pykspa* ir *Conficker*. Azorut kenkėjiška programinė įranga žinoma kaip vagianti informaciją, susijusią su naršymo istorija, slapukais, ID, slaptažodžiais ir t. t. *Pykspa*, dar kitaip vadinama kompiuteriniu kirminu, plinta be vartotojo patvirtinimo, tad gali vogti jo asmeninę informaciją ar stabdyti kai kuriuos procesus. *Conficker* kenkėjiška programa plinta internetu, per USB laikmenas ir dažniausiai naudojama slaptažodžiams atspėti. Šios programos nėra lengvai aptinkamos, todėl vartotojas gali net nežinoti apie jų egzistavimą, nors žala jau bus padaryta. Todėl norint to išvengti ir apsaugoti savo asmeninę informaciją nuo

[90] Pažeidžiamos kompiuterinės sistemos ir programos, NKSC, žiūrėta 2021 m. vasario 15 d., https://www.nksc.lt/rekomendacijos/trojangeneric.html.
[91] Krašto apsaugo ministerija. *Nacionalinė kibernetinės būklės metinė ataskaita*, 15.
[92] *Ibid*, 12.
[93] Naujienos ir saugumo pranešimai, NKSC, žiūrėta 2021 m. vasario 15 d., https://www.nksc.lt/.

neteisėto prisijungimo prie informacinės sistemos ar poveikio elektroniniams duomenims būtina naudoti antivirusines programas, kurios aptinka šias kenkėjiškas programas.

Akivaizdu, kad tokia kenkėjiškų programinių įrangų gausa ne tik kelia pavojų vartotojams ir visuomenės, kuri neturi kompetencijos tokias programas laiku atpažinti, saugumui, tačiau tai didelė problema kalbant apie tokiais būdais padarytų nusikaltimų tyrimą. Nusikaltimus elektroninėje erdvėje tiriantis pareigūnas iš esmės turi būti ir kvalifikuotas informacinių technologijų specialistas, turintis pakankamai žinių, susijusių su tokia programinių įrangų gausa ir jų veikimo pobūdžio atpažinimu. Kitu atveju, laiku neatpažinus ir nesustabdžius procesų ar programai savaime išsitrynus, galima prarasti tyrimui reikšmingą pirminę informaciją, taigi ištirti bylą ir surasti asmenį, padariusį tokį nusikaltimą, tampa labai sudėtinga. Taigi, būtų sunku apibrėžti visus įmanomus metodus ir būdus, naudojamus darant nusikaltimus elektroninėje erdvėje, nes jie keičiasi, atsiranda vis naujų teisinėje veikloje dar negirdėtų kenkėjiškų programų.

2.3. Nusikaltimą elektroninėje erdvėje padaręs asmuo

Nusikaltimų elektroninėje erdvėje, numatytų BK 198, 198[1], 198[2] straipsniuose, subjektu gali būti fizinis ir juridinis asmuo. Šiuos nusikaltimus darantys asmenys neretai pasižymi aukštu intelektu, veikia profesionaliai, geba valdyti informacinės sistemos srautus, programas ir pritaikyti jas atlikdami savo nusikalstamas veikas elektroninėje erdvėje. Tačiau autorė nori pažymėti, kad ne visi nusikaltimus elektroninėje erdvėje darantys asmenys turi aukštą įgūdžių lygį ir veikia profesionaliai. Yra asmenų, kuriems įsilaužimas į kito vartotojo sistemą yra tarsi „žaidimas“[94] ir jie tiesiog bando ieškoti spragų jų informacinėse programose. Kaip buvo minėta anksčiau, tarp nusikaltėlio ir nukentėjusiojo yra kriminalistiškai reikšmingas ryšys. Nusikaltimus elektroninėje erdvėje darantys asmenys dažniausiai neatsitiktinai pasirenka savo aukas ir dažnai jų taikiniu tampa buvę darbdaviai ar mylimieji. Akivaizdu, kad čia svarbus ir nusikaltimo motyvas – kerštas. Kaip savo knygoje teigė Kyung-Shick, virtualioje erdvėje dažnai susiduria motyvuoti pažeidėjai ir tinkami jų taikiniai[95]. Išskiriant pagal motyvus nusikaltėliai skirstomi į šias grupes[96]:

1. Įsilaužėliai (vadinamieji *hakeriai*). 2020 metų sausio mėnesį Europos Sąjungos agentūra, atsakinga už vaistų reguliavimą, pranešė, kad įsilaužėliai iš serverių pavogė COVID-19 vakcinos dokumentus, kurie buvo nutekinti į internetą. Ši agentūra turėjo daugybę konfidencialių dokumentų,

[94] Choi, Kyung- Shick, *Risk factors in computer-crime victimization* (LFB Scholarly Publishing LLC: 2010), 14, žiūrėta 2021 m. vasario 15 d., http://web.b.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/ZTAwMHh3d19fNTIwNTI1X19BTg2?sid=7b099815-71bf-4d03-a4d4-d9054335d37f@pdc-v-sessmgr06&vid=0&format=EB&rid=1.
[95] Choi, Kyung-Shick. *Ibid*, 15.
[96] Darius Štitilis, *Supra note* 8, 20 .

susijusių su COVID-19 vakcina. Ikiteisminio tyrimo metu paaiškėjo, kad įsilaužėliai nuo lapkričio mėnesio neteisėtai gaudavo visus laiškus ir dokumentus, susijusius su eksperimentinių koronaviruso vakcinų vertinimu[97]. Vėliau šie dokumentai su pakeistu turiniu buvo nutekinti į įvairius tinklalapius, skleidžiant dezinformaciją apie šią vakciną ir taip norint įbauginti visuomenę. D. Štitilio teigimu, ši nusikaltėlių grupė yra unikali, nes, nepaisant to, kad jie gerai išmano apie kompiuterines programas ir jų sistemas, dažniausiai tokius nusikaltimus daro tiesiog iš nuobodulio arba norėdami pademonstruoti savo gebėjimus. Šios grupės atstovų dažniausias motyvas – noras patekti į kompiuterinę sistemą[98]. Pateikto pavyzdžio atveju tikėtina, kad motyvas – norėjimas įtikinti kitus savo tiesa ir įrodymas, kad „aš tai galiu padaryti“. Įsilaužėliai dar skirstomi į darbuotojus ir „svetimšalius“[99]. Toks skirstymas dažniausiai remiasi priklausomybe, pvz., darbo. Šis skirstymas labai panašus į mokslininko M. Shewardo organizacijų darbuotojų grupavimą į vidinius ir išorinius darbuotojus.

2. Tipiniai nusikaltėliai. Šių nusikaltėlių pagrindinis motyvas yra pinigai ir naudos gavimas. Tai dažniausiai suaugę asmenys, turintys išsilavinimą, dažnai susijusį su informacinėmis technologijomis, ir aukštą patirties lygį šioje srityje. Jie dažniausiai orientuojasi į nusikaltimus, susijusius su šnipinėjimu, sukčiavimu ar piktnaudžiavimu[100].

3. Vandalai. Šių asmenų tikslas dažniausiai būna žalos padarymas. R. Petrauskas ir D. Štitilis savo knygoje[101] išskyrė dvi grupes vandalų: naudotojus (tie, kurie turi teisėtą prieigą prie kompiuterinės sistemos, tačiau ja piktnaudžiauja) ir svetimšalius (tie, kurie neturi prieigos prie sistemos).

Mokslinėje literatūroje galime rasti ir daugiau skirstymų. Tarkime, užsienio literatūroje[102] pagal incidentus, įvykusius organizacijose, asmenys dažnai skirstomi į tris grupes: įmonių darbuotojus, pašalinius asmenis ir asmenis, užsiimančius organizuotu nusikalstamumu. Įmonių darbuotojai sudaro didžiausią grupę nusikaltėlių, nes turi lengvą prieigą prie kompiuterinės informacijos. Ši grupė dažniausiai vagia informaciją apie klientus ar sunaikina įmonės standžiuosiuose diskuose saugomus duomenis. Kaip nurodė M. Sheward[103], darbuotojai įmonei vienu metu yra ir didžiausias turtas, ir rizika. Savo knygoje M. Sheward apibrėžė konkrečius įvairiose įmonėse ir organizacijose vykdomus įsilaužimus į informacinę sistemą. Tokie įsilaužimai skirstomi į vidinius ir išorinius. Vidiniai – kai tokį nusikaltimą padarė darbuotojas, o išoriniai, dar kitaip vadinami

[97] „EU regulator: Hackers ‘manipulated’ stolen vaccine documents“, žiūrėta 2021 m. vasario 15 d., https://apnews.com/article/public-health-europe-coronavirus-pandemic-coronavirus-vaccine-56efa8e104f0509fa48381fce00b0de6.
[98] Darius Štitilis, *Supra note* 8, 20-21.
[99] Art Browker, Todd G. Shipley, *Supra note*, 23, 24.
[100] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 647.
[101] Darius Štitilis, Rimantas Petrauskas, *Supra note*, 83, 21.
[102] Mc Keown, G. Patrick, *Computer crimes and criminals*, National forum, http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=f5h&AN=9609192203&site=ehost-live.
[103] Mike Sheward, *Supra note*, 24, 12.

pašaliniais, – tai asmenys, kurie neturėjo nieko bendro su įmone, jų nesieja darbiniai santykiai nei dabar, nei praeityje. Vidinės kilmės incidentai dažniausiai išsiskiria tuo, kad apima vieno darbuotojo veiksmus, o išoriniuose dažniausiai dalyvauja daugiau asmenų[104]. Tačiau būna ir taip, kad įsilaužimus į sistemą organizuoja buvęs įmonės darbuotojas, tačiau jis veikia ne vienas, bet keliese, ir naudojami ne to darbuotojo prisijungimo duomenys. Kaip pavyzdį būtų galima paminėti klinikos „Grožio chirurgija“ įvykį[105], kai neteisėtai buvo perimta konfidenciali informacija, susijusi su klinikos pacientų duomenimis, o iš pacientų reikalauta užmokesčio grasinant paviešinti turimą informaciją.

Kalbant apie tokių nusikaltėlių profiliavimą elektroninėje erdvėje, Lietuvoje tai nagrinėjo L. Ruibytė ir B. Balsevičienė[106]. Užsienyje tokie profiliavimo modeliai yra plačiai paplitę ir naudojami tiriant nusikaltimus elektroninėje erdvėje. Literatūroje[107] išskiriamos šios pagrindinės profiliavimo grupės:

1. *Vaikai* (*Kiddie*). Ši grupė nenaudoja sudėtingų programų, pasitelkia kitų jau užprogramuotus modelius. Jie daro tokius nusikaltimus norėdami įrodyti kitiems, kad geba įsilaužti į kito vartotojo programas ir pasisavinti duomenis. Dažniausiai tai jauni, neturintys įgūdžių asmenys.

2. *Kibernetiniai pankai* (*Cyberpunks*). Ši grupė yra labiau įgudusi daryti tokius nusikaltimus, jie dažniausiai jauni. Veikia skleisdami virusus ar rengdami DOS atakas.

3. *Senieji laikmečiai* (*Old times*). Ši grupė yra labiausiai kvalifikuota ir išmananti informacines technologijas. Dažniausiai jų amžius – vidutinis arba vyresnis. Veikia neteisėtai prisijungdami prie kito asmens svetainės ir skleidžia neteisingą informaciją iš teisėto svetainės vartotojo.

4. *Nelaimingas darbuotojas* (*Unhappy insider*). Šie asmenys būna įvairaus amžiaus, laikomi vieni pavojingiausių darant tokio pobūdžio nusikaltimus. Jie veikia vedini kerštо motyvų ir dažniausiai tiesioginės prieigos būdu, jungiantis tiesiogiai prie sistemos, o ne internetu.

Tai tik dalis profiliavimo grupių nusikaltimus elektroninėje erdvėje atliekančių asmenybių tipams nustatyti. Šie profiliavimai galėtų padėti suprasti nusikaltimų elektroninėje erdvėje priežastis ir motyvus bei palengvinti tokių asmenų identifikavimą. Deja, Lietuvoje nėra išsamaus tokių grupių išskyrimo ir nusikaltimų elektroninėje erdvėje profiliavimo metodas, kaip atskleidė valstybinio audito ataskaita, nėra pakankamas ir neapima visų nusikaltimų, padarytų elektroninėje erdvėje[108]. Akivaizdu, kad didžioji dalis asmenų, darančių tokio pobūdžio nusikaltimus, turi gerų įgūdžių dirbdami su

[104] Mike Sheward, *Supra note*, 24, 13.
[105] „Marijampoliečiai įtariami dėl „Grožio chirurgijos“ pacientų duomenų vagysčių“, žiūrėta 2021 m. vasario 15 d., https://www.etaplius.lt/marijampolieciai-itariami-del-grozio-chirurgijos-pacientu-duomenu-vagysciu.
[106] Laima Ruibytė, Birutė Balsevičienė, „Kriminalinio profiliavimo pritaikymo galimybės nusikaltimų įvykdytų elektroninėje erdvėje tyrimui“, žiūrėta 2021 m. vasario 15 d., https://repository.mruni.eu/bitstream/handle/007/15002/Balsevi%20ien%20.pdf?sequence=1.
[107] Art Browker, Todd G. Shipley, *Supra note*, 23, 23.
[108] *Supra note* 3, 10.

įvairiomis programomis, geba pasisavinti kito vartotojo duomenis ir gauti konfidencialią informaciją (slaptažodžius, ID ir t. t.). Nepaisant to, kad nusikaltimų elektroninėje erdvėje kaltininkai veikia užsimaskavę ir slėpdami savo tapatybę, šie nusikaltimų subjektai, kitaip nei kitose neteisėtose veikose, išsiskiria sumanumu, aukštu intelektu ir gebėjimu maskuotis, o tai tik dar labiau apsunkina tokių asmenų identifikavimą.

2.4. Nusikaltimų elektroninėje erdvėje pasikėsinimo dalykas

Nusikaltimų elektroninėje erdvėje aukomis gali tapti ir fiziniai, ir juridiniai asmenys. Milijardai žmonių pasaulyje kasdien internete dalijasi įvairiais savo asmeniniais įrašais ir informacija dažnai net nesusimąstydami, kad tokia informacija gali būti nukreipta prieš juos pačius. Neretai nusikaltimų virtualioje erdvėje aukomis tampa labiau pažeidžiami, patiklesni ir išsiblaškę asmenys. Užpuolikai, pasinaudodami aukos pažeidžiamumu, renka apie ją informaciją, persiunčia kenkėjiškas programines įrangas ir t. t. Taip pat aukomis dažnai tampa apgauti darbuotojai, kurie per klaidą atskleidžia vartotojų vardus ir slaptažodžius arba suteikia papildomą prieigą prie duomenų sistemos. A. Šidlauskas ir S. Ungurytė-Ragauskienė savo straipsnyje teigia, kad „kai išmokstama atakas atremti technologinėmis priemonėmis, psichologinis manipuliavimas sistemos vartotojais ar operatoriais tampa vis patrauklesnis“[109]. Manoma, kad nusikaltimų elektroninėje erdvėje kaltininkai, rinkdamiesi savo aukas, remiasi socialinės inžinerijos metodais. Išskiriami 4 tokie psichologinės įtakos veiksniai[110]:

1. Socialinis programavimas ir smalsumas. Šių asmenų grupė dažniausiai pasirenkama dėl jų noro parodyti savo gebėjimus ir būti pirmiems, todėl jie net nedvejodami gali atskleisti prašomą informaciją.

2. Baimė ir skubėjimas. Tokie asmenys pasirenkami dėl jų emocionalumo ir noro kuo greičiau viską padaryti (pvz., gavus laišką su nuoroda į kenkėjišką programą, neįsigilinus į jo turinį), t. y. kai emocijų vedini jie priima skubotus sprendimus.

3. Pranašumas ir pripažinimas. Tokiai grupei žmonių nusikaltėliai neretai sukuria iliuziją, kad jie gaus kažkokios naudos (atlygį).

4. Pasitikėjimas ir empatija. Šis veiksnys remiasi patiklumu ir autoritetu. Aklai tikint kitais žmonėmis (autoritetais), dažnai bijoma papriešatarauti ir išreikšti abejones[111].

[109] Aurimas Šidlauskas, Svajūnė Ungurytė-Ragauskienė, „Iššūkiai kibernetiniam saugumui: socialinė inžinerija institucinio izomorfizmo kontekste“, *Mokslinis žurnalas*, 2020, 392.
[110] Aurimas Šidlauskas, Svajūnė Ungurytė-Ragauskienė, *Ibid*, 392.

Manoma, kad šie išskirti veiksniai yra reikšmingai susiję su nusikaltimų elektroninėje erdvėje pasirenkamomis aukomis ir jų asmenybėmis. Lietuvoje šis metodas nėra pakankamai išnaudojamas. Lietuvos nacionalinio kibernetinio saugumo centro (toliau – NKSC) 2019 m. ataskaitoje apie jį užsiminta, tačiau informacija – daugiau rekomendacinio pobūdžio, susijusi su rizikos valdymo aspektais. NKSC teigimu, organizacijos, kurios tampa šių nusikaltimų aukomis, dažnai atitinka saugumo politikos kriterijus *de jure*, tačiau organizacinė ir techninė informacinio saugumo atitiktis *de facto* nebūna visiškai įgyvendinamos[112]. Ši priežastis atveria kelią asmenims pasinaudoti tokiomis techninėmis spragomis ir taip įdiegti kenkėjišką programą ar gauti prieigą prie duomenų.

Pažymėtina, kad užsienyje renkami duomenys apie auką yra išskiriami į vieną iš pagrindinių nusikaltimų elektroninėje erdvėje tyrimo procesinių veiksmų ir vadinami *viktimologija*. Šio proceso metu renkama informacija apie auką, bandoma rasti užuominų, kodėl būtent ji ja tapo ir tiriama, galbūt auka turėjo kokių sąsajų su kaltininkais[113]. Turimi duomenys apie auką gali padėti atskleisti daug informacijos apie kaltininką ir jo motyvus darant tokio pobūdžio nusikaltimus. Nusikaltėliai aukas dažnai renkasi pagal jų naudojamą programinę įrangą bei atsižvelgdami į tai, kaip apsaugoti jų duomenys, ar jie naudojasi kokiomis apsaugos priemonėmis ir kt.[114] Teismų praktikoje dažniausiai išryškėja šios aukų grupės: mylimieji, kažkada turėję intymius santykius[115], buvę ar esami darbuotojai[116], pašaliniai asmenys. 2019 m. FBI pateiktoje ataskaitoje „Dėl nusikaltimų internete“ yra išskiriamos tokių nusikaltimo aukų amžiaus grupės[117]:

Amžius	**Bendras skaičius**
Iki 20 metų	10 724
20–29 metų	44 496
30–39 metų	52 820
40–49 metų	51 864
50–59 metų	50 608
Daugiau nei 60 metų	68 013

1 lentelė. Nusikaltimų elektroninėje erdvėje aukų amžiaus grupės

[112] Nacionalinio kibernetinio saugumo būklės ataskaita 2019, NKSC, žiūrėta 2021 m. vasario 15 d., https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf, 19.
[113] Art Browker, Todd G. Shipley, *Supra note*, 23, 16.
[114] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 654.
[115] Lietuvos Aukščiausiojo Teismo 2015 m. sausio 6 d. nutartis, priimta baudžiamojoje byloje Nr. 2K-138/2015, eteismai, žiūrėta 2021 m. vasario 15 d., https://eteismai.lt/byla/148386211638579/2K-138/2015.
[116] Lietuvos Aukščiausiojo Teismo 2019 m. liepos 2 d. nutartis, priimta baudžiamojoje byloje Nr. 2K-199-648/2019, eteismai, žiūrėta 2021 m. vasario 15 d., https://eteismai.lt/byla/113482577300847/2K-199-648/2019.
[117] *2019 internet crime report*, 16.

Kaip matoma iš pateiktos lentelės, dažniausiai tokiomis aukomis tampa vyresni nei 60 metų, o rečiausiai – jaunesni nei 20 metų asmenys. Tačiau internetu vis dažniau pradeda naudotis nepilnamečiai, o ši grupė asmenų yra itin pažeidžiama, nes yra mažiausiai informuota apie tokio pobūdžio nusikaltimus. Europos Komisija, atsižvelgdama į tai, kad vis dažniau tokiomis aukomis tampa vaikai ar pagyvenę asmenys, kuriems gali trūkti būtinų skaitmeninių įgūdžių arba žinių apie jų turimas teisių gynimo priemones, 2020 m. parengė Strategiją nusikaltimų elektroninėje erdvėje aukų teisėms apginti. Šioje strategijoje numatyta, kad nusikaltimų elektroninėje erdvėje aukoms turi būti sudarytos palankesnės sąlygos pranešti apie tokio pobūdžio nusikaltimus ir teikiama reikiama pagalba[118]. Todėl labai svarbu, kad visuomenė būtų vis geriau informuojama apie tokius nusikaltimus ir žmonės netaptų šių nusikaltimų aukomis, o tapę žinotų, kur kreiptis, ir nebijotų ginti savo interesus.

Taigi, šių nusikaltimų aukų asmeninių savybių ir jų skirtumų charakteristika svarbi, nes gali padėti tyrėjams suprasti nusikaltimų priežastis, motyvus ir tai, kokio tikslo nusikaltėliai siekė. Gauta informacija galėtų suteikti žinių apie nusikaltimo padarymo būdą, situaciją ir kaltininką.

2.5. Nusikaltimų elektroninėje erdvėje situacija

Nusikaltimų elektroninėje erdvėje charakteristika, leidžianti suprasti juos kaip besiskiriančius nuo įprastų nusikaltimų, yra terpė, kurioje jie įvyksta – vadinamoji elektroninė erdvė[119]. Viena iš didžiausių problemų tokio pobūdžio nusikaltimų tyrime yra ta, kad auka ir nusikaltėlis tuo pačiu metu gali būti bet kurioje pasaulio vietoje[120]. Padaryti tokio pobūdžio nusikaltimus gali bet kas, niekada fiziškai net nebuvęs nusikaltimo vietos jurisdikcijoje[121]. Nusikaltimo situacijos analizė yra itin svarbi tiriant nusikaltimus elektroninėje erdvėje. Kaip buvo minėta anksčiau, ji glaudžiai susijusi su nusikaltimą padariusio asmens asmenybe ir nusikaltimo padarymo būdu, nes nusikaltėlis atsižvelgia į situaciją, kuri yra susiklosčiusi ir kurioje ketina įgyvendinti savo neteisėtus tikslus[122]. Bet kurioje žmogaus veikloje susiklosto faktinių aplinkybių visuma, sudaranti tam tikrą elementų sistemą, vadinamą situacija[123]. Nusikaltimo padarymo būdas priklausys nuo šių nusikaltimų elektroninėje erdvėje situacijos aplinkybių: nusikaltimą padariusio asmens veiksmų vietos ir laiko, ryšio su auka ir informacinių technologijų įgūdžių.

