MYKOLO ROMERIO UNIVERSITETO
TEISĖS MOKYKLOS
BAUDŽIAMOSIOS TEISĖS IR PROCESO INSTITUTAS

JOVITA BAJAZITOVAITĖ
BAUDŽIAMOJI TEISĖ IR KRIMINOLOGIJA

KOMPIUTERINIŲ NUSIKALTIMŲ LIETUVOJE KRIMINOLOGINIAI ASPEKTAI

Magistro baigiamasis darbas

Darbo vadovas –
Doc. dr. Alfredas Kiškis

Vilnius, 2025

TURINYS

ĮVADAS 3

1. KOMPIUTERINIŲ NUSIKALTIMŲ SAMPRATA, TEISINIS REGULIAVIMAS IR TEISINIS REGLAMENTAVIMAS 8

1.1. Kompiuterinių nusikaltimų samprata 8

1.2. Tarptautinis teisinis reguliavimas 12

1.3. Kompiuterinių nusikalstamų veikų reglamentavimas Lietuvos Respublikos teisėje 16

2. KOMPIUTERINIŲ NUSIKALTIMŲ RAIŠKA 19

2.1. Paplitimas, struktūra ir dinamika Lietuvoje ir Europos Sąjungoje 19

2.2. Kompiuterinių nusikalstamų veikų žala 25

3. NUSIKALTĖLIO CHARAKTERISTIKA IR JO RYŠYS SU AUKA 29

4. KOMPIUTERINIŲ NUSIKALSTAMŲ VEIKŲ VEIKSNIAI 38

5. PREVENCIJA IR KONTROLĖ 43

5.1. Nacionalinės ir tarptautinės strategijos 43

5.2. Dirbtinio intelekto panaudojimas kovoje su kibernetinėmis grėsmėmis 47

6. EMPIRINIS TYRIMAS 51

6.1. Tyrimo metodologija 51

6.2. Tyrimo rezultatų analizė 51

IŠVADOS 64

PASIŪLYMAI 65

LITERATŪRA 66

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS 78

SANTRAUKA LIETUVIŲ KALBA 80

SUMMARY 82

PRIEDAI 83

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ 86

ĮVADAS

Tiriama problema. Tiriama problema galėtų būti apibrėžiama šiais klausimais: kaip apibrėžiamas kompiuterinių nusikaltimų tarptautinis reguliavimas? Koks kompiuterinių nusikaltimų reglamentavimas Lietuvoje? Kokia yra kompiuterinių nusikaltimų raiška 2020 – 2025 m. laikotarpiu? Kokia yra kompiuterinius nusikaltimus darančio asmens, tiriamuoju laikotarpiu, charakteristika? Koks ryšys sieja nusikaltėlį su auka? Kokie veiksniai lemia kompiuterinius nusikaltimus? Kokiomis priemonėmis užtikrinama kompiuterinių nusikaltimų prevencija ir kontrolė?

Baigiamojo darbo aktualumas. Per pastaruosius metus, informacinių technologijų naudojimas tapo neatsiejama kiekvieno žmogaus dalis. 2020 m. prasidėjusi COVID – 19 pandemija padidino nuotolinių paslaugų, elektroninės prekybos galimybes, taip pat, išplėtė nuotolinio darbo galimybes. 2022 m. Lietuvoje interneto vartotojai sudarė 88 proc. 16 – 74 metų amžiaus gyventojų, tad galima teigti, jog gyvename skaitmeninių technologijų amžiuje.[1] 2024 m. Lietuvoje užregistruoti 3874 kibernetinio saugumo pažeidimų atvejai – 63 % daugiau nei 2023 m., fiksuojami ir didelio masto kibernetiniai incidentai, nukreipti į strateginę reikšmę turinčių institucijų duomenis[2].

Jungtinių Amerikos Valstijų kibernetinio nusikalstamumo centro ataskaitoje, 2025 m. buvo gauta virš 67 tūkst. skundų, dėl asmens duomenų saugumo pažeidimų, kurių žala siekė virš 1,3 mlrd. JAV dolerių.[3] Ataskaitoje paminėta, kad išpirkos reikalaujančios kenkėjiškos programinės įrangos yra viena dažniausių grėsmių, nukreiptų prieš ypatingos svarbos infrastruktūros organizacijas. Didelę grėsmę visuomenei kelia ir dirbtinio intelekto panaudojimas darant kompiuterines nusikalstamas veikas. Nusikaltėliai pradėjo naudoti dirbtinio intelekto sistemas, kurios savarankiškai, be žmogaus pagalbos, atlieka nusikalstamus veiksmus, nukreiptus ne tik į fizinius asmenis, bet ir į vyriausybines institucijas, privačias įmones.[4]

Nusikaltėliai sugeba įsilaužti į bet kokio sudėtingumo sistemas, pastebimas net ir gydymo įstaigų informacinių sistemų, bankinių sistemų ar kitų infrastruktūrų sistemų saugumo pavojus,

---

[1] Lietuvos statistikos departamentas, *Skaitmeninė ekonomika ir visuomenė Lietuvoje*, (Vilnius: 2022) 10 - 11, https://osp.stat.gov.lt/documents/10180/10362936/Skaitmenin%C4%97+ekonomika+ir+visuomen%C4%97+Lietuvoje+%282022+m.+leidimas%29.pdf/14d6c6c8-db09-4fb2-9427-3c6104db448a.

[2] „Lietuvos kibernetinių grėsmių paveikslas: ar valstybė pasiruošusi apsaugoti virtualią erdvę?“, *Lietuvos Respublikos Krašto apsaugos ministerija,* 2025 m. spalio 7 d., https://kam.lt/lietuvos-kibernetiniu-gresmiu-paveikslas-ar-valstybe-pasiruosusi-apsaugoti-virtualia-erdve/.

[3] „2025 Internet Crime Report“, Federal Bureau of Investigation, 7 – 13, žiūrėta 2025 m. rugsėjo 15 d., https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

[4] „The Evolving Threat Landscape: How Encryption, Proxies and AI are Expading Cybercrime 2026“, Europol, 36, žiūrėta 2026 m. rugsėjo 15 d., https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf.

galintis sukelti milžinišką žalą.[5] Nors Lietuvoje kompiuterinių nusikaltimų statistika nėra tokia grėsminga kaip kai kuriose didesnėse valstybėse, tačiau stebimos tendencijos liudija apie nuoseklų tokių nusikalstamų veikų skaičiaus didėjimą, jų sudėtingumą bei daromą žalą tiek juridiniams, tiek fiziniams asmenims. Tokia situacija lemia būtinybę ne tik gilinti teisinį ir techninį šio reiškinio supratimą, bet ir analizuoti kriminologiniu požiūriu: tyrinėti šių nusikalstamų veikų paplitimą, nusikaltėlių ypatumus, veiksnius, skatinančius šio pobūdžio nusikalstamumą bei nagrinėti veiksmingos prevencijos galimybes.