Darbo analizuojami BK 198, 198[1], 198[2] straipsniai yra formalios nusikaltimo sudėties, o tai reiškia, kad nusikaltimų padarymo vieta bus laikoma ta, kurioje veikė nusikaltimą padaręs asmuo.

[118]2020-2025 m. ES strategija dėl nusikaltimų aukų teisių, Eur Lex, 2020, 5.
[119] Margarita Dobrynina, Vaida Kalpokas, Simonas Nikartas ir kt., *Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai* (Vilnius, 2011), 325.
[120] Choi, Kyung-Shick. *Supra note*, 94, 17.
[121] Gosh Sumit, Elliot Turini *Supra note*, 43, 29.
[122] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 655.
[123] Snieguolė Matulienė, Vidmantas Egidijus Kurapka, *Kriminalistika teorija ir technika* (Vilnius:2012), 179.

Nusikaltimo padarymo vietos nustatymas yra itin reikšmingas, nes gali suteikti informacijos apie kaltininkus ir įkalčius. Čia ypač svarbus kaltininko ir aukos tarpusavio ryšys. Pavyzdžiui, tokį nusikaltimą darantis asmuo gali teikti pirmenybę tam tikrai interneto sričiai, nes tai traukia aukas. Asmuo gali rinktis su juo asmeniškai susijusią virtualią erdvę, kad būtų lengviau susitikti su aukomis (pvz., žaidimų tinklalapiai ir kt.). Taip pat gali pasitaikyti situacijų, kai kaltininkas, gerai apgalvodamas pasekmes, žalingus padarinius atlieka toli nuo jo paties gyvenamosios teritorijos, kad ji būtų dar platesnė ir būtų sunku jį rasti[124]. Dažnu atveju nusikaltėliai pasirenka konkrečias virtualias erdves, kurios atitinka jų poreikius, o tai gali suteikti tyrėjams informacijos apie pažeidėją.

Pažymėtina, kad nusikaltimo padarymo vieta ir padarinių kilimo vieta gali nesutapti. Taip būna, kai nusikaltimas vykdomas netiesioginiu būdu, ir atvirkščiai – esant tiesioginiam nusikaltimo padarymui[125]. Pavyzdžiui, kriminalinės policijos nusikaltimų nuosavybei tyrimo pareigūnai pranešė baigę ikiteisminį tyrimą dėl neteisėto elektroninių duomenų perėmimo ir panaudojimo bei neteisėto prisijungimo prie informacinės sistemos (BK 198, 198[1] straipsniai)[126]. Šioje situacijoje kaltininkas, buvęs įmones darbuotojas, iš savo namų kompiuterio pasinaudodamas savo turima prieiga neteisėtai prisijungė prie įmonės dokumentų ir taip stebėjo sistemoje esančius neviešus duomenis. Kitame pavyzdyje kaltininkas veikė tiesioginiu būdu[127]: asmuo buvo nuteistas pagal BK 198 straipsnio 1 dalį už tai, kad būdamas darbo vietoje ir naudodamasis darbo kompiuteriu neteisėtai prijungė savo atmintinę, kurioje buvo įdiegta programa, skirta pašalinti, pridėti ar pakeisti „Windows“ operacinės sistemos vartotojo vardą ar slaptažodį. Tokiais veiksmais buvo pašalinti vartotojo duomenys ir sukurtas naujas prisijungimo vardas, tokiu būdu pažeidžiant informacinės sistemos apsaugos duomenis, fiksuotos ir perimtos kitos paskyros vartotojo teisės. Beveik identiškai yra ir su nusikaltimo padarymo laiku. Kaltininkai, rinkdamiesi netiesioginį nusikaltimo padarymo būdą, dažniausiai veikia nakties metu, kai mažesnė tikimybė būti pastebėtiems, o pasirinkdami tiesioginį būdą veikia tos įmonės ar organizacijos darbo metu.

Taigi, šios išvardintos aplinkybės gali suteikti svarios informacijos nusikaltimą tiriančiam pareigūnui. Kaltininko pasirinkimo savybių visuma (auka, nusikaltimo padarymo vieta ir laikas, nusikaltimo padarymo būdas) tyrėjui suteikia esminės informacijos apie nusikaltimo padarymo situaciją ir kitas reikšmingas bylai aplinkybes.

---

[124] Eoghan Casey, *Digital evidence and computercrime* (London Academic press 2004), 130, žiūrėta 2021 m. vasario 15 d., http://web.a.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/ZTAwMHh3d19fMTg5NDY0X19BTg2?sid=445292f0-0692-45da-85e9-9a91245afc38@sessionmgr4008&vid=18&format=EB&rid=2.

[125] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 656.

[126] „Dar viena byla dėl nusikaltimų elektroninėje erdvėje perduota teismui“, žiūrėta 2021 m. vasario 15 d., https://vilnius.policija.lrv.lt/lt/naujienos/dar-viena-byla-del-nusikaltimu-elektronineje-erdveje-perduota-teismui.

[127] *Supra note*, 116.

3. NUSIKALTIMŲ, NUMATYTŲ LR BK 198, 198[1], 198[2] STRAIPSNIUOSE, PRAKTINIAI ATSKLEIDIMO YPATUMAI

3.1. Tyrimo planavimas ir bendradarbiavimas su kitomis institucijomis

Kiekvienas efektyvus nusikaltimo tyrimas pradedamas nuo planavimo. Ikiteisminio tyrimo planavimas yra kontempliacijos procesas, kurio metu iš anksto apsvarstomi tyrimo tikslai ir numatomi veiksmai, kurie grindžiami tam tikromis taisyklėmis (planu ir logika), padedančiomis pasirinkti geriausią procedūrą šiems tikslams pasiekti[128]. Nusikaltimų elektroninėje erdvėje tyrimai yra itin sudėtingi ir turi nemažai išskirtinumų, lyginant su tradiciniais nusikaltimais, padarytais fizinėje erdvėje. Tokiems tyrimams atlikti būtinos ne tik teisinės, bet ir specialiosios, konkrečiai informatikos žinios, kibernetinio saugumo suvokimas. Literatūroje teigiama, kad „specialių žinių prigimtis, jų poreikis baudžiamajame procese bei paskirtis – bylai ištirti būtinų aplinkybių išaiškinimas“[129]. Manoma, kad nusikaltimų elektroninėje erdvėje tyrėjui reikia visų savybių, kaip ir bet kuriam kriminalistui, ir dar kelių papildomai[130]. Todėl šie nusikaltimai yra priskirti specializuotų padalinių kompetencijai.

Prieš pradedant ikiteisminį tyrimą, dažniausiai vertinama išankstinė informacija ir nustatoma, ar yra pagrindas pradėti ikiteisminį tyrimą[131]. Pagal BK 198, 198[1], 198[2] straipsnius, ikiteisminis tyrimas gali būti pradėtas dviem pagrindais: gavus skundą, pranešimą ar pareiškimą arba prokurorui ar ikiteisminio tyrimo pareigūnui nustačius šių nusikaltimų požymius. Priklausomai nuo to, kokia informacija buvo surinkta, sudaromas svarbiausių tyrimo veiksmų planas, kuriame turi būti numatoma: specialių tyrimo priemonių panaudojimas, kratos, apžiūros ir poėmiai, liudytojų apklausos, atpažinimai ir akistatos[132]. Pažymėtina, kad planuojant nusikaltimo tyrimą negalima remtis analogijomis ar kriminalistikos rekomendacijomis. Šios turi būti kūrybiškai pritaikytos konkrečiai situacijai[133]. Tačiau labai svarbu turėti šiuolaikinės praktikos poreikius atitinkančias šių nusikaltimų tyrimo metodikas, kuriose būtų pateikti praktiniai patarimai, detalizuojantys šių nusikaltimų tyrimo procesą nuo pat ikiteisminio tyrimo pradžios iki pabaigos.

---

[128] Žaneta Navickienė, Snieguolė Matulienė, Egidijus Vidmantas Kurapka ir kt., *Planning ab initio pre-trial investigation as the condition for a more effective investigation of crimes,* 388.
[129] Egidijus Vidmantas Kurapka, Snieguolė Matulienė, Eglė Bilevičiūte ir kt, *Specialių žinių taikymo nusikaltimų tyrime mokslinė koncepcija ir jos realizavimo mechanizmas,* (Vilnius: 2012), 20.
https://repository.mruni.eu/bitstream/handle/007/16906/9789955194927.pdf?sequence=1&isAllowed=y.
[130] Littlejohn Shinder, Michael Cross, „Understanding the people on the scene“, žiūrėta 2021 m. vasario 25 d., https://www.sciencedirect.com/topics/computer-science/cybercrime
[131] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 659.
[132] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 660.
[133] Janina Juškevičiūtė, Snieguolė Matulienė, Daiva Kairienė ir kt., *Kriminalistika* (Vilnius 2014), 29.

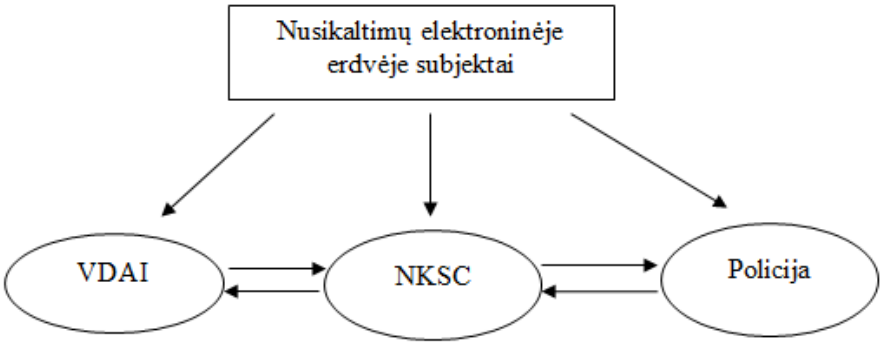
Tyrimo pradžioje svarbu išsiaiškinti kuo daugiau detalių ir aplinkybių, susijusių su byla, iki pradedant ikiteisminį tyrimą, nes ši informacija gali padėti tinkamai nustatyti tyrimo kryptį pradiniame tyrimo etape, o vėliau – ir pasirinkti tinkamus ikiteisminio tyrimo taktinius būdus atliekant pačius tyrimo veiksmus.

Nusikaltimų tyrimas – tai sudėtingas procesas, reikalaujantis itin daug pastangų ir laiko, todėl jis nebūtų įmanomas be kitų ikiteisminio tyrimo subjektų veiksmų suderinimo[134]. Lietuvoje nusikaltimus elektroninėje erdvėje užkardo, atskleidžia ir tiria Lietuvos kriminalinės policijos biuras bei daugelyje apskričių įsteigti kriminalinės policijos nusikaltimų elektroninėje erdvėje specializuoti padaliniai[135]. Informacinių technologijų tyrimus (ekspertizes) atlieka kriminalistinių tyrimų centro informacinių technologijų tyrimo skyrius[136].

Pastaruoju metu viena iš nusikaltimų elektroninėje erdvėje problemų yra šios ekspertizės tyrimo metodikų ir besispecializuojančių šioje srityje specialistų bei ekspertų trūkumas[137]. Lietuvoje, be policijos, šiuos nusikaltimus fiksuoja, tiria[138] NKSC ir Valstybinė duomenų apsaugos inspekcija (toliau – VDAI). NKSC yra atsakinga už kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę[139]. VDAI[140] atlieka tyrimus ir patikrinimus, taip pat teikia pagalbą tiriant incidentus, susijusius su asmens duomenų pažeidimais, ir bendradarbiauja su kitomis institucijomis. Apie nusikaltimą elektroninėje erdvėje nukentėję asmenys praneša vienai iš šių institucijų, o šios pagal poreikį informuoja viena kitą ir tarpusavyje keičiasi svarbia informacija, susijusia su įvykiu (6 pav.). Vienas iš ryškiausių incidentų pandemijos metu – kai internete buvo nutekinti „CityBee“[141] įmonės klientų duomenys. Dėl įvykio įmonės administracija kreipėsi į Lietuvos policiją. Buvo pradėtas ikiteisminis tyrimas pagal BK 198 ir 198[1] straipsnius, taip pat siekiant nustatyti šio įvykio priežastį papildomai buvo kreiptasi į NKSC. Dėl didelio masto privačių duomenų nutekinimo tyrimą pradėjo ir VDAI, kuri dėl šio atvejo ištyrimo bendradarbiauja su NKSC[142].

---

[134] Žaneta Navickienė, „Model of organising pre-trial investigation in tactics of criminalistics“, (daktaro disertacija, Mykolo Romerio universitetas, 2011), 28.
[135] *Supra note* 3, 15.
[136] KTC atliekamų tyrimų ir ekspertizių sąrašas, žiūrėta 2021 m. vasario 25 d., https://ktc.policija.lrv.lt/lt/veiklos-sritys/tyrimai-ir-ekspertizes/ktc-atliekamu-tyrimu-ir-ekspertiziu-sarasas.
[137] „Ar esame pasiruošę spręsti IT specialistų trūkumo klausimą?“, žiūrėta 2021 m. vasario 25 d., https://www.vz.lt/paslaugos/2020/05/11/ar-esame-pasiruose-spresti-it-specialistu-trukumo-klausima.
[138] Atkreiptinas dėmesys į tai, kad NKSC ir VDAI institucijos neturi ikiteisminių tyrimo įstaigų įgaliojimų atlikti ikiteisminį tyrimą, jos tiria incidentus, pranešimus ir įvykius susijusius su kibernetiniais nusikaltimais, tačiau neatlieka ikiteisminio tyrimo veiksmų.
[139] Nacionalinis kibernetinio saugumo centras, žiūrėta 2021 m. vasario 25 d., https://www.nksc.lt/veikla.html
[140] „Dėl valstybinės duomenų inspekcijos vykdomų ir patikrinimų atlikimo taisyklių patvirtinimo“ TAR, žiūrėta 2021 m. vasario 25 d., tyrimų https://www.e-tar.lt/portal/lt/legalAct/3416a700a88411e9b474d97de297fe08.
[141] „Pradėti tyrimai dėl asmens duomenų nutekinimo“, žiūrėta 2021 m. vasario 25 d., https://epilietis.lrv.lt/lt/naujienos/pradeti-tyrimai-del-asmens-duomenu-nutekinimo.



6 pav. Pranešimai apie nusikaltimą elektroninėje erdvėje ir institucijų bendradarbiavimas[143].

Nors šių institucijų bendradarbiavimas yra itin svarbus tiriant tokio pobūdžio nusikaltimus, tačiau, remiantis pateikta valstybinio audito ataskaita[144], matomos tam tikros bendradarbiavimo spragos. Minėta ataskaita atskleidė, kad NKSC neperduoda policijai visos informacijos apie incidentus, kurie turėjo nusikaltimų elektroninėje erdvėje požymių, ir nurodo nukentėjusiesiems patiems kreiptis į policiją. M. Šatas savo disertacijoje pabrėžė, kad stebint Lietuvos teisėsaugos institucijų veiklą ir nusikalstamumo dinamiką nekyla abejonių, kad pagrindinė šių problemų priežastis – teisėsaugos institucijų bendradarbiavimo trūkumas[145].

Todėl šiuo atveju analizuojant pranešimus apie elektroninėje erdvėje padarytas nusikalstamas veikas matyti, jog stokojama bendrų koordinacinių veiksmų, užtikrinančių tikslinės informacijos perdavimą kitai institucijai, įgaliotai priimti sprendimus. Šiuo metu besiklostanti praktika, kai asmenų pranešimai neperduodami reikiamai institucijai, rodo poreikį peržiūrėti pranešimų apie įvykius elektroninėje erdvėje tvarką. Be to, egzistuojanti praktika yra ydinga, nes atsižvelgiant į tai, kad tokio pobūdžio nusikaltimai yra priskiriami latentiniams, asmenys neretai apskritai dvejoja, ar pranešti apie įvykusius incidentus nesulaukus pagalbos iš institucijos, į kurią buvo kreipiamasi, pakartotinai į policiją gali būti ir nebesikreipiama.

Nenustatyti ir neištirti įvykiai elektroninėje erdvėje sudaro grėsmes visam viešajam saugumui, be to, ateityje gali kilti reali grėsmė tokio pobūdžio nusikaltimų užkardymo kontrolės praradimui. Atsižvelgiant į minėtą audito ataskaitą ir kibernetinio saugumo įstatyme įtvirtintas nuostatas, pirma, reikėtų nustatyti griežtai apibrėžtas ir detalias institucijų bendradarbiavimo gaires ir įtvirtinti imperatyvų reikalavimą, kuriuo NKSC visais atvejais turėtų pranešti policijai apie galimai įvykdytus nusikaltimus elektroninėje erdvėje, nes kibernetinio saugumo įstatymas šiuo metu nenumato tokio privalomo reikalavimo ir tarsi palieka diskrecijos teisę institucijai pačiai spręsti,

[143] *Supra note* 3, 29.
[144] *Supra note* 3, 29.
[145] Mindaugas Šatas, *Prokuroro ir ikiteisminio tyrimo pareigūno bendradarbiavimas tiriant sunkius nusikaltimus* (Vilnius, 2011), 25.

kuriuos incidentus perduoti, o kurių ne. Antra, peržvelgti incidentų fiksavimo elektroninėje erdvėje sistemas, kurios galėtų veikti efektyviau: atskirtų ir identifikuotų galimų nusikaltimų kibernetinėje erdvėje atvejus.

Pažymėtina, kad viena iš nusikaltimų elektroninėje erdvėje problemų yra jų veikimas pasauliniu mastu, taigi, auka gali būti bet kurioje pasaulio valstybėje[146]. Atsižvelgiant į tai labai svarbu, kad valstybių įstatyminės bazės dėl nusikaltimų elektroninėje erdvėje būtų kuo išsamiau apibrėžtos ir kriminalizuotos nusikalstamos veikos.

Vienas ryškiausių 2000 m. įvykusių incidentų[147] buvo susijęs su Filipinų valstybės teisinio reguliavimo problema. Buvo nustatyta, kad filipinietis Onelas de Guzmanas (informatikos studentas) sukūrė ir paskleidė „meilės klaidos“ virusą, kuris užkrėtė daugiau nei 45 milijonus kompiuterinių sistemų visame pasaulyje, tačiau už šiuos savo neteisėtus veiksmus asmuo atsakomybėn patrauktas niekada nebuvo. Filipinų įstatymuose tokie nusikaltimai (įsilaužimas ir virusų platinimas) kriminalizuoti nebuvo, nors JAV ir turėjo įtvirtinus įstatymus, susijusius su tokio pobūdžio veikomis. Taigi, O. de Guzmanas negalėjo būti perduotas JAV, nes jo padaryti neteisėti veiksmai Filipinuose nebuvo laikomi nusikaltimais. Šis pavyzdys tik dar kartą patvirtina, koks bendradarbiavimas svarbus ne tik tiriant padarytą nusikaltimą, tačiau įrodo ir bendrai suderintos teisinės bazės svarbą: šalių įstatymuose įtvirtinta atsakomybė už tokio pobūdžio veikas. Bendradarbiavimas su užsienio šalių teisėsaugos institucijomis, operatyvus apsikeitimas informacija ir dalinimasis gerąja patirtimi yra būtinos sėkmingos kovos su tokio pobūdžio nusikalstamumu sąlygos.

Europolas inicijuoja ir koordinuoja ES valstybių narių keitimąsi duomenimis ir žvalgybine informacija tarp nacionalinių teisėsaugos institucijų[148]. Taip pat esant poreikiui yra galimybė sudaryti tarptautinę jungtinę tyrimo grupę. Europos Sąjungos bendradarbiavimo baudžiamosios teisenos srityje agentūra (*Eurojustas*) teikia finansavimą ir lengvina tokių grupių formavimą[149]. Jungtinei tyrimo grupei sudaryti reikalingas teisinis pagrindas ir tarptautinis teisės aktas (7 pav.). Minėta grupė sudaroma, jei Lietuvoje atliekamas sudėtingas, daug pastangų reikalaujantis ikiteisminis tyrimas, susijęs su kitomis valstybėmis, kuriose būtina atlikti suderintus ikiteisminio tyrimo veiksmus[150]. Šios grupės sudarymas gali padėti pagreitinti ir palengvinti tyrimui reikšmingų duomenų rinkimą.

---

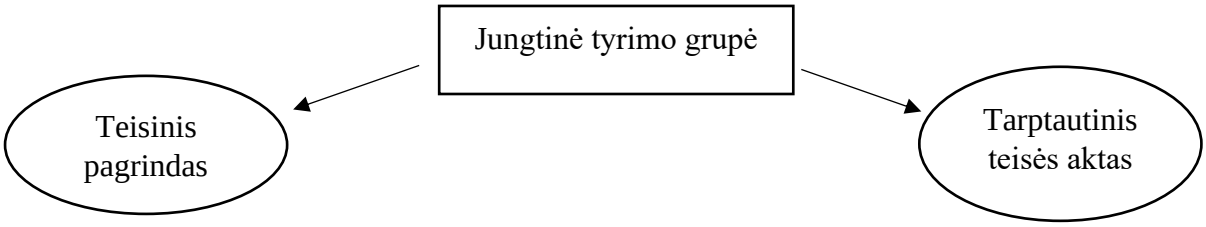
[146] Robert Moore, *Supra note*, 26, 24.

[147] „Love Bug's creator tracked down to repair shop in Manila“, BBC news, žiūrėta 2021 m. vasario 25 d., https://www.bbc.com/news/technology-52458765.

[148] Tarptautinės operacijos, Lietuvos kriminalinės policijos biuras, žiūrėta 2021 m. vasario 25 d., https://lkpb.policija.lrv.lt/lt/tarptautinis-bendradarbiavimas/tarptautines-operacijos

[149] Komisijos komunikatas Europos Parlamentui ir Tarybai Antroji ES vidaus saugumo strategijos įgyvendinimo ataskaita, žiūrėta 2021 m. kovo 3 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52013DC0179&from=EN.

[150] Konvencija dėl Europos Sąjungos valstybių narių savitarpio pagalbos baudžiamosiose bylose, kurią pagal Europos Sąjungos sutarties 34 straipsnį patvirtino Taryba, žiūrėta 2021 m. kovo 2 d., http://www.infolex.lt/ta/66668:str13.



7 pav. Jungtinės tyrimo grupės sudarymas (sudaryta autorės).