Baigiamasis darbas aktualus visuomenei, nes nusikaltėliai elektroninėje erdvėje gali lengvai adaptuotis vis besikeičiančioje aplinkoje ir atsižvelgiant į pokyčius, atrasti naujų kompiuterinių nusikaltimų būdų, todėl svarbu yra tyrinėti kompiuterines nusikalstamas veikas, jų paplitimą, žalą, kitimo tendencijas, jas darančius asmenis, tokiu būdu bus galima pateikti pasiūlymų prevencijos bei kontrolės klausimais.

Baigiamajame darbe tiriamos problemos ištyrimo lygis. Nors apie elektroninius nusikaltimus kalbama daug, tačiau mokslinių leidinių, kuriuose būtų rašoma apie elektroninius nusikaltimus siauraja prasme, t.y. nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui, yra labai mažai.

Lietuvoje kompiuterinius nusikaltimus ir jų prevenciją pradėjo nagrinėti R. Petrauskas ir D. Štitilis mokomajame leidinyje „Kompiuteriniai nusikaltimai ir jų prevencija“[6]. Autoriai nagrinėjo šių nusikalstamų veikų sampratą ir rūšis, prevencijos priemones ir informacinių technologijų įtaką. Vaidas Kalpokas[7] nagrinėjo skirtingų autorių požiūrius, siekdamas pateikti savitą elektroninių nusikaltimų sampratą. Vienas pirmųjų, akcentavusių visuomenės švietimo ir informuotumo didinimo reikšmę mažinant kompiuterinių nusikalstamų veikų riziką buvo S. Starkus[8], kuris taip pat nagrinėjo kompiuterizacijos kriminologinius aspektus. D. Štitilis[9] analizavo elektroninius nusikaltimus siauraja ir plačiąja prasme, vertino teisinį reglamentavimą Lietuvos, Europos Sąjungos ir tarptautiniu mastu, nagrinėjo šių nusikalstamų veikų tikimybes. Kiek vėliau, R. Marcinauskaitė disertacijoje[10] nagrinėjo Lietuvos Respublikos baudžiamojo kodekso 198 ir

---

[5] „Kibernetiniai nusikaltėliai sukūrė tikrą ‚darbo biržą‘ – išpirkos reikalauti gali bet kas“, *LRT*, 2017 m. gegužės 15 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/173003/kibernetiniai-nusikalteliai-sukure-tikra-darbo-birza-ispirkosreikalauti-gali-bet-kas.

[6] Rimantas Petrauskas ir Darius Štitilis, *Kompiuteriniai nusikaltimai ir jų prevencija: mokomasis leidinys parengtas pagal Tempus Phare projektą „Valstybės pareigūnų rengimas teisinės sistemos reformai Lietuvoje* (Vilnius: LTA Leidybos centras, 2000).

[7] Vaidas Kalpokas, „Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos“, *Teisės problemos* 1, 63 (2009), https://teise.org/wp-content/uploads/2023/01/2009-1-kalpokas.pdf.

[8] Saulius Starkus, „Kriminologiniai Kompiuterizacijos Aspektai“, *Jurisprudencija* 20 (2001): 85-92, https://talpykla.elaba.lt/elaba-fedora/objects/elaba:2706487/datastreams/MAIN/content.

[9] Darius Štitilis, *Elektroniniai nusikaltima*i (Vilnius: Mykolo Romerio universitetas, 2011).

[10] Renata Marcinauskaitė, „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 1981 straipsniai)“ (daktaro disertacija, Mykolo Romerio universitetas, 2013).

198[1] straipsnių sudėtis, jų teisinį reglamentavimą bei teorinius ir praktinius aspektus, o 2019 m. monografijoje[11] pateikė kompiuterinių nusikalstamų veikų aiškinimo ir inkriminavimo problemų sprendimus bei kriminalizavimo ypatumus. Lietuvoje kompiuteriniai nusikaltimai daugiausiai nagrinėjami plačiąja prasme, tik nedaugelis autorių pasirenka nagrinėti būtent baudžiamojo kodekso XXX skyriuje numatytas nusikalstamas veikas.

Užsienyje kompiuterinių nusikaltimų veiksnius, aukų viktimologiją bei prevenciją nagrinėjo T. Holt ir A. Bossler.[12] Russell Brewer ir kt.[13] nagrinėjo kaip tradicinių nusikalstamų veikų prevencija gali būti pritaikoma kompiuteriniams nusikaltimams. Xingan Li moksliniame straipsnyje[14] nagrinėjo kompiuterinių nusikalstamų veikų veiksnius, analizavo finansinius, socialinius ir psichologinius nusikaltėlio motyvus. Rahul Karne ir kt.[15], Naeem AllahRakha[16], Shoeb Ali Syed[17] nagrinėjo dirbtinio intelekto vaidmenį kompiuterinių nusikalstamų veikų darymui ir jų prevencijai. Autoriai analizavo dirbtiniu intelektu paremtas kenkėjiškas programas, dirbtinio intelekto panaudojimą informacijos rinkimui apie galimas kibernetines grėsmes. E. Leverett ir A. Kaplan[18] parašė mokslinį straipsnį apie kompiuterinės sistemos trikdymą DDoS atakomis. D. Chudasama ir N. Rapjut[19] nagrinėjo kompiuterinių nusikaltimų prevencijos priemones, kibernetinių grėsmių identifikavimo metodus, tokius kaip išankstiniai perspėjimai (angl. – *tripwires)* ar elektronines spąstų sistemos (angl. – *honeypots).*

---

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

[12] Thomas J. Holt, ir Adam M. Bossler, *Cybercrime in Progress: Theory and Preventon of Technology – Enabled Offenses*, (Niujorkas: Routledge, 2016), https://www.taylorfrancis.com/books/mono/10.4324/9781315775944/cybercrime-progress-thomas-holt-adam-bossler.