Apibendrinant galima teigti, kad tyrimo planavimas yra viena svarbiausių sėkmingo rezultato dalių. Jis susideda iš pirminės informacijos įvertinimo, versijų iškėlimo, tyrimo tikslų ir būdų versijoms patikrinti nustatymo[151]. Planuojant tyrimo eigą ir veiksmus apžvelgiamas ir bendradarbiavimo poreikis. Norint užkirsti kelią tokiems nusikaltimams būtini subalansuoti organizacijų, kurios patyrė žalą, teisėsaugos institucijų, kriminalistinių tyrimų (teismo ekspertizių) ir informacinių technologijų specialistų veiksmai. To siekiant pirmiausia organizacijos turėtų nepamiršti pašalinti trūkumų, tokių kaip neišvystytos prevencinės, detekcinės, korekcinės kontrolės priemonės[152] savo naudojamoje įrangoje privalėtų įdiegti saugias sistemas ir programas, kurios padėtų apsaugoti nuo bet kokio neteisėto įsilaužimo į jų operacines sistemas[153]. Europos Sąjunga kartu su telekomunikacijų operatoriais pateikė kelis patarimus, kaip fiziniams asmenims apsisaugoti nuo kibernetinių išpuolių: saugotis nepageidaujamų el. laiškų ir žinučių, nustatyti sudėtingą WI-FI tinklo slaptažodį, įdiegti antivirusines sistemas ir nuolat atnaujinti įrenginius[154]. Bendradarbiavimas tiriant nusikaltimus elektroninėje erdvėje tiek pačioje šalyje, tiek tarptautiniu ar nacionaliniu lygmeniu (jei reikalinga) yra neatsiejama minėtų nusikaltimų tyrimo dalis. Todėl svarbu, kad institucijos veiktų bendrai, sinerginiais veiksmais: geranoriškai, aiškia ir nustatyta tvarka dalintųsi informacija ir stengtųsi kuo išsamiau atskleisti tokio pobūdžio nusikaltimus.

3.2. Pagrindinės keliamos versijos bei jų tikrinimas

Kriminalistinės versijos – tai tam tikros nusikaltimo rūšies faktiniai duomenys, pagrįsti įvairių jų aplinkybių prielaidomis, kuriomis remiantis aiškinama bylai reikšmingų duomenų kilmė bei jų tarpusavio ryšiai, jų pagalba modeliuojamos veikos darymo mechanizmas ir logiškai pagrindžiamas jos nagrinėjimas[155]. Vienas svarbiausių tyrimo proceso elementų yra tinkamai ir laiku atliekamas

[151] Janina Juškevičiūtė, Snieguolė Matulienė, Daiva Kairienė ir kt., *Supra note,* 133, 31.
[152] *Supra note,* 112.
[153] Mohammad Talib, Virginiah Sekgwathe, *Supra note,* 27.
[154] Tips for cybersecurity when working from home, žiūrėta 2021 m. kovo 6 d., https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home.
[155] Janina Juškevičiūtė, Snieguolė Matulienė, Daiva Kairienė ir kt., *Supra note,* 133, 35.

nusikaltimo tyrimo versijų kėlimas ir jų tikrinimas[156]. Literatūroje[157] versijos dažnai tapatinamos su mokslinėmis hipotezėmis, tačiau jų skirtumas – jog pastarosios keliamos konkrečiam nusikaltimui, o ne bendriems moksliniams, egzistenciniams klausimams išaiškinti.

Ikiteisminio tyrimo tyrėjas, turėdamas skurdžią pradinę informaciją apie įvykusį incidentą, jau vykdamas į nusikaltimo vietą gali iškelti tipines versijas, būdingas šių rūšių nusikaltimams[158]. Nusikaltimų elektroninėje erdvėje tyrimo versijos priklausys nuo turimų duomenų ir konkrečios situacijos. Mokslinėje doktrinoje[159] versijos skirstomos į bendrąsias, atskirąsias ir detaliąsias. Kelios iš bendrųjų tipinių šių nusikaltimų tyrimų versijų:

1. Informacinės ar kompiuterinės sistemos gedimas. Ši versija galėtų pasitvirtinti, jei nukentėjusysis dėl nežinojimo ar per klaidą pranešė apie, jo manymu, galimai įvykusį nusikaltimą, nors iš tikrųjų tai informacinėje sistemoje įvykęs gedimas.

2. Netinkamas įrenginių naudojimas. Ši versija panaši į pirmąją, tačiau skirtumas – kad šiuo atveju pats asmuo netinkamai elgėsi su įrenginiais.

3. Neteisėta prieiga prie informacinės ar programinės sistemos. Ši versija patvirtintų, kad ištiesbuvo įvykdytas nusikaltimas, numatytas BK 198, 198^1, 198^2 straipsniuose.

4. Nusikaltimo inscenizavimas. Ši versija parodytų tai, kad asmuo, pranešęs apie galimai įvykdytą nusikaltimą elektroninėje erdvėje, pats jį ir padarė.

Norint, kad iškeltos versijos iš prielaidų taptų įrodytos, būtina jas patikrinti. Šių versijų tikrinimas apima ikiteisminio tyrimo, kriminalinės žvalgybos ir kitus veiksmus, kurie susideda iš šių etapų: loginio ir išvestų sekmenų tyrimo, versijų teisingumo ar klaidingumo nustatymo[160]. Versijų tikrinimas baigiamas tada, kai viena jų pasitvirtina, o kitos atkrinta ar yra nepagrįstos[161]. Nusikaltimų elektroninėje erdvėje versijos pasitvirtina arba tampa nepagrįstos dažniausiai atlikus šiuos ikiteisminio tyrimo veiksmus: surinkus tyrimui reikšmingus duomenis ir įkalčius, juos apžiūrint, apklausiant liudytojus, gavus ekspertų išvadas. Taigi, versijų kėlimas pradiniame tyrimo etape gali padėti tyrėjui numatyti pagrindinius tyrimo tikslus ir veiksmus, kurie būtini šiai versijai pagrįsti ar paneigti.

3.3. Duomenų, turinčių reikšmės tiriant nusikaltimus, padarytus elektroninėje erdvėje, surinkimas ir identifikavimas

[156] Alvydas Barkauskas, „Nusikaltimo tyrimo versijų teorijos realizavimo galimybės“, *Jurisprudencija*, Vilnius 2005, t. 65(57), 37.
[157] Petras Ancelis, Gediminas Aleksonis, Gediminas Buciunas ir kt., *Tyrimo veiksmai baudžiamajame procese* (Vilnius 2011), 21.
[158] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 819.
[159] Ryšardas Burda, *Kriminalistikos taktika* (Vilnius, 2011), 61.
[160] Janina Juškevičiūtė, Snieguolė Matulienė, Daiva Kairienė ir kt., *Supra note*, 133, 42.
[161] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 951.

Reikšmingų tyrimui duomenų rinkimas yra svarbi nusikaltimo tyrimo sudedamoji dalis. Virtualioje erdvėje padaryti nusikaltimų pėdsakai ir kiti tyrimui reikšmingi duomenys nėra lengvai identifikuojami, surenkami ir gaunami. Vagysčių, plėšimų ar kitų nusikaltimų metu paliktus pėdsakus dažniausiai galima pamatyti, o štai nusikaltimų elektroninėje erdvėje pėdsakai neretai plika akimi nepastebimi[162]. Tokio pobūdžio nusikaltimuose daiktiniai įkalčiai randami retai, nes nusikaltimo pėdsakai (ypač reaguojant pavėluotai) sunaikinami ar paslepiami[163]. Todėl šių nusikaltimų pėdsakams ir bylai reikšmingiems duomenims surinkti būtinos ir teisinės, ir informatikos žinios, kurios padeda geriau suprasti jų kilmę, veikimo pobūdį ir funkcionavimą. Norint sėkmingai užbaigti nusikaltimų elektroninėje erdvėje bylas, tyrimai turi apimti keturis komponentus[164]:

1. duomenų rinkimas siekiant išsaugoti juose esančią informaciją;
2. sisteminga surinktų duomenų apžiūra išlaikant jų vientisumą;
3. šių duomenų vertinimas siekiant nustatyti informacijos tinkamumą tyrimui;
4. ataskaitų teikimas.

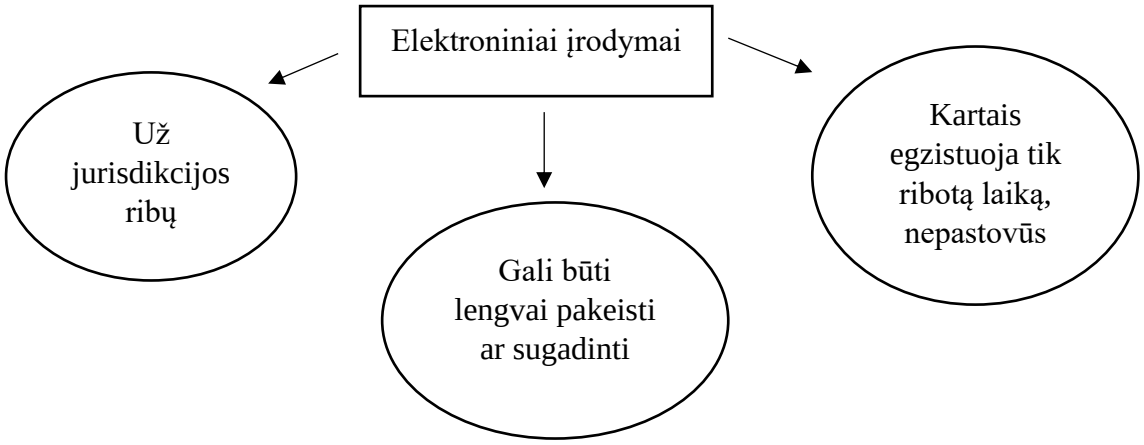
Vienas didžiausių iššūkių, su kuriais tenka susidurti tyrėjui tiriant tokius nusikaltimus, yra virtualių duomenų nepastovumas ir surinkimas išlaikant jų vientisumą. Pasitaiko situacijų, kai tam tikri jau išsaugoti duomenys gali būti ištrinami. Taip nutinka tuomet, kai paslaugos teikėjo užfiksuoti kompiuteriniai duomenys sistemoje saugomi ne ilgiau nei kelios valandos ar kelios paros, nes tai numatyta teisės akto reikalavimuose[165]. Kita problema – kad šie nusikaltimai gali būti padaryti už valstybės sienų ribų (8 pav.). Todėl tokiu atveju objektų tyrimas gali būti paskirtas atlikti kitos valstybės jurisdikcijai.

Nusikaltimų elektroninėje erdvėje tyrimui reikšmingiems duomenims gauti tyrėjai dažnai naudojasi tradiciniais paieškos metodais programinės įrangos įrankiuose arba darbalaukio paieškos sistemose[166]. Tokiu būdu siekiama gauti reikšmingos informacijos, susijusios su asmeniu, padariusiu nusikaltimą. Šių nusikaltimų tyrimo objektais dažniausiai būna kompiuteriai, atminties kortelės, duomenų saugyklos, kietieji diskai, įvairios įrangos, programos ir kt.[167] Informacinių technologijų objektų tyrimai reikalauja daug laiko, technologinių ir materialinių išlaidų, o tai apsunkina ir pailgina jų ištyrimą. Pareigūnai, renkantys virtualius reikšmingus duomenis, turi turėti tam specialių žinių ir

[162] Petras Ancelis, Gediminas Bučiūnas, Marijus Šalčius ir Rolandas Šlepetys, *Atskirų nusikalstamų veikų tyrimas*, (Vilnius 2016), 123.
[163] Margarita Dobrynina, Vaida Kalpokas, Simonas Nikartas ir kt. *Supra note*, 119, 175.
[164] „Cyber crime and cyber terroricm investigators handbook“ (USA, 2014), 60, žiūrėta 2021 m. vasario 26 d., https://books.google.lt/books/about/Cyber_Crime_and_Cyber_Terrorism_Investig.html?id=GR2kAwAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false.
[165] Darius Štitilis, „Kai kurie Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai“, *Jurisprudencija*, 2005, t.67(59).
[166] Farkhund Iqobal, Benjamin C. M. Fung, Rabia Batool ir kt., *Wornet-Based criminal networks mining for cybercrime investigation*, (United Arab Emirates: 2019), 2.
[167] Janina Juškevičiūtė, Snieguolė Matulienė, Daiva Kairienė ir kt., *Supra note,* 133, 217.

asmeninių savybių, pavyzdžiui, kruopštumo. Šie veiksmai turi būti atlikti vadovaujantis įvairiomis taisyklėmis, nes to nepadarius tinkamai nusikaltimą padaręs asmuo gali likti nenubaustas.

Kaip pavyzdį[168] galima būtų pateikti situaciją, kai prokuroras atsisakė tirti vaiko iššaginimo bylą, nes tyrėjas netyčia sugadino pagrindinius įrodymus kompiuterinėje sistemoje. Kompiuteryje buvo daug informacijos (susirašinėjimai su auka, nuotraukos ir t. t.). Tyrimo metu kompiuteris buvo įjungtas ir ištirtas nenaudojant teismo ekspertizės ir aparatūros įrašymo programos, dėl to per klaidą visi duomenys buvo sunaikinti be galimybės juos atkurti. Šis pavyzdys, nors ir nėra tiesiogiai susijęs su darbo analizuojamais straipsniais, patvirtina duomenų fiksavimo ir išsaugojimo svarbą. Jis įrodo, koks reikšmingas gali būti vienas virtualus duomuo ir kaip jo netekus bylos eiga gali pasikeisti akimirksniu, o visas tyrimas – tiesiog sugriūti.



8 pav. Elektroninių įrodymų specifika (sudaryta autorės).

Pirma, nusikaltimų elektroninėje erdvėje tyrimui reikšmingų duomenų surinkimui bei jų identifikavimui keliami tam tikri reikalavimai: juos aptarsime detaliau. Pirmiausia rekomenduojama duomenis surinkti dalyvaujant specialistui. Tai svarbu norint išvengti klaidų, tinkamai duomenis identifikuojant ir surenkant išlaikant jų vientisumą. Antra, negalima išjungti kabelių, kol nebus nustatyta jų paskirtis su kompiuterine įranga. Trečia, jei reikia atverti įrangos korpusą, tai daroma laikantis darbų saugos reikalavimų, kurios nustato tinkama tokių įrangų patikra. Galiausiai, viso proceso metu reikia konsultuotis su specialistu, taip išvengiant įrangos sugadinimo[169]. Antra, būtina, kad specialisto dalyvavimas tiriant tokio pobūdžio nusikaltimus ir renkant duomenis būtų ne tik rekomendacinio pobūdžio, o privalomas todėl, kad neturint pakankamai žinių ir patirties skaitmeniniai duomenys gali būti lengvai pakeisti ar sunaikinti. Lietuvos Respublikos baudžiamojo proceso kodekso (toliau – BPK) 20 straipsnyje numatyta, kad kiekvienu atveju tai, ar gauti duomenys laikytini įrodymais, sprendžia teisėjas ar teismas, kurio žinioje yra byla[170]. Trečia, atvykus į nusikaltimo vietą

[168] Anthony Reyes, Richard Brittson, Kevin Oshea ir kt., *Supra note*, 30, 10.
[169] Petras Ancelis, Gediminas Bučiūnas, Marijus Šalčius ir Rolandas Šlepetys, *Supra note*, 162, 136
[170] Lietuvos Respublikos baudžiamojo proceso kodeksas, Valstybės žinios, žiūrėta 2021 m. vasario 26 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr.

svarbu kuo įmanoma greičiau patraukti asmenis nuo kompiuterio ar su juo susijusių įrenginių, nes duomenys gali būti sunaikinti arba dėl nežinojimo sugadinti. Ketvirta, elektroninių duomenų surinkimas nusikaltimo vietoje paprastai susideda iš šių veiksmų: jų surinkimo ir identifikavimo, nusikaltimo vietos dokumentavimo ir surinktų duomenų išsaugojimo, jų pakavimo ir gabenimo[171]. Šie reikalavimai yra būtini norint tinkamai surinkti bylai reikšmingus duomenis, todėl dėl šios specifinės virtualių duomenų prigimties tyrimus turėtų atlikti tik kompetentingi šios srities specialistai (teismo ekspertai).

Siekiant tobulinti nusikaltimų elektroninėje erdvėje duomenų tyrimą, sutrumpinti jų ištyrimo laiką ir bendradarbiavimą su ES valstybėmis, Generalinė prokuratūra 2019 m. veiklos ataskaitoje yra pateikusi projektą. Šio projekto tikslas – „kartu su kitomis ES valstybėmis narėmis prisijungti prie skaitmeninio keitimosi elektroniniais įrodymais sistemos, kuri būtų skirta vykdant Europos tyrimo orderį surinktiems elektroniniams įrodymams perduoti bei užtikrinti operatyvesnį ir efektyvesnį valstybių narių teisinį bendradarbiavimą baudžiamosiose bylose“[172]. Ši sistema ateityje galėtų padėti sustiprinti tokių nusikaltimų ištyrimą ir užtikrinti efektyvesnį koordinavimą tiriant šias bylas. Be to, pažymėtina, kad Europos Sąjunga skiria itin didelį dėmesį kovai su kibernetiniais nusikaltimais ir bendradarbiavimu tiek tarp Europos Sąjungos narių, tiek tarp trečiųjų šalių. Pavyzdžiui, siekiant padėti ES šalims tirti nusikaltimus elektroninėje erdvėje Europole įsteigtas specializuotas Europos kovos su elektroniniu nusikalstamumu centras[173]; taip pat parengtas EMPACT kibernetinių išpuolių veiksmų planas[174], kuriuo siekiama sužlugdyti išpuolius, susijusius su informacinės sistemos pažeidimais; be to, rengiamos naujos taisyklės[175], kurios, tikimasi, palengvins tarpvalstybinę prieigą prie elektroninių įrodymų; vedamos derybos dėl tarptautinių susitarimų[176], susijusių su elektroniniais įrodymais; 2020 m. parengta ES kibernetinio saugumo strategija[177], stiprinanti bendradarbiavimą su trečiosiomis šalimis. Kibernetinio saugumo strategijoje pateikiamas veiksmų planas, kurio tikslas – gerinti teisėsaugos institucijų gebėjimus rinkti ir identifikuoti skaitmeninius duomenis, suteikiant jiems įgūdžių ir priemonių. Skirtingai negu įprastų nusikaltimų tyrime, tiriant nusikaltimus, padarytus šio

[171] John Ashcroft, *Supra note*, 25, 20.
[172] Lietuvos Respublikos prokuratūros veiklos 2019 metais ataskaita, 24.
[173] „European Cybercrime centre – EC3“, žiūrėta 2021 m. kovo 9 d., https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
[174] Directive 2013/40/eu of the European Parliament and of the council, žiūrėta 2021 m. kovo 9 d., https://eur-lex.europa.eu/legal-content/EN/ALL/?Uri=CELEX%3A32013L0040.
[175] Geresnė prieiga prie e. įrodymų siekiant kovoti su nusikalstamumu, žiūrėta 2021 m. kovo 9 d., https://www.consilium.europa.eu/lt/policies/e-evidence/.
[176] „Taryba suteikė Komisijai įgaliojimus vesti derybas dėl tarptautinių susitarimų, susijusių su e. įrodymais baudžiamosiose bylose“, žiūrėta 2021 m. kovo 9 d., https://www.consilium.europa.eu/lt/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.
[177]The Cybersecurity Strategy, žiūrėta 2021 m. kovo 9 d., https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy.

darbo analizuojamuose straipsniuose, duomenys surenkami laikantis specifinių metodų, taip siekiant išlaikyti jų vientisumą.

3.4. Pirminiai ir tolesni tyrimo veiksmai

Pirminiai ir tolesni tyrimo veiksmai priklausys nuo to, kokia informacija bus gauta, kitaip tariant, nuo susiklosčiusios tyrimo situacijos. Dažniausiai tiriant nusikaltimus elektroninėje erdvėje pasirenkami šie pirminiai[178] (iki 5 darbo dienų[179]) ikiteisminio tyrimo veiksmai:

1. Asmenų, pirminėje informacijoje nurodytų kaip galimų liudytojų, apklausa.
2. Įvykio vietos apžiūra dalyvaujant specialistui.
3. Kriminalinės žvalgybos veiksmų atlikimas (nustatant kaltininkus, pėdsakus ir kitus įrodymus).
4. Įtariamųjų gyvenamųjų ir darbo vietų apžiūra arba (ir) krata.
5. Įrenginių, dokumentų ir kitų tyrimui reikšmingų duomenų poėmis arba apžiūra.
6. Objektų tyrimo skyrimas.

Svarbu kuo įmanoma greičiau apklausti liudytojus, nes dėl specifinių šiuose nusikaltimuose vartojamų terminologijų ir informacinių technologijų sudėtingumo pobūdžio asmuo gali greitai pamiršti svarbią tyrimui informaciją. Apklausa turi būti kuo išsamesnė, jos metu svarbu užfiksuoti bylai reikšmingas aplinkybes. Turėtų būti išsiaiškinama[180], kokiu būdu (tiesioginiu ar netiesioginiu) buvo perimti, sugadinti ar kitaip paveikti informacinės ar kompiuterinės sistemos duomenys, kuriuo metu buvo įvykdytas nusikaltimas (laikas), ar liudytojas žino, kas tai galėjo padaryti, kokiu motyvu ir t. t. Užduodami klausimai galėtų būti tokie:

- Ar kas nors žinojo Jūsų prisijungimo duomenis?
- Kuriuo metu pastebėjote gedimą ar trikdžius?
- Ar su savo slaptažodžiais esate prisijungęs prie kito asmens naudojamo kompiuterio?

Taip pat svarbu paminėti, kad teismo ekspertai, dirbantys su teisėsaugos institucijomis, laikomi techniniais liudytojais. Jie ataskaitose pateikia faktus apie rastus įrodymus ir apie tai, kaip jie buvo gauti[181]. Tačiau tai įvyksta šiek tiek vėliau, nei apklausiami liudytojai, tiesiogiai susiję su padarytu nusikaltimu.

---

[178] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 660-661.

[179] Lietuvos Respublikos generalinio prokuroro įsakymas „Dėl rekomendacijų dėl formalizuotos tvarkos taikymo atliekant ikiteisminį tyrimą patvirtinimo“, Valstybės žinios, žiūrėta 2021 m. kovo 25 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.443828?jfwid=2r1ml6yv.

[180] Lietuvos Respublikos generalinio prokuroro įsakymas „Dėl metodinių rekomendacijų dėl elektroninėje erdvėje vykdomų sukčiavimų (telefoninio sukčiavimo) tyrimo ir nusikalstamų veikų kvalifikavimo patvirtinimo“, žiūrėta 2021 m. vasario 26 d., https://prokuraturos.lt/data/public/uploads/2015/12/rek-del-el-sukciavimu-2014-02-10.pdf.

[181] Mike Sheward, *Supra note*, 24, 190.