[13] Russell Brewer ir kt., *Cybercrime Prevention: Theory and Applications* (Palgrave, 2019), https://www.researchgate.net/publication/337296521_Cybercrime_Prevention_Theory_and_Applications.

[14] Xingan Li, „A Review of Motivations of Illegal Cyber Activities“, *Kriminologija ir socialinė integracija* 25, 1 (2017), https://hrcak.srce.hr/file/266976.

[15] Rahul Karne, Akhil Dudhipala ir Pavan Kumar Pativada, „Cybercrime in India: Legal Frameworks, Emerging Threats, and the Role of AI in Detection and Defence“, *International Journal of Novel Research and Development* 10, 4 (2025), https://www.researchgate.net/publication/392367232_CYBERCRIME_IN_INDIA_LEGAL_FRAMEWORKS_EMERGING_THREATS_AND_THE_ROLE_OF_AI_IN_DETECTION_AND_DEFENCE.

[16] Naeem AllahRakha, „Legal Frameworks for AI – Driven Cybercrime Prevention“, *Uzbek Journal of Law and Digital Policy* 2, 6 (2024), https://www.researchgate.net/publication/399194690_Challenges_in_Regulating_and_Prosecuting_AI_Model_Poisoning_as_Cybercrime.

[17] Shoeb Ali Syed, „AI – Powered Cybercrime: The New Frontier of Digital Threats“, *International Journal of Engineering Technology Research & Management* 6, 2 (2022), https://www.researchgate.net/publication/390441717_AI-POWERED_CYBERCRIME_THE_NEW_FRONTIER_OF_DIGITAL_THREATS.

[18] Eireann Leverett, Aaron Kaplan, „Towards Estimating the Untapped Potential: A Global Malicious DDoS Mean Capacity Estimate“, *Journal of cyber policy* 2, 2 (2017), https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1362020.

[19] Nikhil Rajput ir Dhaval Chudasama, „Protecting Ourselves from Digital Crimes“, *National Journal of Cyber Security Law* 4, 1 (2021), https://www.researchgate.net/publication/352507646_Protecting_Ourselves_from_Digital_Crimes.

Taigi, kompiuterinių nusikaltimų Lietuvoje kompleksinio nagrinėjimo kriminologiniais aspektais rasti nepavyko.

Baigiamojo darbo mokslinis naujumas. Baigiamajame darbe analizuojama naujausiu, 2020 – 2025 m., laikotarpiu baudžiamojo kodekso XXX skyriuje numatytų nusikalstamų veikų raiška Lietuvoje ir šias nusikalstamas veikas padariusių asmenų charakteristika. Greta to, apžvelgiami veiksniai bei naujausios prevencijos priemonės ir pateikiami pasiūlymai jų tobulinimui.

Baigiamojo darbo reikšmė. Įvertinus tai, kad kompiuterinių nusikaltimų skaičius per pastaruosius metus didėjo, šių nusikalstamų veikų padarymo būdai sudėtingėja, svarbu nenustoti ieškoti efektyvių prevencijos priemonių, padėsiančių sumažinti šių nusikalstamų veikų skaičių. Susisteminti baigiamajame darbe gauti duomenys gali būti naudingi fiziniams ir juridiniams asmenims, siekiant suprasti kaip pasireiškia kompiuteriniai nusikaltimai bei kaip nuo jų apsisaugoti. Darbas taip pat gali būti naudingas ir teisėsaugos institucijoms, siekiant šioje srityje permainų ir geresnės šių nusikalstamų veikų tyrimų kokybės. Identifikuotos problemos, susijusios su instituciniu bendradarbiavimu ar viešojo informavimo trūkumu, gali paskatinti korekcijas praktinėje veikloje ar strateginiuose sprendimuose.

Baigiamojo darbo originalumas. Šis darbas orginalus tuo, kad jame yra nagrinėjami Lietuvos Respublikos teisės aktai, Lietuvos ir užsienio mokslininkų straipsniai, apžvelgiama naujausia registruotų kompiuterinių nusikalstamų veikų statistika, veiksniai, prevencija. Atliktas empirinis tyrimas, kurio metu gauti ikiteisminio tyrimo tyrėjų, atliekančių kompiuterinių nusikalstamų veikų tyrimus, rezultatai, papildė teorinę dalį praktinėmis įžvalgomis ir prisidėjo prie išsamesnio tiriamų aspektų nagrinėjimo.

Tyrimo tikslas. Ištirti kompiuterinių nusikaltimų Lietuvoje kriminologinius aspektus ir pateikti siūlymų jų prevencijai.

Tyrimo uždaviniai.

1. Išanalizuoti kompiuterinių nusikaltimų sampratą, tarptautinį teisinį reguliavimą ir nacionalinį teisinį reglamentavimą.

2. Išanalizuoti kompiuterinių nusikaltimų raišką 2020 – 2025 m. laikotarpiu.

3. Atskleisti asmenų, padariusių kompiuterinius nusikaltimus, charakteristiką bei jo ryšį su auka.

4. Atskleisti veiksnius, lemiančius kompiuterinių nusikaltimų atsiradimą ir plitimą.

5. Apžvelgti kompiuterinių nusikaltimų prevencijos ir kontrolės priemones bei pateikti siūlymus prevencijos ir kontrolės gerinimui.

6. Atskleisti ikiteisminio tyrimo tyrėjų, atliekančių kompiuterinių nusikaltimų tyrimus, požiūrį į šių nusikalstamų veikų pobūdį, veiksnius bei prevencijos priemones.

Tyrimo metodika. Baigiamajame darbe naudoti šie tyrimo metodai: *statistinės analizės* (tiriant Lietuvos ir kitų šalių statistinius duomenis susijusius su kompiuteriniais nusikaltimais), *mokslinės literatūros analizės* (analizuojant kompiuterinius nusikaltimus darančių nusikaltėlių charakteristiką ir veiksnius), *dokumentų sisteminės analizės* (analizuojant Lietuvos ir tarptautinio lygmens teisės aktus, kompiuterinių nusikaltimų tarptautinį teisinį reguliavimą), *lyginamasis* (lyginant skirtingose šalyse taikomas prevencijos priemones), *kokybinis duomenų rinkimo* (apklausiant ikiteisminio tyrimo tyrėjus), *apibendrinimo* (apibendrinant statistinius duomenis, išanalizuotą informaciją bei pateikiant išvadas).