Įvykio vietos (taip pat ir įtariamųjų darbo vietos) apžiūroje būtina dalyvauti specialistui, kuris galėtų padėti identifikuoti ir surinkti tyrimui svarbius duomenis. Apžiūrint įvykio vietą svarbu kuo geriau ją apsaugoti nuo pašalinių asmenų, tarkime, nuo įmonės darbuotojų, kurie siūlo savo pagalbą, įsikišimo. Taip yra todėl, kad dėl nežinojimo, kaip elgtis, šie asmenys gali duomenis pakeisti, sugadinti ar padaryti juos nepriimtinus teisme[182]. Neretai tirdamas nusikaltimo vietą pareigūnas ar specialistas mato tik kompiuterį, telefoną ir darbo stalą. Pastarieji yra tik įrenginiai, kuriuose galima aptikti bylai reikšmingų duomenų[183]. Jei nusikaltimą daręs asmuo veikė tiesioginiu būdu, yra tikimybė, kad bus palikti jo pirštų atspaudai, bus matyti įrankių, rašalo, riebalų žymės, bus dulkių, purvo, plaukų, pluoštų ir kt.[184] Tokiu atveju apžiūrint įvykio vietą būtina surinkti ir šiuos įkalčius, nors reikėtų pabrėžti tai, kad šių nusikaltimų pėdsakai dažniausiai būna užšifruoti ir paprastai lengvai nepastebimi. Taip pat svarbu pažymėti, kad nusikaltimų elektroninėje erdvėje įvykio vieta gali būti net keliose fizinėse vietose. Pirmoji iš jų – įtariamojo veikimo vieta, kuri dėl neribotų kompiuterių galimybių gali būti nuo įtariamojo miegamojo iki kavinės, kuri turi belaidį ryšį, o antroji vieta – nukentėjusiojo namuose ar darbo vietoje[185]. Dėl šios priežasties tyrėjas turi gebėti greitai pritaikyti tradicinius metodus, kurie padėtų išsiaiškinti tiek vieną, tiek kitą įvykio vietą.

Pagal Kriminalinės žvalgybos įstatymo 8 straipsnio 1 dalį, žvalgybos tyrimai gali būti pradedami tik dėl BK 198 straipsnio 2 dalyje numatytų nusikaltimų. Todėl, kaip teigiama valstybinio audito ataskaitoje[186], kriminalinės žvalgybos potencialas nusikaltimams elektroninėje erdvėje tirti nepakankamai išnaudojamas. Ataskaita taip pat atskleidė, kad kriminalinės policijos nusikaltimų elektroninėje erdvėje specializuoti padaliniai krūvių problemą bando spręsti ikiteisminius tyrimus ar kitus nesudėtingus procesinius veiksmus skirdami atlikti kriminalinės žvalgybos funkciją vykdantiems pareigūnams[187]. Tai tik dar kartą patvirtina didelį šios srities specialistų trūkumą ir įrodo, kad nusikaltimus elektroninėje erdvėje tiria pareigūnai, neturintys pakankamai žinių. Taip atsitinka todėl, kad tokie specialistai dažniau renkasi privačias įmones, kuriose neretai jų gaunamas atlyginimas būna ženkliai didesnis, o darbo krūviai mažesni. Todėl svarbu, kad minėtos problemos būtų sprendžiamos kuo greičiau, nes ateityje tokių specialistų trūkumas gali dar labiau išaugti.

Įrenginių, dokumentų ir kitų tyrimui reikšmingų duomenų poėmis ir apžiūra. Toliau aptarsime šių duomenų surinkimo tvarką. Surinktus įkalčius reikia kuo geriau apsaugoti nuo dulkių,

---

[182] Richard Boddington, *Practical digital forensics* (Birmingham-Mumbai, 2016), 95.
[183] Mohammad Talib, Virginiah Sekgwathe, *Supra note*, 27.
[184] „Research on investigation and evidence collection of cybercrime Cases“, 3, žiūrėta 2021 m. vasario 26 d., https://iopscience.iop.org/article/10.1088/1742-6596/1176/4/042064/pdf.
[185] Carl J. Franklin, *The investigators guide to computer crime* (Springfield USA, 2006), 33 http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=e000xww&AN=452683&site=ehost-live&ebv=EB&ppid=pp_iv.
[186] *Supra note* 3, 42-43.
[187] *Supra note* 3, 42-43.

mechaninio ar terminio sužeidimo, drėgmės ir t. t. Kiekvieną informacijos laikmeną, atmintinę ar kitus reikšmingus duomenis reikia įpakuoti į atskiras pakuotes, norint sumažint elektromagnetinio lauko poveikį. Pakuotę papildomai taip pat reikėtų apvynioti aliuminio folija[188]. Prieš išrenkant kompiuterinę sistemą labai svarbu nupiešti, sužymėti ir padaryti jungčių diagramą[189]. Tuomet viską surinkus, nufotografavus ir atlikus apžiūrą objektai siunčiami į laboratorijas.

Tolesni tyrimo veiksmai priklausys nuo tyrimo situacijos ir atliktų pirminių veiksmų. Tačiau paprastai analizuojama jau surinkta informacija, jei reikia, ši informacija yra papildoma, pradedamas ikiteisminis tyrimas, įtariamųjų apklausos ir t. t.[190] Neįmanoma išvardyti konkrečiai visiems tokio pobūdžio nusikaltimams galimų tolesnių tyrimo veiksmų sąrašo, nes pastarieji ir jų eiliškumas bus pasirenkami kiekvienoje situacijoje individualiai, atsižvelgiant į konkrečias aplinkybes ir surinktą informaciją.

Apibendrinant galima teigti, kad nusikaltimų elektroninėje erdvėje tyrimus atliekantys pareigūnai turi būti apmokyti, kaip pasirinkti geriausius būdus, surinkti svarbiausius duomenis, kurie padėtų išaiškinti bylos aplinkybes ir atitiktų skaitmeniniams įrodymams keliamus reikalavimus teisme. Todėl dar studijų universitete metu kaip atskira programa galėtų būti įtraukta nusikaltimų elektroninėje erdvėje tyrimo metodika. Užsienyje teisės studijų studentai jau studijuoja privalomą mokslo discipliną, susijusią su kibernetiniais nusikaltimais[191]. Tuo siekiama jau universitete paruošti potencialius nusikaltimus elektroninėje erdvėje galinčius tirti pareigūnus. Taip pat dėl šių nusikaltimų prigimties bendradarbiavimas tiek tarp institucijų, tiek tarptautiniu ar nacionaliniu lygiu turi itin didelę reikšmę šių nusikaltimų baudžiamajam persekiojimui, užkardymui ir atskleidimui. Todėl esamos spragos, susijusios su bendradarbiavimu ir specialistų trūkumu bei dideliais darbo krūviais, negali likti nepastebėtos ir turi būti pašalinamos iš esmės. Dėl šių priežasčių ilgėja šių nusikaltimų tyrimų laikas, laiku neatliekami svarbūs ikiteisminio tyrimo veiksmai (apklausos, kratos, apžiūros) ir dėl to prarandama bylai reikšminga informacija.

[188] Petras Ancelis, Gediminas Bučiūnas, Marijus Šalčius ir Rolandas Šlepetys, *Supra note*, 162, 142.
[189] Janina Juškevičiūtė, Snieguolė Matulienė, Daiva Kairienė ir kt., *Supra note,* 133, 229.
[190] Vidmantas Egidijus Kurapka, Snieguolė Matulienė, *Supra note*, 32, 661.
[191] „Cyber-criminology- a new field of scientific research and criminological investigation“, 6, žiūrėta 2021 m. vasario 26 d., https://www-sciencedirect-com.skaitykla.mruni.eu/science/article/pii/S1742287618300422.

4. NUSIKALTIMŲ, NUMATYTŲ BK 198 , 198[1] , 198[2] STRAIPSNIUOSE, PROBLEMINIAI ASPEKTAI TEISMŲ PRAKTIKOJE

4.1. Tyrimo metodika

Prieš atliekant magistro darbo tyrimo analizę iškeliama hipotezė: bylai reikšmingų duomenų visumos surinkimas nėra pakankamas siekiant nustatyti ir nubausti asmenis, padariusius nusikaltimus, numatytus BK 198, 198[1], 198[2] straipsniuose.

Analizės metu siekiama išsiaiškinti nusikaltimų, numatytų BK 198, 198[1], 198[2] straipsniuose, surinktų duomenų patikimumą ir jų visumos vertinimą teisminio proceso metu. Jei iškelta hipotezė pagal gautus duomenis pasitvirtins, darbe bus pateikiamos hipotezėje iškeltos problemos priežastys ir jos galimi sprendimo būdai. Jei iškelta hipotezė bus paneigta, autorė pateiks tyrimo apibendrinimą ir gautus rezultatus, kurie paneigė minėtą hipotezę.

Informacijai gauti buvo pasirinktas empirinis metodas – teismų praktika nuo 2011 m. iki 2020 m. Šiuo ataskaitiniu laikotarpiu iš viso teismuose buvo išnagrinėtos 1544 bylos[192] (2 lentelė). Išnagrinėtų bylų, susijusių su minėtais nusikaltimais, nėra daug, lyginant su kitais nusikaltimais. Kaip pavyzdį galima būtų paminėti BK 182 straipsnyje įtvirtintą sukčiavimo normą, kuri taip pat dažnai sutaptimi kvalifikuojama kartu su vienu iš šiame tyrime analizuojamų straipsnių. Tokio pobūdžio bylų nuo 2011 iki 2020 m. teismuose išnagrinėta 14 102[193]. Tai reiškia, kad per tokį patį ataskaitinį laikotarpį tokių bylų teismuose išnagrinėta devynis kartus daugiau, lyginant su darbo analizuojamais straipsniais.

Ieškant bylų šiam tyrimui buvo nustatytas kritinės atrankos būdas, kuriuo analizės imties vienetai atrenkami pagal darbo autorės nustatytus kriterijus. Analizės metu atsitiktine tvarka pasirenkamos analizuoti teismų bylos, kuriose asmenys kaltinami pagal BK 198, 198[1], 198[2] straipsniuose numatytus nusikaltimus, iš kurių pagal kritinės atrankos būdą atrenkamos tik tos, kuriose autorė įžvelgė problemas, susijusias su bylai reikšmingų duomenų visumos surinkimu. Atrinktos bylos darbe išsamiai išanalizuotos. Analizuojant teismų praktiką siekiama surasti esmines klaidas, susijusias su duomenų rinkimu ikiteisminio tyrimo metu ir teismų vertinimu.

Tyrimo tikslas yra pagrįsti arba paneigti iškeltą hipotezę. Hipotezė bus laikoma pagrįsta, jei bent 8 bylose bus aptinkami trūkumai, susiję su duomenų surinkimu analizuojamuose straipsniuose. Pasirinkimą lėmė tai, kad per 2020 m. Lietuvoje ikiteisminio tyrimo institucijose šių nusikaltimų užregistruota 431, o ištirta – tik 181[194]. Tai reiškia, kad, nepaisant to, jog šie nusikaltimai ir taip

[192]Lietuvos teismų statistika, Duomenys apie gautas ir ištirtas bylas baudžiamajame procese per 2010-2020 m., žiūrėta 2021 m. kovo 3 d., https://www.teismai.lt/lt/visuomenei-ir-ziniasklaidai/statistika/106.
[193] *Ibid*.
[194] *Supra note* 4.

priskiriami latentiniams (oficialioji statistika neatitinka tikrųjų skaičių, t. y. asmenys nesikreipia į teisėsaugos institucijas), ištirtų bylų skaičius nesiekia nei pusės užregistruotųjų, o tai reiškia, kad tik šiek tiek daugiau nei trečdalis tokių bylų apskritai patenka į teismą. Be to, remiantis tuo, kad per 10 metų minėtų nusikaltimų ištirtų bylų skaičius siekia tik 1544 (t. y. 0,8 proc.[195] visų išnagrinėtų bylų per 10 metų), daroma pagrįsta prielaida, kad 8 bylos iš analizuojamų yra pakankamas skaičius laikyti iškeltą hipotezę teisinga.

Išnagrinėtų bylų skaičius nuo 2011 iki 2020 metų	2011 metai	2012 metai	2013 metai	2014 metai	2015 metai	2016 metai	2017 metai	2018 metai	2019 metai	2020 metai	Iš viso per ataskaitinį laikotarpį:
Neteisėtas elektroninių duomenų perėmimas ir panaudojimas (BK 198 str.)	5	14	28	19	37	27	1	60	32	22	245
Neteisėtas prisijungimas prie informacinės sistemos (BK 198^1 str.)	6	10	43	129	174	193	264	190	88	130	1227
Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis (BK 198^2 str.)	1	8	7	14	10	5	12	5	7	3	72
Iš viso išnagrinėtų bylų:											1544

2 lentelė. BK 198, 198^1, 198^2 straipsnių išnagrinėtų bylų skaičius nuo 2011 iki 2020 m. (sudaryta autorės).

4.2. Tyrimo rezultatai. BK 198 , 198^1 , 198^2 straipsnių teismų praktikos analizė

Ikiteisminiame tyrime surinkti duomenys, kaip buvo minėta anksčiau, yra itin reikšmingi norint asmenims inkriminuoti nusikalstamus veiksmus. Pagal susiformavusią teismų praktiką kasacinės instancijos teismas savo nutartyse ne kartą yra pasisakęs kad „apkaltinamasis nuosprendis negali būti grindžiamas prielaidomis, teismo išvados turi būti pagrįstos įrodymais, neginčijamai patvirtinančiais kaltinamojo kaltę padarius nusikalstamą veiką“[196]. Todėl svarbu, kad bylai reikšmingi

[195] Per 10 metų laikotarpį iš viso išnagrinėtų bylų yra 192044, analizuojamų straipsnių išnagrinėta per tą patį laikotarpį 1544. Buvo sudaroma proporcija 192044-100 proc., 1544-x ir buvo gautas rezultatas 0,8 proc.

[196] Baudžiamojo proceso kodekso normų, reglamentuojančių nuosprendžių surašymą, apžvalga (BPK 302–305, 307 straipsniai), žiūrėta 2021 m. kovo 3 d., https://www.lat.lt/lat-praktika/teismu-praktikos-apzvalgos/baudziamuju-bylu-apzvalgos/68.

duomenys būtų surinkti tinkamai, o jų apžiūras ir vertinimus atliktų tik tos srities specialistai tam, kad būtų išvengta klaidų ir nesklandumų bylai pasiekus teisminio proceso etapą.

Ankstesniuose skyriuose buvo identifikuota, kad viena iš problemų, susijusių su šių nusikaltimų ištyrimu, yra būtent nepakankamas ir netinkamas duomenų surinkimas, todėl kaltininkai lieka nenubausti. Kitaip tariant, padarius tokias klaidas teismas priima išteisinamuosius nuosprendžius teisiamų asmenų veiksmuose nenustačius nusikaltimo požymių. Kaip pavyzdį galima pateikti situaciją, „kai asmuo (byloje nurodoma, kad jis buvo UAB „Recesus“ pardavimų vadybininkas) buvo kaltinamas tuo, kad naudodamasis įmonės interneto ryšio elektroninės prieigos adresu ir kompiuterine technika 2011 m. rugpjūčio 10 d. 14.36 val. ir 14.52 val., neteisėtai pasinaudodamas žinomu prisijungimo vardu ir slaptažodžiu, prisijungė prie elektroninio pašto dėžutės, kuri priklauso UAB „Corpus Medica“ [197]. Prisijungimo laiku šis asmuo neteisėtai stebėjo elektroninių ryšių tinklais siunčiamos informacijos turinį“. Šioje situacijoje asmeniui buvo inkriminuojami šie nusikaltimai: BK 166, 198, 198^1 straipsniai. Taip pat buvo kaltinamas ir juridinis asmuo – UAB „Recesus“. Įmonės veiksmai buvo kvalifikuoti pagal BK 198 straipsnio 1 ir 3 dalis ir 198^1 straipsnio 1 ir 3 dalis.

Ikiteisminio tyrimo metu buvo nustatyta, kad UAB „Recesus“ patalpoje yra penki kompiuteriai, turintys tą patį IP adresą. Atkreiptinas dėmesys į tai, kad šio tyrimo metu buvo surinkta duomenų, kad būtent šiuo IP adresu ir buvo prisijungta prie nukentėjusiosios el. pašto ir šis adresas priklauso UAB „Recesus“ maršrutizatoriui. Atsižvelgiant į tai galima daryti išvadą, kad viename iš šių penkių kompiuterių buvo bylai reikšmingų duomenų, todėl norint sužinoti, kuris konkrečiai kompiuteris buvo naudojamas bandant neteisėtai prisijungti prie el. pašto, reikėtų tyrimui paimti visus kompiuterius ir išsamiai juos ištirti. Tačiau, kaip matyti iš bylos duomenų, į galimai padaryto nusikaltimo vietą vykęs ikiteisminio tyrimo tyrėjas, atlikęs patalpoje esančių kompiuterių apžiūrą ir nenustatęs, iš kurio kompiuterio buvo jungtasi, objektų tyrimui nusprendė paimti tik vieną kompiuterį, kuriuo naudojosi kaltinamasis. Taip pat atkreiptinas dėmesys į tai, kad naršymo istorijoje išliko duomenys tik nuo 2011 m. spalio mėnesio. Jie galėjo buvo ištrinti ar kitaip paslėpti, nes nuo įvykusio incidento iki įvykio vietos apžiūros buvo praėję beveik penki mėnesiai. Pažymėtina, kad šioje apžiūroje nedalyvavo specialistas, kuris vėliau minėjo, kad buvo galima atkurti ištrintus duomenis. Daroma išvada, kad dėl žinių trūkumo ar aplaidumo šie veiksmai nebuvo atlikti. Tolesnio tyrimo metu, t. y. dar po penkių mėnesių atlikus kaltinamojo kompiuterio standžiojo disko iš elektroninių duomenų, esančių laikmenoje, ir duomenų apie veikas, galėjusias vykti 2011 m. rugpjūčio 10 d., ar duomenų apie prisijungimus prie elektroninių pašto dėžučių nėra. Todėl nepaisant to, kad buvo surinkta informacijos, iš esmės patvirtinančios įvykdytus nusikalstamus veiksmus būtent iš šios įmonės

[197] Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-680-530/2013, eteismai, žiūrėta 2021 m. kovo 4 d., https://eteismai.lt/byla/128140400772250/1-680-530/2013.

patalpų, tačiau teismas nuosprendyje nurodė, kad „byloje nėra jokių objektyvių įrodymų, kad buvo stebimas elektroninių laiškų turinys. Nenustatytas ir prisijungęs asmuo, galėjęs matyti elektroninių laiškų siuntėjus bei jų turinį“[198]. Teismas nustatė, kad nagrinėjamu atveju nebuvo surinkta įrodymų, kurie „patvirtintų, jog kaltinamasis atliko konkrečius veiksmus, kurie įeina į nusikaltimų, numatytų BK 198 ir 198[1] straipsniuose, sudėtį. Taip pat byloje nebuvo objektyvių įrodymų, kad nusikalstamai veikai atlikti buvo naudojami UAB „Recesus“ kompiuteriai. Teismo vertinimu, kilus pagrįstoms abejonėms dėl kaltinamojo kaltės teismas, ištyręs visus esamus įrodymus, objektyviais duomenimis negali pašalinti jų, todėl vadovaudamasis suformuota teismų praktika visas kilusias abejones vertina kaltinamųjų naudai ir kaltinamieji išteisintini pagal pareikštus kaltinimus“[199]. Taigi, tai yra pavyzdys, kai nusikaltimų elektroninėje erdvėje, numatytų BK 198, 198[1] straipsniuose, ištyrimui pritrūko duomenų, kurie, manytina, buvo netinkamai surinkti, todėl ir kaltininkai liko nenubausti.

Analizuojant šią bylą autorė išskyrė kelias klaidas, kurios galėjo lemti tokį teismo sprendimą (visos kartu arba viena iš minėtų):

1. Kaip buvo minėta anksčiau, tiriant tokius nusikaltimus ikiteisminio tyrimo pareigūnui reikalingos ne tik teisinės, bet ir išsamios informatikos žinios, kurios padeda geriau suvokti elektroninių įrenginių veikimą ir pėdsakų elektroninėje erdvėje aptikimą[200]. Šiuo atveju ikiteisminio tyrimo pareigūnas, manytina, neturėjo pakankamai specialių žinių ir kompetencijos, kuri būtų padėjusi jam tinkamai įvertinti ir identifikuoti įvykio vietoje esančius bylai reikšmingus duomenis.

2. BPK 180 straipsnyje numatytas galimas specialisto dalyvavimas apžiūrint įvykio vietą. Šioje situacijoje įvykio vietos apžiūroje nedalyvavo informacinių technologijų specialistas, kuris gebėtų padėti surinkti labiausiai tikėtinus duomenis.

3. Generalinio prokuroro rekomendacijoje yra numatyta, kad „visus arba daugelį būtinų proceso veiksmų galima atlikti iš karto po to, kai gautas pranešimas apie įvykį, iš karto po įvykio vietos apžiūros arba ne vėliau kaip per 5 darbo dienas nuo ikiteisminio tyrimo pradėjimo“[201]. Todėl manoma, kad šiuo atveju buvo pasirinktas netinkamas ikiteisminio tyrimo veiksmų planas. Remiamasi tuo, kad įvykio vietos apžiūra atlikta po daugiau nei 2 mėnesių, o tai reiškia, kad per tą laiką kaltinamasis galėjo pašalinti nusikaltimo padarymo pėdsakus, o dėl to vėliau nepavyko aptikti bylai reikšmingų duomenų.

Akivaizdu, kad esminės klaidos, kurios padaromos ikiteisminio tyrimo metu, ne visais atvejais gali būti pašalintos teisminio nagrinėjimo etape, o dėl to pažeidžiamos asmens teisės į teisingą bylos nagrinėjimą. Šios problemos vienas iš sprendimų būdų galėtų būti specialisto ir ikiteisminio

[198] *Supra note*, 197.
[199] *Supra note*, 197.
[200] Petras Ancelis, Gediminas Bučiūnas, Marijus Šalčius ir Rolandas Šlepetys, *Supra note*, 162, 123.
[201] *Supra note*, 179.

tyrimo pareigūno bendradarbiavimas bei dalyvavimas apžiūrint įvykio vietą. Kitas svarbus momentas – kad tyrėjas turėtų ne tik fundamentalių teisinių, bet ir specialiųjų žinių, pritaikytų tiriant tokio pobūdžio nusikaltimus. Ž. Navickienė savo disertacijoje pabrėžė, kad tyrėjui reikalingos kompleksinės, visapusiškos, išsamios įvairių mokslinių sričių žinios ir gebėjimas jas pritaikyti atliekant ikiteisminį tyrimą[202]. Dėl šių priežasčių ikiteisminį tyrimą atliekantiems pareigūnams turėtų būti nustatyti griežtesni kriterijai dirbant su nusikaltimais elektroninėje erdvėje, taip pat turėtų būti įtvirtintas imperatyvus reikalavimas, kuris numatytų privalomą specialistų dalyvavimą tiriant tokių įvykių vietas.