Tyrimo struktūra. Baigiamąjį darbą sudaro įvadas, šeši skyriai, išvados, pasiūlymai, santrauka lietuvių ir anglų kalbomis, literatūros sąrašas. Pirmajame skyriuje analizuojama kompiuterinių nusikaltimų samprata, tarptautinis teisinis reguliavimas bei kompiuterinių nusikaltimų reglamentavimas Lietuvos Respublikos teisėje. Antrajame skyriuje nagrinėjama 2020 – 2025 m. laikotarpio kompiuterinių nusikaltimų raiška bei galima žala. Trečiajame skyriuje pateikiama kompiuterinių nusikaltimų nusikaltėlio charakteristika bei jo ryšys su auka. Ketvirtajame skyriuje atskleidžiami veiksniai, lemiantys kompiuterinių nusikaltimų atsiradimą ir plitimą. Penktajame skyriuje apžvelgiami kompiuterinių nusikaltimų prevencijos ir kontrolės priemonės. Šeštajame skyriuje pateikiama empirinio tyrimo metodologija bei tyrimo rezultatų analizė.

Ginamieji teiginiai.

1. Didžiausią dalį Lietuvoje užregistruotų kompiuterinių nusikaltimų sudaro neteisėtas prisijungimas prie informacinių sistemų.

2. Daugiausiai kompiuterinių nusikaltimų padaro vyrai.

Dirbtinio intelekto priemonės darbo rengimo metu buvo naudotos informacijos paieškai, jos sisteminimui bei teksto redagavimo tikslams. Dirbtinio intelekto įrankiai naudoti kaip pagalbinė priemonė, o visa darbe pateikta informacija buvo savarankiškai vertinama ir analizuojama.

1. KOMPIUTERINIŲ NUSIKALTIMŲ SAMPRATA, TEISINIS REGULIAVIMAS IR TEISINIS REGLAMENTAVIMAS

Šiuolaikiniame pasaulyje kompiuterinių nusikaltimų samprata bei teisinis reguliavimas ir reglamentavimas šiandien įgauna vis didesnę reikšmę, kadangi sparčiai tobulėjančios informacinės technologijos plečia tiek teisėtų, tiek neteisėtų veiksmų galimybes elektroninėje erdvėje. Kompiuterio pagalba įvykdomos įvairios nusikalstamos veikos, kurios kelia riziką ne tik fizinių ir juridinių asmenų saugumui, bet ir valstybei, ekonomikai bei visuomenei. Šiame darbo skyriuje bus siekiama išnagrinėti kompiuterinių nusikalstamų veikų sampratą atribojant ją nuo elektroninių nusikalstamų veikų sąvokos, taip pat, nagrinėjamas kompiuterinių nusikaltimų tarptautinis teisinis reguliavimas bei teisinis reglamentavimas Lietuvos Respublikoje. Šiame darbe teisinis reguliavimas suprantamas kaip platesnė tarptautinių teisės normų ir principų visuma, o teisinis reglamentavimas – kaip konkrečių taisyklių, tvarkų ar reikalavimų nustatymas ir įtvirtinimas teisės aktuose.

1.1. Kompiuterinių nusikaltimų samprata

Kompiuterinių nusikaltimų atsiradimas yra glaudžiai susijęs su informacinių technologijų plėtra. XX amžiuje atsiradus pirmiesiems kompiuteriams, pastebimas ir pamažu kylantis kompiuterinių nusikaltimų skaičius. D. B. Parker – laikomas šių nusikaltimų tyrimų pradininku, kuris nuo XX a. aštuntojo dešimtmečio pradžios dalyvavo kompiuterinių nusikaltimų ir saugumo tyrimuose Jungtinėse Amerikos Valstijose (toliau – JAV), taip pat, buvo vienas pagrindinių autorių 1979 metų leidinio „Kompiuteriniai nusikaltimai – baudžiamosios justicijos išteklių vadovas (angl. – „*Computer Crime – Criminal Justice Resource Manual"*), kuriame kompiuterinius nusikaltimus apibrėžė plačiąja prasme kaip „bet koks neteisėtas veiksmas, kuriam atlikti būtinos kompiuterinių technologijų žinios".[20] Toks apibrėžimas yra diskutuotinas, kadangi tai suponuotų, jog bet kuri nusikalstama veika padaryta pasitelkiant kompiuterį arba kompiuterinių technologijų žinias, automatiškai laikytinas kompiuterinių nusikaltimu. Autorės nuomone, tai iš esmės išplečia sąvoką gerokai plačiau, nei ji suprantama šiuolaikinėje teisinėje doktrinoje. Baudžiamajame įstatyme kiekviena nusikalstamos veikos kategorija turi skirtingą saugomą vertybę, tad mokslininkai kompiuterinius nusikaltimus atriboja pagal saugomą vertybę- informacinių sistemų ir elektroninių duomenų saugumą.[21]

---

[20] National Criminal Justice Information and Statistics Service, *Criminal Justice Resource Manual* (U.S.: 1979), 5, https://www.ojp.gov/pdffiles1/Digitization/61550NCJRS.pdf.
[21] Marcinauskaitė, *supra note,* 11: 22.

Plečiantis kompiuterių naudojimui ir daugėjant su jais susijusių nusikaltimų, vis didesnis dėmesys buvo skiriamas šių nusikaltimų teisinio apibrėžimo analizei. Įvairiuose šaltiniuose galima pastebėti, jog kompiuteriniai nusikaltimai yra apibūdinami skirtingais terminais, priklausomai nuo konteksto. Vieni mokslininkai naudoja terminą „elektroniniai nusikaltimai“ (angl. *computer crime*), kiti - „su kompiuteriais susiję nusikaltimai“ (angl. *computer- related crime*) ar „technologijų nusikaltimai“ (angl. *high-tech crime*) ir panašiai.[22] XX a. pabaigoje, XXI a. pradžioje sparčiai išplito ne tik kompiuterių, bet ir interneto vartotojų skaičius. 1995 m. interneto naudotojų skaičius buvo 39,5 mln., 2005 m. siekė 1 mlrd. vartotojų, o 2010 m. beveik pasiekė 2 mlrd. interneto vartotojų pasaulyje.[23] Tokie statistiniai duomenys rodo sparčiai augantį interneto vartotojų skaičių, o toks intensyvus internetinės erdvės plėtimasis sudaro palankesnes sąlygas didėti ir su informacinėmis technologijomis susijusiam nusikalstamumui, nes besiplečianti vartotojų bazė lemia platesnį potencialių taikinių spektrą ir sudėtingesnį virtualios erdvės saugumo užtikrinimą. Įvairūs mokslininkai siekė atriboti kompiuterinių nusikaltimų sąvoką nuo kitų, gimininguų terminų, tokių kaip elektroniniai ar kibernetiniai nusikaltimai, pabrėždami jų skirtumus bei konceptualias ribas. G. E. Higgins teigė, jog kompiuterinius nusikaltimus galima suskirstyti į tris atskiras kategorijas. Pirmoji - kompiuterį panaudojant kaip priemonę daryti nusikalstamas veikas. Pavyzdžiui, neteisėtas kompiuterinės įrangos, muzikos ar filmų atsisiuntimas. Antroji- kompiuteris kaip objektas. Pasinaudojant įvairiomis priemonėmis ir turint specialiųjų žinių, asmenys gali įsilaužti į svetimą kompiuterį, vienas žinomiausių būdų yra programa „Trojos arklys“, kurios tikslas pagrobti svetimą informaciją arba ją ištrinti, arba užkrėsti kompiuterį virusu. Trečioji – kompiuteris kaip nusikalstamos veikos saugykla. Kompiuteris gali būti naudojamas laikyti duomenis, kurie savaime yra neteisėti, pavyzdžiui, pavogti asmens duomenys, finansiniai duomenys gauti sukčiavimo būdu arba pornografinio turinio medžiaga.[24] Kiti užsienio autoriai kompiuterinio pobūdžio nusikaltimus skirstė į dvi kategorijas, t.y. smurtinius arba potencialiai smurtinius nusikaltimus ir nesmurtinius nusikaltimus, laikantis nuomonės, kad kompiuteriniai smurtiniai nusikaltimai yra tokie, kurie kelia aukoms tiesioginę arba galimą fizinę grėsmę, pavyzdžiui, kibernetinis terorizmas.[25] Tokia terminų tapatinimo problema išlieka aktuali ir Lietuvoje, nors daugelis autorių pritaria nuomonei, jog kompiuteriniai nusikaltimai turėtų būti kriminalizuoti atsižvelgiant į šių nusikalstamų veikų saugomą vertybę – elektroninių duomenų ir

[22] Mindaugas Kiškis ir kt., *Teisės informatika ir informatikos teisė* (Vilnius: Mykolo Romerio universitetas, 2006), 230.
[23] Simon Kemp, „Digital 2026: Internet Ussers Pass The 6 Billions Mark“, *Datareportal,* 2025 m. spalio 15 d., https://datareportal.com/reports/digital-2026-six-billion-internet-users.
[24] George Higgins, *Cybercrime. An introduction to an Emerging Phenomenon (*New York: McGraw-Hill, 2010). ,1 – 2.
[25] Debra Littlejohn Shinder, *Scene of the Cybercrime: Computer forensics handbook* (Rockland: Syngress Publishing, 2002), 19 - 30.

informacinių sistemų saugumas, nors plačiąja prasme vertinant kompiuterinius nusikaltimus, tai apimtų kur kas daugiau saugomų vertybių, o tuo pačiu ir kitų nusikalstamų veikų, kaip sukčiavimas, elektroninio dokumento suklastojimas ar disponavimas juo (R. Petrauskas, D. Štitilis,[26] R. Marcinauskaitė,[27] U. Grigaitytė, M. Mackevičiūtė)[28].

Įvertinus skirtingų autorių požiūrį dėl kompiuterinių nusikaltimų tapatinimo problematikos, galima teigti, jog:

Kompiuteriniais nusikaltimais siaurąja prasme laikomos tik tos nusikalstamos veikos, kurios tiesiogiai siejasi su elektroniniais duomenimis ir informacinėmis sistemomis, kadangi jų esmę sudaro neteisėtas poveikis skaitmeninei informacijai ar jos apdorojimo sistemoms, siekiant sutrikdyti veiklą, pažeisti duomenų vientisumą ir gauti neteisėtos naudos. Tikslas - elektroniniai duomenys ir informacinė sistema.

Kompiuteriniais nusikaltimais plačiąja prasme laikomos tik tos nusikalstamos veikos, kurios atliekamos kompiuterinę informaciją panaudojant kaip nusikaltimo dalyką arba kai pats kompiuteris panaudojamas kaip nusikaltimo priemonė tikslui pasiekti.

2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų (toliau - Budapešto Konvencija)[29] įtvirtino, jog kompiuterinių nusikaltimų sąvoką pakeitė elektroninių nusikaltimų terminas, nurodant, jog elektroniniai nusikaltimai skirstomi į:

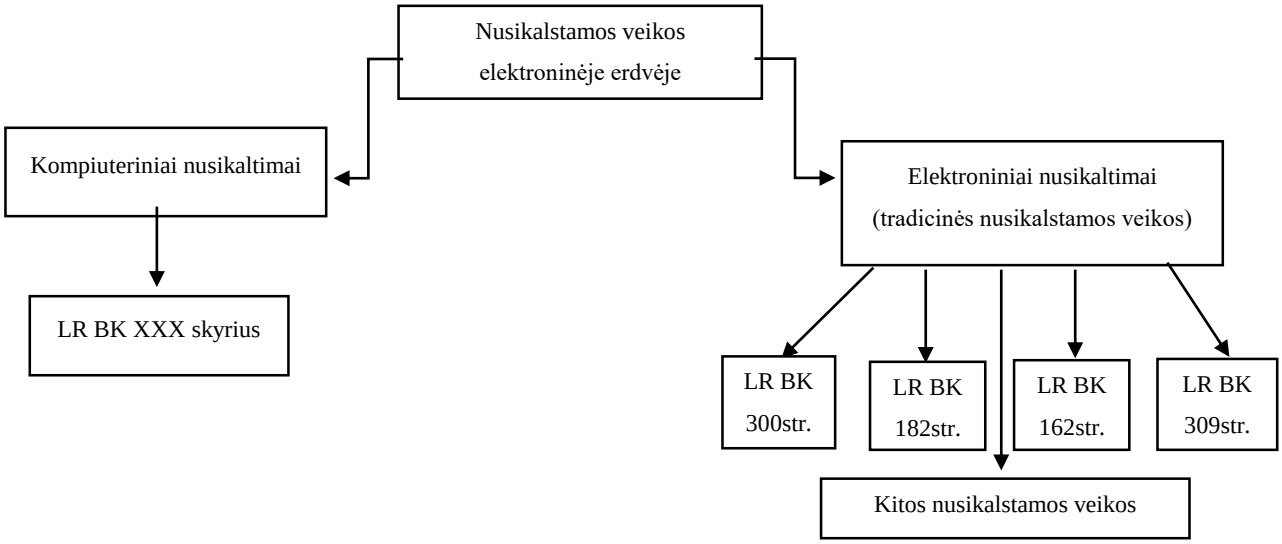
1. Nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui:
   a. *Neteisėta prieiga*
   b. *Neteisėta perimtis*
   c. *Poveikis duomenims*
   d. *Poveikis sistemai*
   e. *Netinkamas įtaisų naudojimas*
2. Su kompiuteriais susiję nusikaltimai (su kompiuteriais susijęs klastojimas, sukčiavimas)
3. Su turiniu susiję nusikaltimai (su vaikų pornografija susiję nusikaltimai)
4. Su autorių teisių ir gretutinių teisių pažeidimais susiję nusikaltimai.