Tiriant tokio pobūdžio nusikaltimus svarbus tinkamas pėdsakų identifikavimas ir, esant poreikiui, – jų atkūrimas. Asmenys, kompiuteriuose diegę įvairaus tipo programas, kurios padeda nuslėpti nusikalstamus veiksmus, taip siekia išvengti atsakomybės. Analizuojant teismų praktiką buvo pastebėta, kad kai kuriais atvejais dėl įdiegtų specifinių operacinių sistemų, sukurtų konkrečiam tikslui, sudėtingumo, t. y. siekiant paslėpti nusikaltimo padarymo pėdsakus nėra įmanoma jų atkurti. Todėl specialistai, atlikdami šių objektų tyrimus, negali rasti bylai svarbių duomenų.

Štai, pavyzdžiui, „kaltinamasis 2017 m. liepos 22 d. apie 19.16 val., būdamas Kauno r., pasinaudodamas kompiuterine technika ir internetu bei atspėtu prisijungimo prie nukentėjusiosios „Facebook“ paskyros vardu ir slaptažodžiu neteisėtai prisijungė prie „Facebook“ sistemos, taip pažeisdamas informacinės sistemos apsaugos duomenis. Asmuo identifikavo save kaip teisėtą duomenų naudotoją“ [203].

Ikiteisminio tyrimo metu iš kaltinamojo namų buvo paimtas jam priklausantis „Asus“ kompiuteris ir atlikta jo apžiūra, tačiau jokių tyrimui reikšmingų duomenų nerasta. Atkreiptinas dėmesys į tai, kad ir šiuo atveju apžiūrint įvykio vietą specialisto dalyvavimas neatrodė būtinas, dėl to į įvykio vietą vyko tik ikiteisminio tyrimo pareigūnas. Vėliau specialistui paskirta atlikti šio kompiuterio analizę, kurios metu buvo pastebėta, kad kietajame diske 2017 m. liepos 23 d. naujai įdiegta operacinė sistema gali neatstatomai ištrinti kietojo disko duomenis. Todėl nebuvo rasta duomenų apie diske išlikusius įrašus, apie galimus IP adresus 2017 m. liepos 22 d. Iš pateiktos bylos medžiagos akivaizdu, kad kaltininkas būtent šiam tikslui, t. y. norėdamas nuslėpti savo padarytus nusikalstamus, kompiuteryje įdiegė šią programą. Šiuo konkrečiu atveju bylos eigoje buvo surinkta ir kitų duomenų, kurie visgi patvirtino kaltininko kaltę. Tad galima daryti išvadą, kad ne visais atvejais galima identifikuoti nusikaltimo pėdsakus, todėl asmenys yra išteisinami pritrūkus jų kaltę

[202] Žaneta Navickienė, „Ikiteisminio tyrimo organizavimo modelis kriminalistikos taktikoje“ (daktaro disertacija, Mykolo Romerio universitetas, 2011), 121.
[203] Kauno apylinkės teismo 2018 m. liepos 30 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-2411-917/2018, eteismai, žiūrėta 2021 m. kovo 4 d., https://eteismai.lt/byla/261624687010066/1-2411-917/2018?word=bpk%2053%20str.%203%20d.

pagrindžiančių įrodymų. Atsižvelgiant į tai, kad sparčiai tobulėja technologijos, kuriami įvairūs virusai, kenkėjiškos programos, kurios padeda kaltininkams užmaskuoti savo pėdsakus, siūloma tobulinti ir papildyti turimus informacinių technologijų išteklius bei nuolatos dėl tokių pėdsakų rinkimo ir jų atkūrimo galimybių dalintis gerąja patirtimi su užsienio valstybėmis.

Kitoje byloje teismas konstatavo, kad neturi pagrindo kategoriškai ir abejonių nekeliančiai išvadai, jog kaltinamasis padarė jam inkriminuotus nusikaltimus, t. y. „kaltinimuose nurodytomis aplinkybėmis prisijungė prie VšĮ „Informacinės sistemos“ bei neteisėtai perėmė ir panaudojo elektroninius duomenis, atskleidžiančius VšĮ komercinę paslaptį. Objektyvių, aiškių ir patikimų įrodymų, leidžiančių priimti apkaltinamąjį nuosprendį, nebuvo surinkta. Atsižvelgiant į tai kaltinamasis dėl nusikalstamų veikų, numatytų BK 198[1] str. 1 d., 198 str. 1 d., išteisintinas“[204]. Šioje situacijoje buvo atliktas ne vienas objektų tyrimas. Jų išvados patvirtino, kad vartotojas buvo prisijungęs prie duomenų ir galėjo būti neteisėtai jungtasi, tačiau neįrodyta, kad byloje nurodytu laiku ir aplinkybėmis prisijungė būtent kaltinamasis. Šiuo atveju svarbu pažymėti, kad nei ikiteisminio tyrimo metu, nei teisme nebuvo galimybės nustatyti, kad prie informacinės sistemos buvo jungtasi konkrečiai nusikaltimo padarymo dieną. Taip pat specialistas parodė, kad „aplinkybė dėl nurodyto laiko yra tik tikėtina dėl nustatytų chronologinių datų neatitikimų, kurių priežastis taip ir nebuvo nustatyta. Labiausiai tikėtina, jog yra iškraipyta naršymo istorija, būtent dėl ko nėra galimybės nustatyti prisijungimo laiko“[205].

Iš pateiktos bylos medžiagos matoma, kad sudėtingos programos, įvairūs kaltininkų naudojami šriftai ne visais atvejais gali būti įveikiami net informacinių technologijų specialistams. Atsižvelgiant į tai, kad 2015–2019 m. net 30 proc. specializuotų pareigūnų nedalyvavo rengiamuose mokymuose[206], siūlytina ikiteisminio tyrimo pareigūnams, tiriantiems nusikaltimus elektroninėje erdvėje, bei specialistams, tiriantiems šių nusikaltimų objektus, bent kartą per metus rengti įvairius mokymus užtikrinant, kad visi subjektai, tiriantis tokio pobūdžio nusikaltimus, dalyvautų parengtose mokymo programose. Šiuo metu tokias programas ir mokymus rengia Lietuvos kibernetinių nusikaltimų centras[207], NKSC, policija ir kt.

Kitoje byloje susiklostė situacija, kai teisėsaugos institucijos dėl nusikaltimų elektroninėje erdvėje tyrimo sudėtingumo ir ribotų tokių duomenų surinkimo galimybių turėjo nutraukti ikiteisminį tyrimą, nes stokojama informacijos, įrodančios nusikaltimo sudėties požymius. Štai, pavyzdžiui[208], 2009 m. birželio 3 d. buvo pradėtas ikiteisminis tyrimas pagal BK 198[1] straipsnio 1 dalį. Kaltinamasis

[204] Vilniaus miesto apylinkės teismo 2016 m. balandžio 8 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-243-932/2016, eteismai, žiūrėta 2021 m. kovo 9 d., https://eteismai.lt/byla/56669072237197/1-243-932/2016.
[205] *Ibid*.
[206] *Supra note* 3, 10.
[207] „Mokymai“, žiūrėta 2021 m. kovo 24 d., http://www.l3ce.eu/mokymai/.
[208] *Supra note*, 79.

buvo kaltinamas tuo, kad slapta seka savo buvusią žmoną: sužino apie jos mobiliojo ryšio skambučius, siunčiamas trumpąsias žinutes, el. paštu siunčiamus laiškus bei jos buvimo vietą. Tauragės rajono apylinkės prokuratūra 2009 m. spalio 19 d. nutarimu nutraukė ikiteisminį tyrimą, nes nenustatė duomenų, kurie patvirtintų kaltinamojo nusikalstamus veiksmus, numatytus BK 198[1] straipsnyje. Vėliau nukentėjusioji pateikė skundą Tauragės rajono apylinkės teismui, tačiau skundas buvo atmestas. Teismas nurodė, kad „ikiteisminis tyrimas pagal pateiktą pareiškimą atliktas išsamiai ir visapusiškai, atlikti visi būtini tyrimo veiksmai, ištirtos visos nusikalstamos veikos padarymo aplinkybės, tinkamai įvertinti surinkti duomenys ir padaryta pagrįsta išvada, jog kaltininkas nepadarė nusikalstamų veikų, numatytų BK 198[1] straipsnio l dalyje“[209].

Ikiteisminio tyrimo metu buvo surinkta duomenų, kad nukentėjusios naudojamu mobiliojo ryšio telefono numeriu buvo užsakyta „Locitor“ paslauga. Ši paslauga suteikia galimybę sužinoti asmens buvo vietą, kitaip tariant, leidžia jį sekti. Atkreiptinas dėmesys į tai, kad pats kaltinamasis pripažino šią paslaugą užsakęs žmonos telefonu, tačiau neigė, kad stebėjo ir sekė ją. Taip pat nukentėjusioji teigė, kad vos tik sužinojo apie šią paslaugą, iš karto pasikeitė mobiliojo telefono numerį. Klaipėdos apygardos teismas pažymėjo, kad „tyrimo metu surinkti duomenys apibrėžtų galimos nusikalstamos veikos sudėtį, jei tie duomenys atspindėtų veikos ir objektyviąją, ir subjektyviąją puses. Nors veikos objektyvieji požymiai tarsi ir žinomi, tačiau subjektyvieji veikos požymiai nėra nustatyti ir dėl ribotų galimybių jų nustatyti nėra įmanoma“[210]. Be to, aukštesnysis teismas pabrėžė, kad „neturi pagrindo kitaip vertinti prokuratūros pareigūnų priimtų nutarimų ir naikinti Apylinkės teismo ikiteisminio tyrimo teisėjos nutartį, kuria atmestas nukentėjusiosios skundas. Nors nukentėjusioji skunde nurodo, kad įvykio aplinkybės ištirtos neišsamiai, tačiau galimybių tirti ir nustatyti kitus duomenis nėra“[211]. Akivaizdu, kad nukentėjusiajai nebūtų aktuali tokia programa. Tačiau surinkti tokius duomenis, kurie patvirtintų, kad tai galėjo padaryti kitas asmuo, yra beveik neįmanoma, o kiti byloje esami duomenys negali patvirtinti buvusio nusikaltimo požymių. Kita vertus, teismas iš esmės pripažino, kad kaltinamasis galimai galėjo padaryti BK 198[1] straipsnyje numatytą nusikaltimą, nes buvo surinktų objektyviųjų požymių visuma, tačiau stokojant subjektyviųjų nusikalstamos veikos požymių ir nesant galimybės šiems trūkumams pašalinti nukentėjusiosios skundą atmetė. Šiuo atveju nei ikiteisminio tyrimo pareigūnai, nei teismas nežinojo, kaip įrodyti kaltę asmens veiksmuose.

Taigi, norint užkirsti kelią šioms spragoms ateityje, reikėtų papildyti ar nustatyti papildomus saugos reikalavimus tokių paslaugų įdiegimo ir naudojimosi taisyklėse. Svarbu pažymėti, kad, norint

[209] *Supra note*, 79.
[210] *Ibid*.
[211] *Ibid*.

įdiegti minėtą paslaugą, užtenka ją atsisiųsti ir patvirtinti trumpąja žinute, nėra jokių papildomų sąlygų ir reikalavimo identifikuoti naudotojo tapatybę. Todėl paslaugos, kurios gali suvaržyti asmenų teises ir laisves, turi būti itin skrupulingai peržvelgtos ir sugriežtintos jų įdiegimo sąlygos.

Išanalizuoti trys pavyzdžiai leidžia daryti apibendrinamas išvadas, kad:

1. „Kiekvienam nuodui yra sukurtas priešnuodis“. Remiantis tuo manytina, kad stokojama informacinių technologijų išteklių arba kompetencijos dirbant su nusikaltimais elektroninėje erdvėje, kuriais naudojantis galima būtų atkurti ir surasti kaltininkų sunaikintus duomenis įrangose.

2. Norint įdiegti įvairias programas, kuriomis gali būti suvaržomos kitų asmenų teisės, tokios kaip teisė į privatų gyvenimą, į asmeninį privatumą, yra lengvai pasiekiamos, nėra numatytų griežtų įdiegiamų programų taisyklių.

Dar vienas šių nusikaltimų tyrimo išskirtinumas, kuris apsunkina duomenų surinkimą, yra šių nusikaltimų subjektai. Kaip buvo analizuota ankstesniuose skyriuose, tokie asmenys dažnai šiuos nusikaltimus daro tiesiog iš nuobodulio arba norėdami pademonstruoti savo gebėjimus kitiems[212]. Neretai tokie asmenys išsiskiria aukštu intelektu, greitu loginiu mąstymu ir įvairiomis programomis gali paslėpti savo tapatybę.

Viename iš pavyzdžių[213] programišių grupėje buvo sukurtas įrašas: „Pranešiau jiems apie skyles internetiniame puslapyje, bet jie nesusitvarko, tad imkite prisijungimus ir pažaiskite.“ Koks buvo prisijungimo vardas ir slaptažodis, kaltinamasis jau nebeprisimena. Be to, „jis iš karto prisijungė prie Varnių parko valdymo sistemos ir matė, kad turinio valdymo sistema buvo nepatogi administratoriui. Prisijungęs kaip administratorius jis pabuvo apie dvi minutes ir pažiūrėjo, kaip veikia ta sistema, ir mano, kad galėjo kažką pakeisti, bet dabar jau tikrai neprisimena, ką jis galėjo pakeisti. Jam pasirodė, kad ta turinio valdymo sistema buvo jau pasenusi ir neintuityvi, todėl jis, spaudinėdamas visur, mano, kad galėjo kažką pakeisti“[214]. „Facebook“ grupėje „Programišiai“ kaltinamasis jau nepriklauso.

Kitame pavyzdyje kaltininkas parodė, „kad jau 15–16 metų susidomėjo kompiuteriais, atakomis. Atakos, kurias jis panaudojo, yra labai senos ir iki šiol laikomos pačiomis pavojingiausiomis. Viskas prasidėjo iš sportinio intereso. Bendraudamas su pažįstamų komanda, žiūrėjo kas kurį peršoks“ [215]. Taigi, akivaizdu, kad tokie asmenys nesiekia gauti finansinės naudos, jų motyvai nesusiję su kerštu buvusiam darbdaviui ar su neištikimos žmonos sekimu. Šie asmenys jaučia

[212] Darius Štitilis, *Supra note* 8, 20-21.
[213] Kauno apylinkės teismo 2016 m. rugpjūčio 10 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-1085-408/2016, eteismai, žiūrėta 2021 m. kovo 9 d., https://eteismai.lt/byla/42311899198538/1-1085-408/2016.
[214] *Supra note*, 213.
[215] Klaipėdos apylinkės teismo 2017 m. gruodžio 8 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-412-890/2017, eteismai, žiūrėta 2021 m. kovo 7 d., https://eteismai.lt/byla/138444974884084/1-412-890/2017.

pasitenkinimą vien įsilauždami į kito asmens informacinę sistemą ir duomenis. Todėl dėl šios priežasties sudėtingiau tokius asmenis identifikuoti, nes nukentėjusieji jokiais ryšiais su jais nesusiję.

Atkreiptinas dėmesys į tai, kad tokių grupių, kaip byloje nurodyti „Programišiai“, „Hakeriai“, yra labai daug, jas galima aptikti „Facebook“, „Discord“ ir kitose platformose. Visos jos sukurtos legaliai ir prieinamos bet kuriam norinčiajam. Dažnu atveju, ypač veikiant, kaip byloje minima, iš sportinio intereso ar malonumo, šie asmenys viešai giriasi savo padarytais nusikaltimais virtualioje erdvėje. Viena vertus, tokios grupės yra legaliai sukurtos ir vien dėl įtartino pavadinimo bausti už tokių grupių kūrimą pagrindo nėra. Kita vertus, teisėsaugos institucijos turėtų skirti daugiau dėmesio tokių grupių turinio stebėjimui. Tai svarbu norint sustabdyti planuojamus nusikaltimus elektroninėje erdvėje.

Daugėjant teisinės pagalbos atvejų, nuo kurių priklauso bylos užbaigimo terminai, užkirsti nusikalstamumui kelią trukdo tai, jog tai yra latentininiai, sudėtingi, užmaskuoti socialiniai reiškiniai[216]. Nusikaltimai elektroninėje erdvėje pasižymi specifiniu surinktų duomenų tyrimu ir jų identifikavimu. Dėl šių surinktų objektų tyrimo sudėtingumo ir ilgų tyrimų eilių neretai tenka bendradarbiauti su kitomis valstybėmis, dėl to prailgėja tokio pobūdžio nusikaltimų ištyrimo laikas ir bylų perdavimas teismo kompetencijai. Taigi, ar bendradarbiavimas renkant tyrimui reikšmingus duomenis yra pakankamas norint patraukti asmenis atsakomybėn? Europos Komisija yra pažymėjusi, kad „beveik du trečdaliai nusikaltimų, kurių elektroninių įrodymų yra kitoje šalyje, deramai neištiriami ir jų kaltininkai nepatraukiami baudžiamojon atsakomybėn – visų pirma dėl to, kad surinkti įrodymams reikia labai daug laiko, arba dėl teisinių sistemų skirtumų“[217].

Kaip pavyzdį[218] būtų galima paminėti situaciją, kurioje buvo reikalingas bendradarbiavimas su Vokietijos ir Rusijos Federacinėmis Respublikomis. Kaip matyti iš bylos duomenų, 2013 m. rugpjūčio 6 d. Lietuva Vokietijos Federacinės Respublikos atsakingoms institucijoms išsiuntė teisinės pagalbos prašymą – gauti tam tikrą informaciją. Po daugiau kaip 3 mėnesių, t. y. 2013 m. lapkričio 29 d., Vokietijos Federacinė Respublika įvykdė pagalbos prašymą ir pateikė surinktus duomenis. Lietuvoje šių bylai reikšmingų duomenų apžiūra įvykdyta balandžio 24 d., t. y. tik po beveik 5 mėnesių.

Kitas teisinės pagalbos prašymas 2013 m. liepos 30 d. buvo išsiųstas Rusijos Federacijos kompetentingoms institucijoms. Po daugiau kaip 10 mėnesių, t. y. 2014 m. gegužės 9 d., atsakymas

[216] Danguolė Senutienė, Linas Ubartas, „Tarptautinis bendradarbiavimas tiriant nusikaltimus: teoriniai ir teisiniai pagrindai”, žiūrėta 2021 m. kovo 8 d., https://repository.mruni.eu/bitstream/handle/007/15112/Seniutien%C4%97.pdf?sequence=1&isAllowed=y, 251.

[217] „Saugumo sąjunga. Komisija lengvina prieigą prie elektroninių įrodymų“, žiūrėta 2021 m. kovo 9 d., https://ec.europa.eu/commission/presscorner/detail/lt/IP_18_3343?fbclid=IwAR18d-jgujltyFXAKyHyV-ps6q8RQOyA9VuDuBtty4CDWlLG3MdmDN2mzgg.

[218] Šiaulių apygardos teismo 2018 m. kovo 27 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-17-744/2018, žiūrėta 2021 m. kovo 9 d., https://eteismai.lt/byla/131499013849817/1-17-744/2018.

buvo gautas ir pateiktos dvi kompaktinės plokštelės su informacija. Po dar 3 mėnesių, t. y. 2014 m. rugpjūčio 27 d., Lietuva išsiuntė pakartotinį prašymą Rusijos Federacijai dėl prieš tai gauto atsakymo patikslinimo. Po 9 mėnesių, t. y. 2015 m. gegužės 6 d., buvo gautas atsakymas į šį prašymą. Taip pat pažymėtina, kad ne vienas gautas duomuo iš Rusijos Federacijos valstybės buvo pažeistas, dėl ko galimybės jų peržiūrėti nebuvo: „atidarius el. laišką, gautą 2013 m. gegužės 26 d. 20:32 val. iš vartotojo M. V. el. pašto dėžutės, aptikta tyrimui reikšminga informacija. Ne vienas duomuo buvo pažeistas, dėl to nebuvo galimybės jų peržiūrėti“[219].

Taigi, kaip matyti iš bylos medžiagos, Lietuvos teisėsaugos institucijoms bylai reikšmingų duomenų teko laukti iš viso beveik 2 metus, jau nekalbant apie tai, kad kai kurie duomenys buvo sugadinti dėl byloje nenurodytų priežasčių, todėl jie nebeturėjo tyrimui jokios vertės.

Kitu pavyzdžiu[220] būtų galima paminėti situaciją, kai kaltinamasis nuo 2013 m. rugsėjo 16 d. iki 2015 m. birželio 9 d. įgijo ir laikė programinę įrangą turėdamas tikslą daryti nusikaltimus, numatytus BK 198 straipsnio 1 d., ir 198^1 straipsnio 1 d. Taip pat nuo 2015 m. vasario 14 d. iki 2015 m. birželio 9 d., t. y. iki kratos atlikimo dienos, asmuo padarė daugybę nusikalstamų veikų fizinių ir juridinių asmenų atžvilgiu, taip pažeisdamas ne vieną baudžiamajame įstatyme saugomą vertybę. Kaltinamasis, įvertindamas rezultatą, gautą darant nusikalstamą veiką, vėliau nuspręsdavo, kokius neteisėtus veiksmus ir kokio asmens atžvilgiu jis vėl atliks. Iš viso kaltinamasis įvykdė 423 tyčinius nusikaltimus.

Tyrimo metu buvo apklausti liudytojai. Daugelis net nežinojo, kad prie jų el. pašto ar banko duomenų buvo kėsinamasi prisijungti ar buvo prisijungta. Taip pat buvo atlikta krata kaltinamojo namuose, paimti tyrimui reikšmingi duomenys (laikmenos, kompiuteriai, mobilusis telefonas). Surinkti duomenys buvo perduoti Lietuvos teismo ekspertizių centrui atlikti objektų tyrimus ir pateikti išvadas. Objektai kratos metu buvo paimti 2015 m. birželio 9 d., o paskutinės specialisto išvados byloje pateiktos 2017 m. sausio 3 d., t. y. po maždaug metų ir septynių mėnesių.

BPK 176 straipsnyje įtvirtinta, kad ikiteisminis tyrimas turi būti atliktas per įmanomus trumpiausius terminus. Dėl sunkių ar labai sunkių nusikaltimų per 9 mėnesius dėl bylos sudėtingumo apimties ar svarbių aplinkybių terminai gali būti pratęsiami. Valstybinio audito ataskaitoje[221] nustatyta, kad 2016–2019 m. visų nusikaltimų elektroninėje erdvėje specializuotų padalinių ikiteisminiai tyrimai trunka ilgiau nei 9 mėnesius, t. y. daugiau nei 40 proc. bylų yra išnagrinėjamos per ilgesnį nei 9 mėnesių laikotarpį. Akivaizdu, kad tokia praktika yra nusistovėjusi ir ikiteisminiai tyrimai užtrunka ilgiau, nei numatyta įstatyme, todėl atsiranda rizika prarasti svarbią informaciją, kuri byloje galėtų tapti reikšmingais duomenimis.