[26] Petrauskas ir Štitilis, *supra note,* 6: 6.
[27] R. Marcinauskaitė, *supra note,* 10: 13 - 20.
[28] Ugnė Grigaitytė ir Miglė Mackevičiūtė, „Nusikaltimai virtualioje erdvėje- šiuolaikiniai iššūkiai ir prevencijos galimybės“, *Teisės mokslo pavasaris* Nr. 4, (2020): 276, https://www.zurnalai.vu.lt/openseries/article/view/21070/20214.
[29] „2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų (Žin., 2004, Nr. 36-1188)“, Infolex, žiūrėta 2025 m. rugsėjo 15 d., https://www-infolex-lt.skaitykla.mruni.eu/ta/84371#B_0.

2004 metais Lietuvoje įsigaliojus Budapešto Konvencijai, daugelyje šalių, tuo pačiu ir Lietuvoje buvo atlikti svarbūs pakeitimai tuometiniame baudžiamajame įstatyme[30] buvusių straipsnių bei papildyti naujais straipsniais. Galima teigti, jog kompiuterinės nusikalstamos veikos yra įtvirtintos Lietuvos Respublikos baudžiamojo kodekso (toliau - BK) aktualios redakcijos XXX skyriuje „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“, kuriame įtvirtintos tokios nusikalstamos veikos kaip „Neteisėtas poveikis elektroniniams duomenims“ (196 straipsnis), „Neteisėtas poveikis informacinei sistemai“ (197 straipsnis), Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“ (198 straipsnis), „Neteisėtas prisijungimas prie informacinės sistemos“ (198-1 straipsnis), „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis“ (198-2 straipsnis).[31]

Taigi, toks elektroninių nusikaltimų sąvokos išaiškinimas Budapešto Konvencijoje rodo, kad kompiuterinių nusikaltimų sąvoką apima tik tos nusikalstamos veikos, kurios įtvirtintos Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje, o visos kitos „tradicinės“ nusikalstamos veikos, kurios gali būti atliekamos elektroninėje erdvėje, nėra laikomos kompiuteriniais nusikaltimais, o priskiriamos elektroninių nusikaltimų sąvokai *(žr. 1 schemą)*.

1 schema. Elektroninėje erdvėje padarytų nusikalstamų veikų schema.



Autorė nori pabrėžti, jog „tradicinių“ nusikalstamų veikų sąrašas, kuris patenka į elektroninių nusikaltimų ribas, nėra baigtinis, kadangi Lietuvos Respublikos BK nėra apibrėžta elektroninių nusikaltimų saugoma vertybė. Tai yra tokios nusikalstamos veikos, kurios veikė

[30] „Lietuvos Respublikos baudžiamasis kodeksas (Žin., 2000, Nr. 89-2741)“, redakcija Nr. 4, Infolex, žiūrėta 2025 m. rugsėjo 15 d., https://www-infolex-lt.skaitykla.mruni.eu/ta/66150:ver4.
[31] „Lietuvos Respublikos baudžiamasis kodeksas (Žin., 2000, Nr. 89-2741), redakcija Nr. 121 (aktuali redakcija)“, Infolex, žiūrėta 2025 m. rugsėjo 15 d., https://www-infolex-lt.skaitykla.mruni.eu/ta/66150:ver121.

fizinėje erdvėje, tačiau tobulėjant technologijoms, šios nusikalstamos veikos praplėtė savo padarymo būdus ir vietas – persikėlė ir į elektroninę erdvę.

Apibendrinant galima teigti, jog sparčiai tobulėjant informacinėms technologijoms, nuosekliai daugėja ir elektroninėje erdvėje daromų nusikalstamų veikų. Tradiciniai nusikaltimai vis dažniau persikelia į virtualią erdvę, įgaudami naujas formas ir būdus. Nors kompiuterinių nusikaltimų sąvoka nėra tapati elektroninių nusikaltimų sąvokai, tačiau jos sąveikauja tarpusavyje ir turi tam tikrus bendrus bruožus, todėl tam tikrame kontekste šios sąvokos gali būti laikomos sinonimais. Kompiuterinių nusikalstamų veikų sąvoką tiksliausiai apibrėžia Lietuvos Respublikos BK XXX skyriuje įtvirtintos nusikalstamos veikos. Toliau šiame skyriuje bus analizuojamas kompiuterinių nusikaltimų tarptautinis teisinis reguliavimas.

1.2. Tarptautinis teisinis reguliavimas

Kompiuteriniai nusikaltimai dažnai pasižymi tarptautiniu pobūdžiu bei sudėtinga jurisdikcine priklausomybe. Šių nusikaltimų išskirtinumas kelia iššūkį nacionalinei teisės sistemai, nes “tradiciniai” šių veikų ištyrimo bei baudžiamosios atsakomybės pritaikymo būdai dažnai yra nepakankami, siekiant užtikrinti veiksmingą prevenciją bei tyrimą. Dėl to, tarptautinis teisinis reguliavimas yra būtinas, koordinuojant valstybių veiksmus, sudarant tarptautines sutartis bei standartizuojant procedūras kompiuterinių nusikaltimų prevencijai ir baudžiamąjai atsakomybei.

Dėl sparčiai plintančių kompiuterinių nusikaltimų, jų padarymo būdų bei teisinių spragų yra ypač sunku tokius nusikaltimus sukontroliuoti. Priešingai nei tradiciniai nusikaltimai, kurie paprastai apsiriboja fizinėmis teritorijoms su apibrėžtomis teisinėmis sistemomis, kompiuteriniai nusikaltimai peržengia vienos valstybės sienas ir neretai apima kelias jurisdikcijas. Tuo pačiu, neretai nusikaltėliai veikia tose jurisdikcijose, kuriose įstatymai yra prasčiau vykdomi ir mažiau dėmesio sutelkiama kompiuterinių nusikaltimų prevencijai ir ištyrimui. Tai lemia, kad aukos kitose pasaulio šalyse nukenčia nuo tokių veikų ir joms nėra sumokama patirtos žalos kompensacija, nusikaltimai lieka neištirti ir kaltininkas nenustatytas.[32] Todėl tarptautinis bendradarbiavimas yra itin svarbus veiksnys kovoje su kompiuteriniais nusikaltimais. Taigi, tokios šalių teisinės sistemos, grįstos tarptautiniais susitarimais, kaip pavyzdys Budapešto Konvencija, sukurtos ir iki šiol yra kuriamos siekiant sustiprinti tarpvalstybinį bendradarbiavimą, nustatyti

[32] Muhammad Umar Asghar, Muhammad Hassan Javed ir Sumia Azhar, „The regulation of Cybercrime in Internation Law: Discussing the Legal Frameworks and Challenges in Regulating Cybercrime“, *Indus Journal of Social Sciences* 3, 2 (2025): 418, https://www.researchgate.net/publication/391623650_The_Regulation_of_Cybercrime_in_International_Law_Discussing_the_Legal_Frameworks_and_Challenges_in_Regulating_Cybercrime.

suvienodintus kovos su kompiuteriniais nusikaltimais standartus ir palengvinti tarpvalstybinį informacijos bei išteklių dalijimąsi.[33]

Viena išsamiausių ir pažangiausių konvencijų kovai su kompiuteriniais nusikaltimais laikoma Budapešto Konvencija. Jos tikslas yra suvienodinti baudžiamąją politiką, sukuriant bendrą teisinį pagrindą kovai su elektroniniais nusikaltimais bei suderinti veiksmingą elektroninių įrodymų rinkimą skatinant tarptautinį bendradarbiavimą. Svarbu paminėti, jog Budapešto Konvencijos 35 straipsnyje įtvirtinta nuostata, jog kiekviena valstybė narė privalo teikti skubią pagalbą tyrimui bylos nagrinėjimui paskirdama ryšio punktą, veikiantį visą parą 7 dienas per savaitę. Tai yra labai naudinga kai reikia teikti neatidėliotiną pagalbą, renkant įrodymus ar konsultuojantis.

2025 metų duomenimis[34], Budapešto Konvenciją ratifikavo 81 valstybė, iš jų daugiau nei 26 šalys yra Europos Sąjungos valstybės narės. Atsižvelgiant į tai, kad Europoje yra apie 50 valstybių, galima teigti, kad Budapešto konvencija daro nemažą įtaką kovai su elektroniniais nusikaltimais, tačiau siekiant kuo geresnių rezultatų - daugiau šalių turėtų į tai įsitraukti, jog būtų suvienodintas teisinis reguliavimas bei glaudesnis bendradarbiavimas. Visgi, nors ir yra pritariama nuomonei, jog Budapešto Konvencija yra pagrindinis įrankis kovai su tokio pobūdžio nusikaltimais, tačiau yra manoma, jog ji „susiduria su ribotais prisitaikymo prie sparčiai besivystančių technologijų sunkumais ir iššūkiais dėl skirtingo valstybių narių įsipareigojimo lygio.“[35] Tokie sunkumai kelia problemą, jog yra nenuosekliai kuriamos elektroninių nusikaltimų prevencijos ir baudžiamojo persekiojimo priemonės, o tai yra naudinga nusikaltėliams.

Budapešto Konvencijos realizavimo įrankiu laikoma tarptautinė kriminalinės policijos organizacija – Interpolas. Jau nuo 1990 metų ši organizacija aktyviai veikia tiriant ir išaiškinant įvairaus pobūdžio elektroninius nusikaltimus, o šios organizacijos svarba matoma ir šiais laikais. Šiuo metu, ją sudaro 196 šalys, kurios nuolatos bendradarbiauja tarpusavyje, atlieka bendras operacijas. Viena naujausių jų atliktų sėkmingų operacijų įvyko 2025 m. lapkričio 27 d., kai 19 skirtingų šalių buvo suimti 574 asmenys, įtariami verčiantis el. pašto užgrobimu, skaitmeninio turto prievartavimu ir išpirkos reikalaujančiomis kenkėjiškų programų virusais (angl. - *Ransomware).* Operacijos metu buvo susigrąžinta apie 3 mln. JAV dolerių, taip pat pašalinta daugiau nei 6000 kenkėjiškų nuorodų bei iššifruoti šeši skirtingi išpirkos reikalaujančių programų

[33] Asghar, Javed ir Azhar, *supra note*, 32: 418.
[34] „Chart of signatures and ratifications of Treaty 185“, Council of Europe Portal, žiūrėta 2025 m. gruodžio 26 d., https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.
[35] Enver Bucaj ir Kenan Idrizaj, „The need for cybercrime regulation on a global scale by the international law and cyber convention“, *Multidisciplinary Reviews* 8, 1 (2024): 4, https://www.researchgate.net/publication/385089998_The_need_for_cybercrime_regulation_on_a_global_scale_by_the_international_law_and_cyber_convention.

būdai. Mėnesį trukusi operacija padėjo susieti šiuos nusikaltėlius su įvykdytais nusikaltimais, kurių metu finansiniai nuostoliai, viršijo 21 mln. JAV dolerių.[36]

Be kriminalinės žvalgybos atliekamų veiksmų bei realių nusikalstamų veikų užkardymų, Interpolas nuolat teikia ekspertų konsultacijas, organizuoja mokymus, internetines mokymo programas, seminarus. 2025 m. spalio 25 d. Vietname Interpolas organizavo konferenciją „Nuo sistemos iki praktinių tyrimų: Interpolo vaidmuo įgyvendinant JT Konvenciją dėl kibernetinių nusikaltimų“[37], kurioje buvo pristatyta, jog Interpolas, turėdamas pasaulinio lygio pajėgumus, platų narių skaičių, gali „Konvencijos straipsnius paversti realiais veiksmais“, kitaip sakant, veikiant pagal Budapešto Konvenciją išardyti elektroninėje erdvėje veikiančių nusikaltėlių tinklus pasitelkiant tarpvalstybinį bendradarbiavimą.