[219] *Supra note*, 218.
[220] *Supra note*, 211.
[221] *Supra note* 3, 37.

Taigi, išanalizavus šias kelias situacijas matoma, kad ikiteisminių tyrimų trukmė pailgėja dėl atliekamų ilgų objektų tyrimų termino. Atkreiptinas dėmesys į tai, kad, apžvelgus pirmąją situaciją, matome, jog iš Vokietijos Federacijos duomenys buvo gaunami tris kartus greičiau, lyginant su Rusijos Federacija. Manoma, kad taip gali būti todėl, jog Vokietija yra Europos Sąjungos narė, tad keitimasis duomenimis tampa paprastesnis ir operatyvesnis. Atsižvelgiant į tai, viena vertus, reikėtų stiprinti bendradarbiavimą su trečiosiomis šalimis, siekiant pagreitinti elektroninių duomenų operatyvumo klausimą. Kita vertus, matoma, kad Lietuvoje atliekami objektų tyrimai taip pat trunka pernelyg ilgą laiką. Dėl to vienas iš sprendimų būdų galėtų būti informacinių technologijų ekspertizes atliekančių specialistų skaičiaus didinimas, taip paskirstant darbo krūvius ir pagreitinant objektų tyrimų trukmę. Dėl paprastesnio bendradarbiavimo su trečiosiomis šalimis, nors Lietuva šiuo metu pasirašiusi nemažai dvišalių ir daugiašalių susitarimų dėl teisinės pagalbos, taip pat ir su Rusijos Federacija, tačiau nėra numatyto susitarimo, kuris užtikrintų sklandesnį keitimąsi elektroniniais duomenimis. Atsižvelgiant į tai, kad tokio pobūdžio nusikaltimai darosi vis pavojingesni, jų mastas nuolatos auga ir ne tik šalies viduje, bet ir už sienų ribų, tiek tarptautinis, tiek nacionalinis bendradarbiavimas turi būti stiprinamas. Svarbu įvertinti turimus teisinius aktus, derinti naujus susitarimus, kurie šį procesą palengvintų.

Vis dėlto atlikus tyrimo analizę galima teigti, kad bylai reikšmingų duomenų visuma tiriant nusikaltimus, numatytus BK 198, 198^1, 198^2 straipsniuose, nėra pakankama norint nubausti asmenis, galimai padariusius tokio pobūdžio nusikaltimus. Tiriant nusikaltimus elektroninėje erdvėje, numatytus BK 198, 198^1, 198^2 straipsniuose, susiduriama su įvairiomis problemomis (3 lentelė). Viena pagrindinių problemų galima būtų laikyti nepakankamą ir netinkamą duomenų surinkimą, todėl kaltininkai lieka nenubausti. Vienoje iš nagrinėtų situacijų, nors tam tikri duomenys įrodė, kad asmuo padarė nusikalstamą veiką, dėl netinkamai surinktų duomenų ikiteisminio tyrimo metu svarbiausi duomenys buvo prarasti. Manytina, kad renkant duomenis, susijusius su elektroniniais nusikaltimais, į įvykio vietas turėtų vykti asmenys, turintys specialių žinių. Jie galėtų tinkamai surinkti ir identifikuoti visus bylai reikšmingus duomenis. Teismai, įvertinę, kad trūksta įrodymų, pasirenka kelis kelius: asmenis išteisina arba grąžina bylą ikiteisminio tyrimo institucijai surinkti papildomus įrodymus.

Kita problema, su kuria susiduriama tiriant tokio pobūdžio nusikaltimus, yra pėdsakų identifikavimas ir jų atkūrimas. Kai kuriais atvejais dėl įdiegtų specifinių programų, sukurtų paslėpti ir ištrinti naršymo istoriją, neįmanoma jos atkurti. Įdiegus tokias programas specialistai, atlikdami šių objektų tyrimus, negali rasti bylai svarbių duomenų, leidžiančių patraukti asmenis baudžiamojon atsakomybėn. Kadangi teismai visas kilusias abejones vertina kaltinamojo naudai, tokiais atvejais pritrūkus įrodymų asmenys yra išteisinami.

Ne mažiau aktuali problema yra ir tyrimo sudėtingumas bei ribotos tokių duomenų surinkimo galimybės. Autorės analizuotame pavyzdyje, nors ir buvo tam tikrų duomenų, kad buvo padaryta nusikalstama veika, tačiau surinkti duomenys, kurie patvirtintų, kad tai galėjo padaryti konkretus asmuo, buvo neįmanoma, o kiti byloje esami duomenys negalėjo patvirtinti buvusio nusikaltimo požymių, todėl asmuo buvo išteisintas. Kaip problemą autorė išskyrė tyrimo sudėtingumą, kurį lemia šių nusikaltimų subjektai, kurių nesieja jokie ryšiai su aukomis ir šie niekieno nevaržomi įvairiose platformose aptarinėja savo padarytus ar ketinamus padaryti nusikaltimus elektroninėje erdvėje. Galiausiai, tokio pobūdžio nusikaltimai yra tiriami per ilgą laiką ir taip yra pažeidžiamas operatyvumo principas. Taigi, tiriant nusikaltimus elektroninėje erdvėje susiduriama su nemažai problemų, tačiau dažniausiai ištirti tokius nusikaltimus pritrūksta specialių žinių bei pačių duomenų, kurių nepavyksta atkurti.

Autorė taip pat atkreipia dėmesį, kad teismai, vertindami tokio pobūdžio nusikaltimus, pabrėžia ir dažnai remiasi *ultima ratio* ir *in dubio pro reo* principais, kurių esmė – kad baudžiamoji atsakomybė yra kraštutinė priemonė, kad visos nepašalintos abejonės baudžiamojo proceso metu dėl padaryto nusikaltimo būtų vertinamos kaltininko naudai. Dėl šių priežasčių kai kurios bylos buvo nutrauktos dėl nusikaltimo mažareikšmiškumo[222], kitos[223] – neįrodžius nusikalstamos veikos objektyviųjų ir subjektyviųjų požymių. Kita vertus, teismai pabrėžia, kad „neteisėto prisijungimo prie informacinės sistemos mažareikšmiškumo aspektu kasacinės instancijos teismo praktikoje yra išaiškinta, kad neteisėtas prisijungimas prie informacinės sistemos paprastai negali būti laikomas nereikšmingu, vertinant iš baudžiamosios teisės pozicijų“[224]. Tačiau nepaisant to daugelis bylų nutraukiamos būtent dėl šios priežasties.

Dar vienas aspektas – kad kaltininkai, darydami nusikaltimus, numatytus BK 198, 198[1], 198[2] straipsniuose, dažnai išsisuka gaudami pinigines baudas[225], o ne realias laisvės atėmimo bausmes, nors minėtų BK straipsnių dispozicijose numatytos alternatyvios bausmės (bauda, areštas arba laisvės atėmimas). Todėl manoma, kad nors teismai ir pabrėžia, kad nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui yra pavojingi, tačiau daugeliu atveju laisvės atėmimas nelaikomas proporcinga bausme kalbant apie minėtus nusikaltimus. Galima daryti išvadą, kad taip yra todėl, jog teismai, darydami išvadas, remiasi jau surinktais duomenimis ikiteisminio proceso metu, o darbe

[222] *Supra note*, 81; „Vilniaus apygardos teismo 2016 m. lapkričio 24 d. nutartis, priimta baudžiamojoje byloje Nr. 1A-417-626/2016“, eteismai, žiūrėta 2021 m. kovo 9 d., https://eteismai.lt/byla/162473775875048/1A-417-626/2016.
[223] *Supra note*, 201.
[224] *Supra note*, 116.
[225] Kauno apylinkės teismo 2016 m. gruodžio 21 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1A-477-498/2016, žiūrėta 2021 m. kovo 9 d., https://eteismai.lt/byla/95072395049798/1A-477-498/2016; „Kauno apylinkės teismo 2016 m. rugpjūčio 19 d. baudžiamasis įsakymas, priimtas baudžiamojoje byloje Nr. 1-1803-668/2016“, eteismai, žiūrėta 2021 m. kovo 9 d.,
https://eteismai.lt/byla/100191818629678/1-1803-668/2016?word=neteis%C4%97tas%20prisijungimas%20prie%20informacin%C4%97s%20sistemos.

atskleistos problemos tiriant nusikaltimus elektroninėje erdvėje parodė, kad stokojama šių nusikaltimų tyrimo metodikos, todėl duomenys nėra tinkamai surenkami arba nepavyksta jų išsaugoti.

Eil. Nr.	Problema	Autorės siūlomas sprendimo būdas/rekomendacijos	Subjektai, kuriems skirtas sprendimo būdas/rekomendacija
1.	Nepakankamas ir netinkamas duomenų surinkimas	Ikiteisminį tyrimą atliekantiems pareigūnams turėtų būti nustatyti griežtesni kriterijai (aukštasis teisinis išsilavinimas, įvadiniai kursai, kurių metu būtų vertinama, ar asmuo tikrai turi pakankamai gebėjimų ir gali dirbti tokį atsakingą darbą, bent minimalios informatikos žinios bei jų tobulinimas įvairiuose mokymuose) dirbant su nusikaltimais elektroninėje erdvėje. Be kita ko, turėtų būti įtvirtintas imperatyvus reikalavimas, kuris numatytų privalomą specialistų dalyvavimą tiriant tokių nusikaltimų įvykių vietas. Taip pat siūlytina dar studijų metu daugiau dėmesio skirti šių nusikaltimų tyrimo ypatumams nagrinėti.	Policijos departamentui, Generalinei prokuratūrai, universitetams ruošiantiems teisininkus.
2.	Pėdsakų identifikavimas ir jų atkūrimas	Ikiteisminio tyrimo pareigūnams, tiriantiems nusikaltimus elektroninėje erdvėje, prokurorams, organizuojantiems tokių veikų tyrimą, bei specialistams, tiriantiems šių nusikaltimų objektus, periodiškai rengti įvairius mokymus užtikrinant, kad visi subjektai, tiriantys tokio pobūdžio nusikaltimus, dalyvautų mokymuose pagal parengtas mokymo programas, taip pat tobulinti ir papildyti turimus informacinių technologijų išteklius.	Policijos departamentui, Generalinei prokuratūrai.
3.	Nusikaltimų subjektai	Atsižvelgiant į tai, kad šiuos nusikaltimus vykdantys asmenys dažnai reiškiasi įvairiose elektroninėse platformose, teisėsaugos institucijos turėtų aktyviai ir nuolatos rinkti informaciją apie pažeidėjus, ją analizuoti ir vertinti. Be to, svarbu peržvelgti incidentų fiksavimo elektroninėje erdvėje sistemas, kurios galėtų efektyviau veikti ir padėtų greičiau identifikuoti potencialių tokio pobūdžio nusikaltimų atvejus.	Policijos departamentui.
4.	Ilgas ikiteisminių tyrimų laikas	Būtina įdarbinti daugiau informacinių technologijų tyrimus (ekspertizes) atliekančių specialistų (ekspertų), taip paskirstant darbo krūvius ir pagreitinant objektų tyrimų trukmę. Stiprinti tarpinstitucinį bendradarbiavimą, nustatant griežtai apibrėžtas ir detalias institucijų bendradarbiavimo gaires. Taip pat įvertinti turimus teisinius aktus bei derinti naujus susitarimus su užsienio šalimis.	Krašto apsaugos ministerijai, Policijos departamentui, Generalinei prokuratūrai, Vidaus reikalų ministerijai.

3 lentelė. Pagrindinės problemos tiriant nusikaltimus elektroninėje erdvėje bei jų sprendimo būdai (sudaryta autorės).

Taigi, akivaizdu, kad tiriant nusikaltimus elektroninėje erdvėje susiduriama su daugybe identifikuotų problemų (žr. 3 lentelę). Todėl labai svarbu ne tik tinkamai identifikuoti problemas, bet ir teikti rekomendacijas. Turi būti priimami atitinkami sprendimai, kurie palengvintų darbe analizuotų nusikaltimų elektroninėje erdvėje tyrimą. Autorė išskyrė 4 esmines problemas ir pateikė jų sprendimo būdus bei pasiūlymus; taip pat nurodė subjektus, kuriems šie sprendimo būdai/rekomendacijos skirti.

IŠVADOS

1. Nusikaltimai elektroninėje erdvėje yra pavojingi, nusikaltėliai veikia globaliu mastu, taip sukeldami realų pavojų visuomenės saugumui bei pažeisdami pagrindines žmogaus teises ir įstatymus. Mokslinėje doktrinoje nėra bendro apibrėžimo, kas konkrečiai laikoma nusikaltimais elektroninėje erdvėje, tačiau pritartina tiems mokslininkams, kurie teigia, kad nusikaltimų elektroninėje erdvėje terminologija yra tikslesnė apibūdinant tokio pobūdžio nusikaltimus, nes apima didesnį nusikaltimų, kurie gali būti įvykdomi virtualioje erdvėje, spektrą.

2. 2004 m. Lietuvoje ratifikuota Europos Sąjungos konvencija „Dėl nusikaltimų elektroninėje erdvėje“ yra laikoma pamatine tarp tokio pobūdžio nusikaltimus reglamentuojančių teisės aktų. Po šios konvencijos ratifikavimo Europos Sąjungos direktyva dėl elektroninių nusikaltimų bei direktyva, kuria buvo pakeistas Europos Tarybos pamatinis sprendimas dėl atakų prieš informacines sistemas, turėjo itin didelę reikšmę Lietuvos vidaus baudžiamajai teisei, nes buvo padaryti esminiai pakeitimai BK XXX skyriuje.

3. Nusikaltimų kriminalistinė charakteristika – tai koreliaciniais ryšiais tarpusavyje susijusių konkrečių duomenų apie tam tikrą nusikaltimą požymių visuma. Nusikaltimų elektroninėje erdvėje kriminalistinė charakteristika sudaryta iš šių keturių elementų: padarymo būdo, nusikaltimo subjekto, pasikėsinimo dalyko ir nusikaltimo situacijos. Šie keturi elementai ir kiekvienas iš jų atskirai tiriant bylos aplinkybes sudaro tam tikrą rinkinį informacijos, susijusios su konkrečiu nusikaltimu. Šios informacijos požymių visuma bei gebėjimas pritaikyti šių elementų koreliacinius ryšius yra tyrimo metodikos pamatas, be kurio tinkamai ir laiku ištirti nusikaltimą gali būti sudėtinga, o kartais – net ir beveik neįmanoma.

4. Nusikaltimų elektroninėje erdvėje tyrimai yra labai sudėtingi ir turi nemažai išskirtinumų, lyginant su tradiciniais nusikaltimais, padarytais fizinėje erdvėje. Tokiems tyrimams atlikti būtinos ne tik teisinės, bet ir specialiosios žinios, kurių neretai tiriant šiuos nusikaltimus stokojama. Darbe buvo identifikuotos problemos, susijusios su tarpinstituciniu bendradarbiavimu, specialistų trūkumu bei dideliais ir nepaskirstytais darbo krūviais. Tokios spragos kelia itin didelį susirūpinimą ir gali didinti nenustatytų ir neištirtų įvykių elektroninėje erdvėje kiekį. Tokia praktika sudaro grėsmes visam viešajam saugumui, be to, ateityje gali kilti reali grėsmė tokio pobūdžio nusikaltimų užkardymo kontrolės praradimui.

5. Nusikaltimų, numatytų BK 198, 198^1, 198^2 straipsniuose, tyrimo specifika yra savita, todėl tiriant šiuos nusikaltimus susiduriama su tam tikromis problemomis. Viena pagrindinių problemų galima būtų laikyti nepakankamą ir netinkamą duomenų surinkimą, dėl kurio kaltininkai lieka nenubausti. Kita aktualija yra pėdsakų identifikavimo ir jų atkūrimo problema. Ne mažiau aktuali

problema – ribotos tokių duomenų surinkimo galimybės. Kaip problemą galima išskirti ir tyrimo sudėtingumą, nulemtą šių nusikaltimų subjektų, kurių nesieja jokie ryšiai su aukomis ir šie nevaržomai įvairiose platformose aptarinėja savo virtualioje erdvėje padarytus ar ketinamus padaryti nusikaltimus. Galiausiai, tokio pobūdžio nusikaltimai yra tiriami ilgą laiką ir taip yra pažeidžiamas operatyvumo principas. Vis dėlto galima teigti, kad dažniausiai tiriant tokius nusikaltimus pritrūksta specialiųjų žinių bei nepavyksta atkurti pačių duomenų.

6. Teismai sprendimuose pabrėžia, kad nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui yra pavojingi, tačiau daugeliu atvejų laisvės atėmimas nelaikomas proporcinga bausme. Teismai, darydami išvadas, remiasi ikiteisminio proceso metu jau surinktais duomenimis, tačiau stokojama šių nusikaltimų tyrimo metodikos, kadangi sprendimuose akcentuojama, jog kai duomenys nėra tinkamai surenkami ir (arba) išsaugomi, neturint svarių įrodymų, asmenis patraukti atsakomybėn neįmanoma.

PASIŪLYMAI

1. Ikiteisminio tyrimo pareigūnams, tiriantiems nusikaltimus elektroninėje erdvėje, prokurorams, organizuojantiems šių veikų tyrimą, bei specialistams, tiriantiems šių nusikaltimų objektus, siūloma periodiškai dalyvauti įvairiuose tiksliniuose mokymuose užtikrinant, kad visi subjektai, tiriantys tokio pobūdžio nusikaltimus, įgytų naujausių žinių ir praktinių gebėjimų, reikalingų tokiems nusikaltimams tirti.

2. Virtualiems policijos patruliams siūlytina daugiau dėmesio skirti įvairių grupių turinio stebėjimui, periodiškai analizuoti ir vertinti surinktą informaciją, numatyti įspėjamojo turinio pranešimus dėl neteisėtų veiksmų. Tai svarbu norint sustabdyti elektroninėje erdvėje planuojamus daryti nusikaltimus.

3. Didinti informacinių technologijų tyrimus (ekspertizes) atliekančių specialistų (ekspertų) skaičių, taip paskirstant darbo krūvius ir pagreitinant objektų tyrimų trukmę.

4. Stiprinti tarpinstitucinį bendradarbiavimą nustatant griežtai apibrėžtas ir detalias institucijų bendradarbiavimo gaires. Nustatyti imperatyvų reikalavimą, kuriuo NKSC visais atvejais turėtų pranešti policijai apie galimai padarytus nusikaltimus elektroninėje erdvėje. Taip pat įvertinti turimus teisinius aktus bei derinti naujus susitarimus su užsienio šalimis, kurie palengvintų bendradarbiavimą bei keitimąsi informacija tiriant tokio pobūdžio nusikaltimus.

LITERATŪROS SĄRAŠAS

1. Įstatymai ir kiti teisės aktai

1. Konvencija dėl elektroninių nusikaltimų. TAR, Žiūrėta 2021 m. sausio 10 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195.

2. Directive 2013/40/eu of the European Parliament and of the council. Žiūrėta 2021 m. kovo 9 d., https://eur-lex.europa.eu/legal-content/EN/ALL/?Uri=CELEX%3A32013L0040.

3. Europos tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas. Eur-lex. Žiūrėta 2021 m. sausio 25 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32005F0222.

4. Lietuvos Respublikos baudžiamasis kodeksas. TAR. Žiūrėta 2021 m. sausio 5 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr.

5. Lietuvos Respublikos baudžiamasis kodeksas (1961 m.). Vyriausybės žinios. Žiūrėta 2021 m. sausio 25 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.20465/jxfupAglbe.

6. Lietuvos Respublikos baudžiamojo proceso kodeksas. Valstybės žinios. Žiūrėta 2021 m. vasario 26 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr.

7. Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo pakeitimo įstatymas. Valstybės žinios. Žiūrėta 2021 m. sausio 16 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.207019.

8. Lietuvos Respublikoje elektroninių ryšių įstatymas. Valstybės žinios. Žiūrėta 2021 m. sausio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232036/SgfuAtlPUO.

9. Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198^1, 198^2 straipsnių ir priedo pakeitimo ir kodekso papildymo 270^3 straipsniu įstatymas. TAR. Žiūrėta 2021 m. sausio 21 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ce192022135111e5af81c7d24921dbde.

10. Lietuvos kibernetinio saugumo įstatymas. TAR. Žiūrėta 2021 m. sausio 21 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee.

11. Konvencija dėl Europos Sąjungos valstybių narių savitarpio pagalbos baudžiamosiose bylose, kurią pagal Europos Sąjungos sutarties 34 straipsnį patvirtino Taryba. Žiūrėta 2021 m. kovo 2 d., http://www.infolex.lt/ta/66668:str13.

12. Lietuvos Respublikos generalinio prokuroro įsakymas dėl metodinių rekomendacijų dėl elektroninėje erdvėje vykdomų sukčiavimų (telefoninio sukčiavimo) tyrimo ir nusikalstamų veikų kvalifikavimo patvirtinimo. Žiūrėta 2021 m. vasario 26 d., https://prokuraturos.lt/data/public/uploads/2015/12/rek-del-el-sukciavimu-2014-02-10.pdf.

13. Lietuvos Respublikos generalinio prokuroro įsakymas „Dėl rekomendacijų dėl formalizuotos tvarkos taikymo atliekant ikiteisminį tyrimą patvirtinimo“. Valstybės žinios. Žiūrėta 2021 m. kovo 25 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.443828?jfwid=2r1ml6yv.

2. Specialioji literatūra

14. Ancelis, Petras, Bučiūnas, Gediminas, Šalčius, Marijus ir Šlepetys, Rolandas. *Atskirų nusikalstamų veikų tyrimas*. Vilnius 2016.

15. Ancelis, Petras, Aleksonis, Gediminas, Buciunas, Gediminas ir kt., *Tyrimo veiksmai baudžiamajame procese*. Vilnius 2011.

16. Ashcroft, John. *Electronic crime scene investigation: a guide for first responders*. Washington, 2001.

17. Barkauskas, Alvydas. „Nusikaltimo tyrimo versijų teorijos realizavimo galimybės“, *Jurisprudencija*, Vilnius 2005, t. 65(57).

18. Вехов, В. Б., Попова, В. В., Ильюшин, Д. А., *Тактические особенности расследования преступлений в сфере компьютерной информаций.* Москва: «ЛэксЭст», 2004.

19. Browker, Art Todd G. Shipley, *Investigating internet crimes*. Wyman Street, Waltham, MA 02451,USA, 2014. Žiūrėta 2021 m. sausio 15 d., http://web.a.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/ZTAwMHh3d19fNTAzNTkyX19BTg2?sid=bc8e17ea-299d-4fbe-ab49-98f8508ced2a@sessionmgr4008&vid=6&format=EB&rid=1.

20. Boddington, Richard. *Practical digital forensics*. Birmingham-Mumbai, 2016.

21. Burda, Ryšardas. *Kriminalistikos taktika*. Vilnius, 2011.

22. Casey, Eoghan. *Digital evidence and computercrime*. London Academic press 2004. Žiūrėta 2021 m. vasario 15 d.

23. Clough, Jonathan. *Data Theft? Cybercrime and the Increasing Criminalization of Access to Data*. Criminal Law Forum: 2011.

24. Clough, Jonathan. *Principles of cybercrime*. Cambridge university press: 2010.

25. „Cyber crime and cyber terroricm investigators handbook“. USA, 2014. Žiūrėta 2021 m. vasario 26 d.

26. „Cyber-criminology- a new field of scientific research and criminological investigation“. Žiūrėta 2021 m. vasario 26 d. https://www-sciencedirect-com.skaitykla.mruni.eu/science/article/pii/S1742287618300422.

27. Dobrynina, Margarita, Kalpokas, Vaida, Nikartas, Simonas ir kt. *Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai*. Vilnius, 2011.

28. Franklin, Carl J. *The investigators guide to computer crime*. Springfield USA, 2006. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=e000xww&AN=452683&site=ehost-live&ebv=EB&ppid=pp_iv.

29. Grigaitytė, Ugnė, Mackevičiūtė, Miglė. „Nusikaltimai virtualioje erdvėje – šiuolaikiniai iššūkiai ir prevencijos galimybės“. *Teisės mokslo pavasaris 2020*.

30. Goranin, Nikolaj, Mažeika, Dalius. *Nusikaltimai elektroninėje erdvėje ir jų tyrimų metodikos*. Kaunas: 2011. Žiūrėta 2021 m. sausio 20 d., http://www.esparama.lt/documents/10157/490675/Nusikaltimai_elektronineje_erdveje_ir_ju_tyrimo_metodikos.pdf.

31. Higgins, G. E. *Cybercrime: An Introduction to an Emerging Phenomen. Library of Congress Cataloging*. 2010.

32. *Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos: Duomenys apie nusikalstamumą Lietuvos Respublikoje per 2020 m. sausio-gruodžio mėn.2020 m*. Nr. 24 St.-52.

33. *Internet organized crime threat assessment*. OCTA 2020, Europol, European Union Agency for Law Enforcement Cooperation: 2020.

34. Iqobal, Farkhund, Fung, Benjamin C. M., Batool, Rabia ir kt., *Wornet-Based criminal networks mining for cybercrime investigation*. United Arab Emirates: 2019.

35. Juškevičiūtė, Janina, Matulienė, Snieguolė, Kairienė, Daiva. *Kriminalistika*. Vilnius 2014.

36. Keown, Mc, Patrick, G. *Computer crimes and criminals*. National forum. http://search.ebscohost.com.skaitykla.mruni.eu/login.aspx?direct=true&db=f5h&AN=9609192203&site=ehost-live.

37. Kyung-shick, Choi. *Risk factors in computer-crime victimization*. LFB Scholarly Publishing LLC: 2010. Žiūrėta 2021 m. vasario 15 d.,

38. Козлов, В. Е. *Теория и практика борьбы с компьютерной преступностью*. Москва: Горячая линия – Телеком, 2002.

39. Krašto apsaugo ministerija. *Nacionalinė kibernetinės būklės metinė ataskaita*.

40. Kurapka, Vidmantas Egidijus, Matulienė, Snieguolė. *Kriminalistika: taktika ir metodika*. Vilnius: 2013.

41. Kurapka, Vidmantas Egidijus Matulienė, Snieguolė, Bilevičiūtė, Eglė ir kt., *Specialių žinių taikymo nusikaltimų tyrime mokslinė koncepcija ir jos realizavimo mechanizmas.* Vilnius: 2012.

42. Kurapka, Vidmantas Egidijus, Malevski, Hendryk. „Šiuolaikinė nusikaltimų tyrimo koncepcija ir jos kriminalistinis bei procesinis užtikrinimas. Pirmieji rezultatai“. *Jurisprudencija*, 2003, 43 (35).

43. Lietuvos Respublikos prokuratūros veiklos 2019 metais ataskaita.

44. Majid, Yra. „Cybercrime and sočiety“. Žiūrėta 2021 m. sausio 11 d.

45. Marcinauskaitė, Renata. *Nusikalstamos veikos elektroninėje erdvėje*. Vilnius: Registrų centras, 2019.

46. Marcinauskaitė, Renata. „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai)“. Daktaro disertacija, Mykolo Romerio universitetas, 2013, žiūrėta 2021 m. sausio 5 d. https://repository.mruni.eu/bitstream/handle/007/15957/Disertacija_Marcinauskait%c4%97.pdf?sequence=2&isAllowed=y.

47. Matulienė, Snieguolė, Kurapka, Vidmantas Egidijus. *Kriminalistika teorija ir technika.* Vilnius: 2012.

48. Matulienė, Snieguolė. „Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimų metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija“. Daktaro disertacija, Lietuvos teisės universitetas, 2014.

49. Milinis, Albertas, Gruodytė, Edita, Gutauskas, Aurelijus, ir kt., *Lietuvos baudžiamoji teisė specialioji dalis, pirmoji knyga*. Vilnius: 2013.

50. Moore, Robert. *Search and seizure of digital evidence.* New York, 2005.

51. Navickienė, Žaneta, Matulienė, Snieguolė, Kurapka, Egidijus Vidmantas, ir kt., *Planning ab initio pre-trial investigation as the condition for a more effective investigation of crimes*.

52. Navickienė, Žaneta. „Model of organising pre-trial investigation in tactics of criminalistics“. Daktaro disertacija, Mykolo Romerio universitetas, 2011.

53. Navickienė, Žaneta. „Ikiteisminio tyrimo organizavimo modelis kriminalistikos taktikoje“. Daktaro disertacija, Mykolo Romerio universitetas, 2011.

54. Reyes, Anthony, Brittson, Richard, Steel, James ir kt. *Cyber Crime Investigations : Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors.* Syngress publishing Rocland: 2007.

55. „Research on investigation and evidence collection of cybercrime Cases“. Žiūrėta 2021 m. vasario 26 d. https://iopscience.iop.org/article/10.1088/1742-6596/1176/4/042064/pdf.

56. Ruibytė, Laima, Balsevičienė, Birutė. „Kriminalinio profiliavimo pritaikymo galimybės nusikaltimų įvykdytų elektroninėje erdvėje tyrimui“. Žiūrėta 2021 m. vasario 15 d.

57. Senutienė, Danguolė, Ubartas, Linas. „Tarptautinis bendradarbiavimas tiriant nusikaltimus: teoriniai ir teisiniai pagrindai". Žiūrėta 2021 m. kovo 8 d. https://repository.mruni.eu/bitstream/handle/007/15112/Seniutien%C4%97.pdf?sequence=1&isAllowed=y.

58. Sheward, Mike. *Hands-on incident responce and digital forensic*. United Kingdom, 2018.

59. Shinder, Littlejohn, Cross, Michael. „Understanding the people on the scene". *Žiūrėta* 2021 m. vasario 25 d. https://www.sciencedirect.com/topics/computer-science/cybercrime.

60. Sumit, Gosh, Turini, Elliot. *Cybercrimes: a multidisciplinary analysis*. Springer Heidelberg Dordrecht London New York: 2010. Žiūrėta 2021 m. vasario 10 d. https://link-springer-com.skaitykla.mruni.eu/book/10.1007%2F978-3-642-13547-7.

61. Šatas, Mindaugas. *Prokuroro ir ikiteisminio tyrimo pareigūno bendradarbiavimas tiriant sunkius nusikaltimus*. Vilnius, 2011.

62. Štitilis, Darius. *Elektroniniai nusikaltimai*. Vilnius: Mykolo Romerio universitetas, 2011.

63. Štitilis, Darius ir kt., *Interneto ir technologijų teisė*. Vilnius: Registrų centras, 2016.

64. Štitilis, Darius ir kt., *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Vilnius: Justitia, 2011.

65. Štitilis, Darius, Petrauskas, Rimantas. *Kompiuteriniai nusikaltimai ir jų prevencija*. Lietuvos teisės akademija: Vilnius, 2000.

66. Štitilis, Darius. „Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos". Daktaro disertacija, Lietuvos Teisės universitetas, 2002.

67. Štitilis, Darius. „Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai", *Jurisprudencija*, 2003. t. 47 (39).

68. Štitilis, Darius. „Kai kurie Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai", *Jurisprudencija*, 2005, t.67(59).

69. Šidlauskas, Aurimas, Ungurytė-Ragauskienė, Svajūnė. „Iššūkiai kibernetiniam saugumui: socialinė inžinerija institucinio izomorfizmo kontekste", *Mokslinis žurnalas*, 2020.

70. Talib, Mohammad, Sekgwathe, Virginiah. „Cyber forensics: computer security and incident response", ISSN: 2220-9085, International journal. Žiūrėta 2021 m. sausio 26 d.

71. Танасевич, В. Г. *Образцов В. А. О криминалистической характеристике преступлений* // Вопросы борьбы с преступностью. Вып.25. 1976.

72. *Valstybinio audito ataskaita: ar veiksmingai kovojama su elektroniniais nusikaltimais, 2020 m. Nr. VAE-7*, 4.

73. *2019 internet crime report*.

74. „2020-2025 m. ES strategija dėl nusikaltimų aukų teisių“, Eur lex. 2020.
http://web.a.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/ZTAwMHh3d19fMTg5NDY0X19BTg2?sid=445292f0-0692-45da-85e9-9a91245afc38@sessionmgr4008&vid=18&format=EB&rid=2.
http://web.b.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/ZTAwMHh3d19fNTIwNTI1X19BTg2?sid=7b099815-71bf-4d03-a4d4-d9054335d37f@pdc-v-sessmgr06&vid=0&format=EB&rid=1.
https://books.google.lt/books/about/Cyber_Crime_and_Cyber_Terrorism_Investig.html?id=GR2kAwAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false.
https://books.google.lt/books/about/Cybercrime_and_Society.html?id=Ye4QAAAAQBAJ&printsec=frontcover&so
https://repository.mruni.eu/bitstream/handle/007/15002/Balsevi%20ien%20.pdf?sequence=1.
https://repository.mruni.eu/bitstream/handle/007/16906/9789955194927.pdf?sequence=1&isAllowed=y.
https://www.academia.edu/8332048/CYBER_FORENSICS_COMPUTER_SECURITY_AND_INCIDENTRESPONSE?auto=download&email_work_card=download-paper.
urce=kp_read_button&redir_esc=y#v=onepage&q&f=false.

3. Teismų praktika

75. Baudžiamojo proceso kodekso normų, reglamentuojančių nuosprendžių surašymą, apžvalga (BPK 302–305, 307 straipsniai). Žiūrėta 2021 m. kovo 3 d. https://www.lat.lt/lat-praktika/teismu-praktikos-apzvalgos/baudziamuju-bylu-apzvalgos/68.

76. Klaipėdos apygardos teismo 2010 m. kovo 1 d. nutartis, priimta baudžiamojoje byloje Nr. 1S-49-50/2010. Eteismai. Žiūrėta 2021 m. vasario 15 d. https://eteismai.lt/byla/80718850183473/1S-49-50/2010.

77. Klaipėdos apylinkės teismo 2017 m. gruodžio 8 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-412-890/2017. Žiūrėta 2021 m. kovo 7 d. https://eteismai.lt/byla/138444974884084/1-412-890/2017.

78. Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-680-530/2013. Eteismai. Žiūrėta 2021 m. kovo 4 d. https://eteismai.lt/byla/128140400772250/1-680-530/2013.

79. Kauno apylinkės teismo 2016 m. rugpjūčio 10 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-1085-408/2016. Eteismai. Žiūrėta 2021 m. kovo 9 d. https://eteismai.lt/byla/42311899198538/1-1085-408/2016.

80. Kauno apylinkės teismo 2016 m. rugpjūčio 19 d. baudžiamasis įsakymas, priimtas baudžiamojoje byloje Nr. 1-1803-668/2016. Eteismai. Žiūrėta 2021 m. kovo 9 d. https://eteismai.lt/byla/100191818629678/1-1803-668/2016?word=neteis%C4%97tas%20prisijungimas%20prie%20informacin%C4%97s%20sistemos.

81. Kauno apylinkės teismo 2016 m. gruodžio 21 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1A-477-498/2016. Eteismai. Žiūrėta 2021 m. kovo 9 d. https://eteismai.lt/byla/95072395049798/1A-477-498/2016.

82. Kauno apylinkės teismo 2018 m. liepos 30 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-2411-917/2018. Eteismai. Žiūrėta 2021 m. kovo 4 d. https://eteismai.lt/byla/261624687010066/1-2411-917/2018?word=bpk%2053%20str.%203%20d.

83. Lietuvos Aukščiausiojo Teismo 2015 m. sausio 6 d. nutartis, priimta baudžiamojoje byloje Nr. 2K-138/2015. Eteismai. Žiūrėta 2021 m. vasario 15 d. https://eteismai.lt/byla/148386211638579/2K-138/2015.

84. Lietuvos Aukščiausiojo Teismo 2018 m. lapkričio 6 d. nutartis, priimta baudžiamojoje byloje Nr. 2K-293-788/2018. Eteismai. Žiūrėta 2021 m. sausio 30 d. https://eteismai.lt/byla/278248162686377/2K-293-788/2018?word=vilius%20sutkus.

85. Lietuvos Aukščiausiojo Teismo 2019 m. liepos 2 d. nutartis, priimta baudžiamojoje byloje Nr. 2K-199-648/2019. Eteismai. Žiūrėta 2021 m. vasario 15 d. https://eteismai.lt/byla/113482577300847/2K-199-648/2019.

86. Šiaulių apygardos teismo 2018 m. kovo 27 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-17-744/2018. Žiūrėta 2021 m. kovo 9 d. https://eteismai.lt/byla/131499013849817/1-17-744/2018.

87. Telšių rajono apylinkės teismo 2016 m. kovo 1 d. baudžiamasis įsakymas, priimtas baudžiamojoje byloje Nr. 1-58-187/2016. Eteismai. Žiūrėta 2021 m. vasario 15 d. https://e-teismai.lt/byla/134583854524928/1-58-187/2016.

88. Vilniaus apygardos teismo 2014 m. gegužės 15 d. nutartis, priimta baudžiamojoje byloje Nr. 1A-338-312/2014. Eteismai. Žiūrėta 2021 m. vasario 15 d. https://eteismai.lt/byla/63488840739284/1A-338-312-2014.

89. Vilniaus apygardos teismo 2016 m. lapkričio 24 d. nutartis, priimta baudžiamojoje byloje Nr. 1A-417-626/2016. Eteismai. Žiūrėta 2021 m. kovo 9 d. https://eteismai.lt/byla/162473775875048/1A-417-626/2016.

90. Vilniaus miesto apylinkės teismo 2016 m. balandžio 8 d. nuosprendis, priimtas baudžiamojoje byloje Nr. 1-243-932/2016. Eteismai. Žiūrėta 2021 m. kovo 9 d. https://eteismai.lt/byla/56669072237197/1-243-932/2016.

4. Internetiniai puslapiai

91. „Ar esame pasiruošę spręsti IT specialistų trūkumo klausimą?“. Žiūrėta 2021 m. vasario 25 d. https://www.vz.lt/paslaugos/2020/05/11/ar-esame-pasiruose-spresti-it-specialistu-trukumo-klausima.

92. „Council of Europe committee of ministres“. Žiūrėta 2021 m. vasario 15 d. https://rm.coe.int/16804f6e76.

93. „Dar viena byla dėl nusikaltimų elektroninėje erdvėje perduota teismui“. Žiūrėta 2021 m. vasario 15 d. https://vilnius.policija.lrv.lt/lt/naujienos/dar-viena-byla-del-nusikaltimu-elektronineje-erdveje-perduota-teismui.

94. „Dėl valstybinės duomenų inspekcijos vykdomų ir patikrinimų atlikimo taisyklių patvirtinimo“. TAR. Žiūrėta 2021 m. vasario 25 d. tyrimų https://www.e-tar.lt/portal/lt/legalAct/3416a700a88411e9b474d97de297fe08.

95. „EU regulator: Hackers ‘manipulated’ stolen vaccine documents“. Žiūrėta 2021 m. vasario 15 d.
https://apnews.com/article/public-health-europe-coronavirus-pandemic-coronavirus-vaccine-56efa8e104f0509fa48381fce00b0de6.

96. „European Cybercrime centre – EC3“. Žiūrėta 2021 m. kovo 9 d. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

97. „Geresnė prieiga prie e. įrodymų siekiant kovoti su nusikalstamumu“. Žiūrėta 2021 m. kovo 9 d. https://www.consilium.europa.eu/lt/policies/e-evidence/.

98. „How criminals profit from the covid-19 pandemic“. Europol. Žiūrėta 2021 m. vasario 4 d. https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic.

99. „Karantinas pakeitė vartotojų įpročius: beveik penktadalis internetu pirks daugiau“. Verslo žinios. Žiūrėta 2021 m. vasario 15 d. https://www.vz.lt/versli-lietuva/2020/06/22/karantinas-pakeite-vartotoju-iprocius-beveik-penktadalis-internetu-pirks-daugiau.

100. „Komisijos komunikatas Europos Parlamentui ir Tarybai Antroji ES vidaus saugumo strategijos įgyvendinimo ataskaita“. Žiūrėta 2021 m. kovo 3 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52013DC0179&from=EN.

101. „KTC atliekamų tyrimų ir ekspertizių sąrašas“. Žiūrėta 2021 m. vasario 25 d. https://ktc.policija.lrv.lt/lt/veiklos-sritys/tyrimai-ir-ekspertizes/ktc-atliekamu-tyrimu-ir-ekspertiziu-sarasas.

102. „Lietuvos teismų statistika“, Duomenys apie gautas ir ištirtas bylas baudžiamajame procese per 2010-2020 m.“ Žiūrėta 2021 m. kovo 3 d. https://www.teismai.lt/lt/visuomenei-ir-ziniasklaidai/statistika/106.

103. „Love Bug's creator tracked down to repair shop in Manila“. BBC news. Žiūrėta 2021 m. vasario 25 d., https://www.bbc.com/news/technology-52458765.

104. „Marijampoliečiai įtariami dėl „Grožio chirurgijos“ pacientų duomenų vagysčių“. Žiūrėta 2021 m. vasario 15 d. https://www.etaplius.lt/marijampolieciai-itariami-del-grozio-chirurgijos-pacientu-duomenu-vagysciu.

105. „Mokymai“. Žiūrėta 2021 m. kovo 24 d. http://www.l3ce.eu/mokymai/.

106. „Naujienos ir saugumo pranešimai“. NKSC. Žiūrėta 2021 m. vasario 15 d. https://www.nksc.lt/.

107. „Nacionalinis kibernetinio saugumo centras“. Žiūrėta 2021 m. vasario 25 d. https://www.nksc.lt/veikla.html.

108. „Nacionalinio kibernetinio saugumo būklės ataskaita 2019“. NKSC. Žiūrėta 2021 m. vasario 15 d.
https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf, 19.

109. „OECD Guidelines for the Security of Information Systems, 1992“. Žiūrėta 2021 m. vasario 10 d.
http://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.

110. „OAS“. Žiūrėta 2021 m. vasario 10 d. http://www.oas.org/juridico/english/89-9&final%20Report.pdf.

111. „Pažeidžiamos kompiuterinės sistemos ir programos“. NKSC. Žiūrėta 2021 m. vasario 15 d. https://www.nksc.lt/rekomendacijos/trojangeneric.html.

112. „Policija pradėjo ikiteisminį tyrimą dėl bendrovės citybee klientų pavogtų duomenų“. Policija. Žiūrėta 2021 m. vasario 16 d. https://policija.lrv.lt/lt/naujienos/policija-pradejo-ikiteismini-tyrima-del-bendroves-city-bee-klientu-pavogtu-duomenu.

113. „Pradėti tyrimai dėl asmens duomenų nutekinimo“. Žiūrėta 2021 m. vasario 25 d. https://epilietis.lrv.lt/lt/naujienos/pradeti-tyrimai-del-asmens-duomenu-nutekinimo.

115. „Saugumo sąjunga. Komisija lengvina prieigą prie elektroninių įrodymų“. Žiūrėta 2021 m. kovo 9 d.
https://ec.europa.eu/commission/presscorner/detail/lt/IP_18_3343?fbclid=IwAR18d-jgujltyFXAKyHyV-ps6q8RQOyA9VuDuBtty4CDWlLG3MdmDN2mzgg.

116. „Taryba suteikė Komisijai įgaliojimus vesti derybas dėl tarptautinių susitarimų, susijusių su e. įrodymais baudžiamosiose bylose“. Žiūrėta 2021 m. kovo 9 d.

https://www.consilium.europa.eu/lt/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.

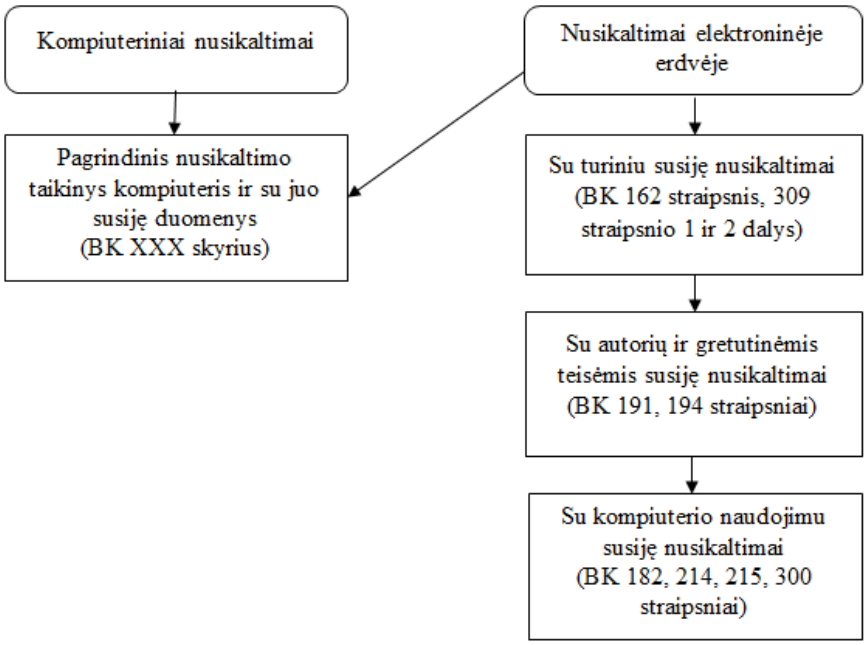
117. „Tarptautinės operacijos“. Lietuvos kriminalinės policijos biuras. Žiūrėta 2021 m. vasario 25 d. https://lkpb.policija.lrv.lt/lt/tarptautinis-bendradarbiavimas/tarptautines-operacijos.

118. „The Cybersecurity Strategy“. Žiūrėta 2021 m. kovo 9 d. https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy.

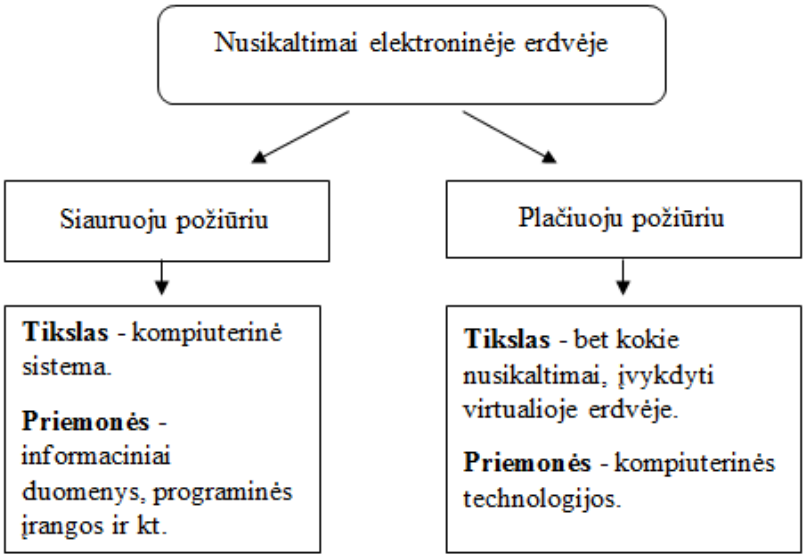
119. „Tips for cybersecurity when working from home“. Žiūrėta 2021 m. kovo 6 d. https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home.

PRIEDAI

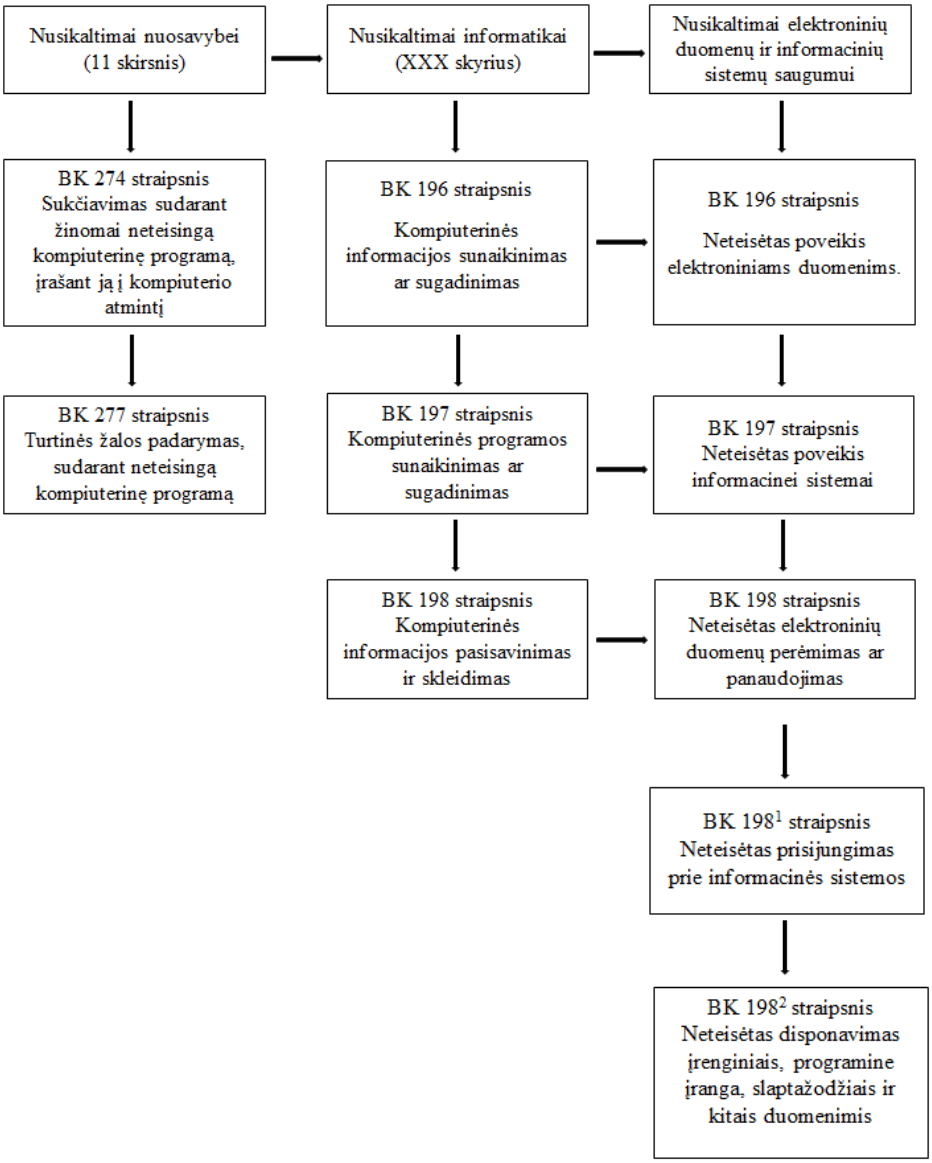
1 PRIEDAS



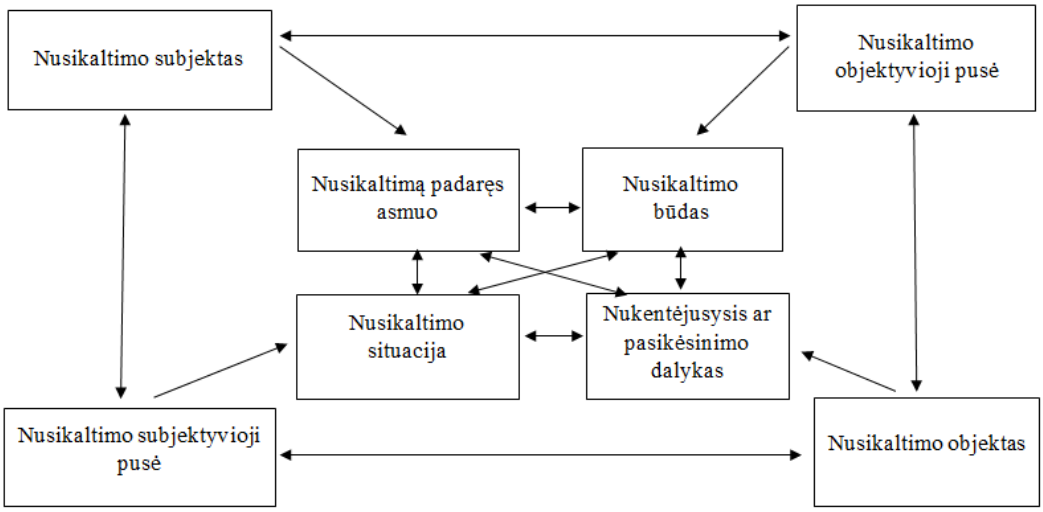
1 pav. Kompiuterinių nusikaltimų ir nusikaltimų elektroninėje erdvėje, sampratų lyginamoji schema (sudaryta autorės).



2 pav. Nusikaltimų elektroninėje erdvėje sąvokos apibrėžtis, remiantis siauruoju ir plačiuoju požiūriais (sudaryta autorės).



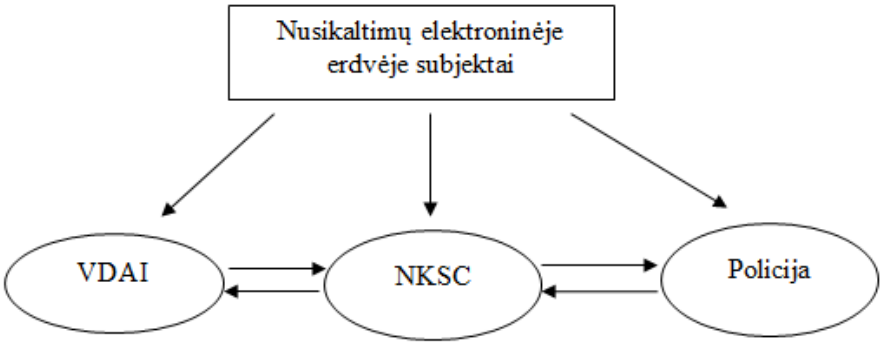
3 pav. Nusikaltimų elektroninėje erdvėje reglamentavimas, BK (1961 m.-2007 m.) (sudaryta autorės).



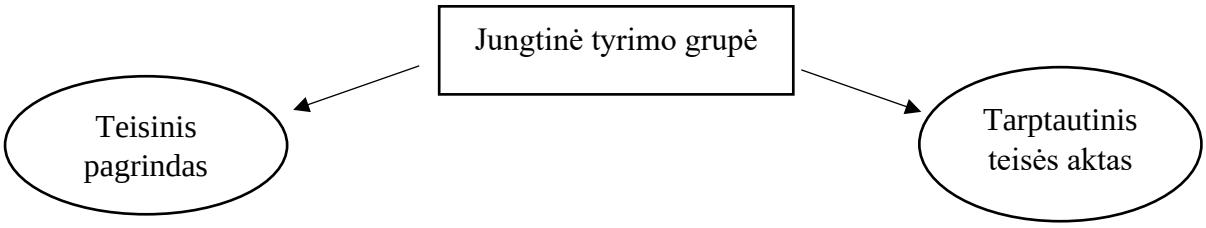
4 pav. Nusikaltimų kriminalistinės charakteristikos ir nusikaltimo sudėties elementų santykių struktūra.

Azorult	Pykspa	Conficker	Downadup	He-andromeda	Sality-p2q	Wrokni	Wannacrypt	Lokibot
9 %	7 %	6 %	5 %	3 %	2 %	2 %	2 %	1 %

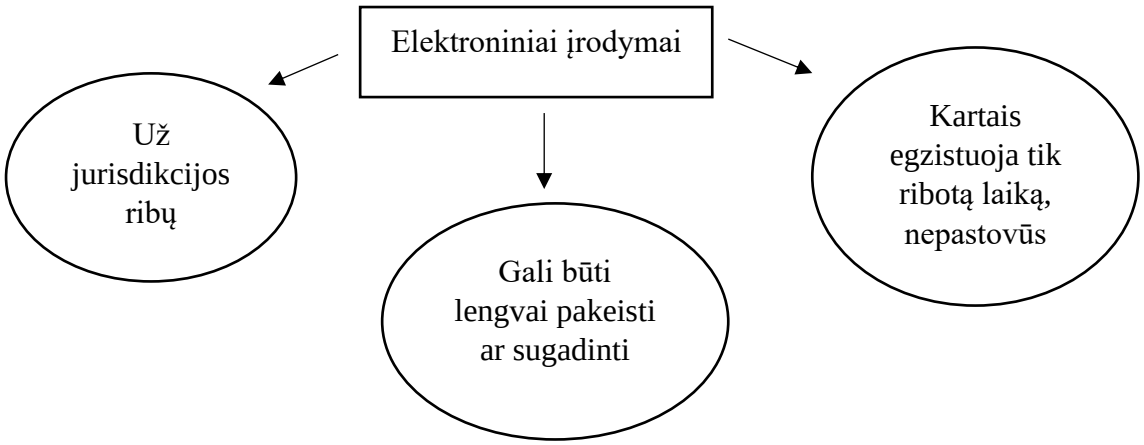
5 pav. 9 labiausiai paplitusios kenkimo programinės įrangos, susijusios su lietuviškais IP adresais.



6 pav. Pranešimai apie nusikaltimą elektroninėje erdvėje ir institucijų bendradarbiavimas.



7 pav. Jungtinės tyrimo grupės sudarymas (sudaryta autorės).



8 pav. Elektroninių įrodymų specifika (sudaryta autorės).

Amžius	Bendras skaičius
Iki-20 metų	10,724
20-29 metų	44,496
30-39 metų	52,820
40-49 metų	51,864
50-59 metų	50,608
Daugiau nei 60 metų	68,013

1 lentelė. Nusikaltimų elektroninėje erdvėje, aukų amžiaus grupės

Išnagrinėtų bylų skaičius nuo-iki (2011-2020 metų)	2011 metai	2012 metai	2013 metai	2014 metai	2015 metai	2016 metai	2017 metai	2018 metai	2019 metai	2020 metai	Iš viso per ataskaitinį laikotarpį
Neteisėtas elektroninių duomenų perėmimas ir panaudojimas (BK 198 str.)	5	14	28	19	37	27	1	60	32	22	245
Neteisėtas prisijungimas prie informacinės sistemos (BK 198^1 str.)	6	10	43	129	174	193	264	190	88	130	1227
Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis (BK 198^2 str.)	1	8	7	14	10	5	12	5	7	3	72
Iš viso išnagrinėtų bylų:											1544

2 lentelė. BK 198, 198^1, 198^2 straipsnių, išnagrinėtų bylų skaičius, laikotarpiu nuo (2011-2020 m.) (sudaryta autorės).

Eil. Nr.	Problema	Autorės siūlomas sprendimo būdas/rekomendacijos	Subjektai, kuriems skirtas sprendimo būdas/rekomendacija
1.	Nepakankamas ir netinkamas duomenų surinkimas	Ikiteisminį tyrimą atliekantiems pareigūnams turėtų būti nustatyti griežtesni kriterijai (aukštasis teisinis išsilavinimas, įvadiniai kursai, kurių metu būtų vertinama ar asmuo tikrai turi pakankamai gebėjimų ir gali dirbti tokį atsakingą darbą, bent minimalios informatikos žinios bei jų tobulinimas įvairiuose mokymuose) dirbant su nusikaltimais elektroninėje erdvėje. Be kita ko, turėtų būti įtvirtintas imperatyvus reikalavimas, kuris numatytų privalomą specialistų dalyvavimą tiriant tokių nusikaltimų įvykių vietas. Taip pat siūlytina dar studijų metu daugiau dėmesio skirti šių nusikaltimų tyrimo ypatumams nagrinėti.	Policijos departamentui, Generalinei prokuratūrai, universitetams ruošiantiems teisininkus.
2.	Pėdsakų identifikavimas ir jų atkūrimas	Ikiteisminio tyrimo pareigūnams, tiriantiems nusikaltimus elektroninėje erdvėje, prokurorams organizuojantiem tokių veikų tyrimą, bei specialistams tiriantiems šių nusikaltimų objektus, periodiškai rengti įvairius mokymus, užtikrinant, kad visi subjektai, tiriantys tokio pobūdžio nusikaltimus, dalyvautų mokymuose pagal parengtas mokymo programas, taip pat tobulinti ir papildyti turimus informacinių technologijų išteklius.	Policijos departamentui, Generalinei prokuratūrai.
3.	Nusikaltimų subjektai	Atsižvelgiant į tai, kad šiuos nusikaltimus vykdantys asmenys dažnai reiškiasi įvairiose elektroninėse platformose, teisėsaugos institucijos turėtų aktyviai ir nuolatos rinkti informaciją apie pažeidėjus, ją analizuoti ir vertinti. Be to, svarbu peržvelgti incidentų fiksavimo elektroninėje erdvėje sistemas, kurios galėtų efektyviau veikti ir padėtų greičiau identifikuoti potencialių tokio pobūdžio nusikaltimų atvejus.	Policijos departamentui.
4.	Ilgas ikiteisminių tyrimų laikas	Būtinus informacinių technologijų tyrimus (ekspertizes) atliekančių specialistų (ekspertų) skaičiaus didinimas, taip paskirstant darbo krūvius ir pagreitinant objektų tyrimų trukmę. Stiprinti tarpinstitucinį bendardarbiavimą, nustatant griežtai apibrėžtas ir detalias institucijų bendradarbiavimo gaires. Taip pat, įvertinti turimus teisinius aktus bei derinti naujus susitarimus su užsienio šalimis.	Krašto apsaugos ministerijai, Policijos departamentui, Generalinei prokuratūrai, Vidaus reikalų ministerija.

3 lentelė. Pagrindinės problemos tiriant nusikaltimus elektroninėje erdvėje bei jų sprendimo būdai (sudaryta autorės).

SANTRAUKA

Darbe buvo analizuojama nusikaltimų elektroninėje erdvėje atskleidimo teisiniai ir praktiniai ypatumai. Darbas aktualus, nes svarbu ištirti problemas, susijusias su nusikaltimų elektroninėje erdvėje samprata, išanalizuoti šių nusikaltimų tyrimo ypatumus bei tokių nusikaltimų rūšių užkardymą ateityje. Darbo tikslas buvo atskleisti nusikaltimų, padarytų elektroninėje erdvėje, tyrimo metodikos probleminius aspektus. Pirmasis keliamas uždavinys buvo susijęs su nusikaltimų, padarytų elektroninėje erdvėje, sampratos atskleidimu. Išanalizavus teisės aktus ir mokslo doktrina galima teigti, kad kompiuteriniai nusikaltimai yra viena iš sudedamųjų nusikaltimų elektroninėje erdvėje sampratos dalių ir yra tikslesni apibūdinant tokio pobūdžio nusikaltimus, nes apima didesnį ratą nusikaltimų, kurie vykdomi virtualioje erdvėje. Kitas darbo uždavinys buvo susijęs su tyrimo aspektais per kriminalistinės charakteristikos prizmę. Nusikaltimų elektroninėje erdvėje padarymo būdų ir metodų yra labai įvairių, jie nuolatos keičiasi, atsiranda vis naujų ir sudėtingesnių programų, dėl ko šie nusikaltimai tampa vis pavojingesni ir reikalaujantys iš nusikaltimą tiriančio tyrėjo vis daugiau kruopštumo ir specialių žinių. Darbe iškeltas trečias uždavinys buvo išanalizuoti nusikaltimų elektroninėje erdvėje BK 198, 198^1, 198^2 straipsnių ikiteisminio tyrimo ypatumus. Darbe buvo identifikuotos problemos susijusios su bendradarbiavimu, specialistų trūkumu, bei dideliais ir nepaskirstytais darbo krūviais. Galiausiai, darbe buvo siekiama išanalizuoti probleminius aspektus bei pateikti problemų sprendimo būdus ir rekomendacijas. Nusikaltimų, numatytų BK 198, 198^1, 198^2 straipsniuose, tyrimo specifika yra savita ir tiriant šiuos nusikaltimus yra susiduriama su tam tikromis problemomis. Viena pagrindinių problemų galima būtų laikyti nepakankamą ir netinkamą duomenų surinkimą, todėl kaltininkai lieka nenubausti. Kita problema, su kuria susiduriama tiriant tokio pobūdžio nusikaltimus, yra pėdsakų identifikavimas ir jų atkūrimas. Ne mažiau aktuali problema yra ir tyrimo sudėtingumas bei ribotų tokių duomenų surinkimo galimybės. Kaip problemą, galima išskirti tyrimo sudėtingumą. Galiausiai, tokio pobūdžio nusikaltimai yra tiriami ilgą laiką ir taip yra pažeidžiamas operatyvumo principas. Vis dėlto, galima teigti, kad dažniausiai ištirti tokius nusikaltimus pritrūksta specialių žinių bei pačių duomenų, kurių nepavyksta atkurti. Siekiant išvengti šių mokymų, siūlytina organizuoti įvairius mokymus ikiteisminio tyrimo pareigūnams, daugiau dėmesio skirti įvairių grupių turinio stebėjimui, norint sustabdyti planuojamus daryti nusikaltimus elektroninėje erdvėje, didinti informacinių technologijų ekspertizes atliekančių specialistų skaičių bei stiprinti tiek tarptautinį, tiek nacionalinį bendradarbiavimą.

SUMMARY

In the master's thesis analyzed the legal and practical peculiarities of cybercrime detection. The topicality of the work, because important problems are solved in the concept of cybercrime, after analyzing the peculiarities of the investigation of these crimes and such issues of crime. The aim of the work was to reveal the problematic aspects of the methodology of investigation of crimes committed in cyberspace. The first task was to reveal the concept of cybercrime. An analysis of legislation and scientific doctrine suggests that cybercrime is one of the components of the concept of cybercrime and is more accurate in describing this type of crime as it covers a wider range of crimes committed in cyberspace. Another task of the work was related to the aspects of the investigation through the prism of forensic characterization. The ways and means of committing cybercrime are very diverse, they are constantly changing, new and more complex programs are emerging, making these crimes increasingly dangerous and requiring more and more diligence and expertise from the investigator investigating the crime. The third task of the work was to analyze the peculiarities of the pre - trial investigation of articles 198, 198^1, 198^2 of the Criminal Code in the electronic space. Problems related to cooperation, lack of specialists, and large and unallocated workloads were identified in the work. Finally, the aim of the work was to analyze the problematic aspects and provide solutions and recommendations. The specifics of the investigation of the crimes provided for in Articles 198, 198^1 and 198^2 of the CC are peculiar and certain problems are encountered in the investigation of these crimes. One of the main problems could be considered insufficient and inadequate data collection, leaving perpetrators unpunished. Another problem encountered in investigating this type of crime is the identification and recovery of traces. No less relevant is the complexity of the study and the limited possibilities for collecting such data. As a problem, the complexity of the study can be singled out. Finally, this type of crime is being investigated for a long time and thus the principle of expediency is violated. However, it can be argued that in most cases, the investigation of such crimes lacks specialized knowledge and the data themselves, which cannot be recovered. In order to avoid this training, it is recommended to organize various trainings for pre-trial investigation officers, to pay more attention to monitoring the content of various groups in order to stop cybercrime, increase the number of IT specialists and strengthen both international and national cooperation.

Forma patvirtinta Mykolo Romerio universiteto

Senato 2012 m. lapkričio 20 d. nutarimu Nr.1SN-10

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2021

Kaunas

Aš, Mykolo Romerio universiteto (toliau – Universitetas), viešojo saugumo akademijos , teisės ir policijos veiklos katedros, teisės ir ikiteisminio proceso programos,

(fakulteto / instituto, programos pavadinimas)

Studentas (-ė) Rasa Pažėrienė,

(vardas, pavardė)

patvirtinu, kad šis rašto darbas / bakalauro / magistro baigiamasis darbas „Nusikaltimų elektroninėje erdvėje atskleidimo teisiniai ir praktiniai ypatumai“:

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

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

Tvirtinu Rasa Pažėrienė

(parašas) *(vardas, pavardė)*