Svarbų vaidmenį tarptautinio teisinio reguliavimo raidoje taip pat užima 1989 m. Europos Tarybos priimtos rekomendacijos Nr. R(89)9[38], kuriose buvo sistemiškai aptarti kompiuteriniai nusikaltimai ir pateiktos gairės valstybėms narėms dėl jų kriminalizavimo. Rekomendacijose buvo siūloma kompiuterinius nusikaltimus išskirti į dvi grupes. Pirmoji grupė, tai nusikalstamos veikos, kurios laikytinos pavojingiausiomis ir kurias yra būtina kriminalizuoti (neteisėta prieiga prie kompiuterinių sistemų, neteisėtas duomenų perėmimas, duomenų ar programų pakeitimas/sunaikinimas, kompiuterinis sukčiavimas, kompiuterinis klastojimas), antrojoje grupėje nurodomos mažiau pavojingos nusikalstamos veikos, dėl kurių kriminalizavimo dar būtina svarstyti (neteisėtas programų naudojimas, autorių teisių pažeidimas, privatumo pažeidimai, piktnaudžiavimas duomenimis). Tokie suformuoti nusikaltimų kriminalizavimo principai tapo pagrindu vėliau priimtai Budapešto Konvencijai.

1995 m. Europos Taryba priėmė rekomendaciją Nr. R(95)13[39], kurioje išreiškė didelį susirūpinimą, jog pastebimas vis didesnis informacinių technologijų vystymasis ir jų naudojimas daugelyje visuomenės sektorių, kas gali sukelti padidintą nusikalstamumą. Didelis dėmesys skiriamas įrodymų rinkimui elektroninėje erdvėje, kadangi iškyla rizika, jog valstybės narės nesugebės bendradarbiaujant tinkamai surinkti įrodymus elektroninėje erdvėje. Dėl to

---

[36] „574 arrests and USD 3 million recovered in coordinated cybercrime operation across Africa“, Interpol, žiūrėta 2025 m. gruodžio 26 d., https://www.interpol.int/News-and-Events/News/2025/574-arrests-and-USD-3-million-recovered-in-coordinated-cybercrime-operation-across-Africa.

[37] „From Framework to Fieldwork: INTERPOL‘s Role in Advancing the UN Cybercrime Convention“, United Nations Office on Drugs and Crime, žiūrėta 2025 m. gruodžio 27 d., https://hanoiconvention.org/side-event/from-framework-to-fieldwork-interpols-role-in-advancing-the-un-cybercrime-convention/.

[38] European Committee on Crime Problems, *Computer – Related Crime, Recommendation No. R(89)9 on computer - related crime and final report of the European Committee on Crime Problems* (Strasbourg: Council of Europe, 1990), https://www.oas.org/juridico/english/89-9&final%20Report.pdf.

[39] Council of Europe, *Recommendation No. R(95) 13, of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law Connected with Information Technology* (Strasbourg: Council of Europe, 1995), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76.

rekomendacijose yra aptartos baudžiamojo proceso problemos, nurodyti nauji procesiniai veiksmai kaip krata ir poėmis, techninis stebėjimas (telekomunikacijų kontrolė), akcentuojama, jog turi būti svarstoma galimybė steigti specializuotus padalinius tokio pobūdžio nusikalstamoms veikoms tirti, skatinti tokių darbuotojų mokymus ir technologinių žinių išplėtimą.

Kiek vėliau, kompiuteriniams nusikaltimams plintant ir keičiantis jų formoms, priimti nauji, visuotinai svarbūs teisės aktai. 2013 m. Europos parlamentas ir Taryba priėmė direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR[40]. Direktyva pažymi organizuoto nusikalstamumo grėsmę, kuri yra nukreipta prieš informacines sistemas, kurios yra itin svarbios valstybių narių ir Sąjungos informacinei sistemai. Tai kelia riziką informacinės visuomenės stabilumui, laisvei, saugumui, ir apskritai visos valstybės funkcionavimui. Taip pat, pabrėžiama ir prevencija, jog kibernetinių grėsmių, pažeidžiamumų ir su informacinėmis sistemomis susijusių rizikų nustatymas bei savalaikis informavimas apie juos yra esminė veiksmingos kibernetinio saugumo prevencijos ir reagavimo dalis. Ankstyvas saugumo spragų atpažinimas ir pranešimas leidžia sumažinti padaromą žalą ir greičiau imtis apsaugos priemonių. Direktyva pažymi, jog valstybės narės turėtų siekti sukurti sąlygas, kurios skatintų greitai ir efektyviai pranešti apie tokias spragas kompetentingoms institucijoms. Tačiau Lietuvos praktika[41] rodo, kad šių nuostatų įgyvendinimas susiduria su tam tikrais iššūkiais. Pagal Nacionalinio kibernetinio saugumo centro (toliau – NKSC) pateiktą informaciją, kibernetinio saugumo (toliau – KS) spragą pastebėjęs asmuo turi 4 pasirinkimus:

1. Neatskleidimas. Asmuo apie spragą nieko neinformuoja.
2. Pilnas atskleidimas. Apie spragą pranešama viešai, nesudarant galimybės subjektui laiku pašalinti spragos.
3. Ribotas atskleidimas. Informacija apie spragą pateikiama NKSC.
4. Informacijos apie spragą pranešimas kibernetinio saugumo subjektui, kurio sistemoje buvo aptikta spraga.

Tačiau Lietuvos Respublikos teisėje iki šiol nėra aiškiai apibrėžto KS spragų atskleidimo apibrėžimo, o nacionaliniai kibernetinio saugumo subjektai ne visada viešai skelbia atsakingo atskleidimo apie spragą tvarką, todėl spragą aptikęs asmuo negali būti tikras ar ši spraga bus pašalinta, o tuo pačiu, susidūręs su tokia problema nežino ką tiksliai turėtų daryti – ar žinią

[40] „2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR“, EUR - Lex, žiūrėta 2026 m. sausio 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32013L0040.

[41] „Pranešti apie spragą“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. sausio 2 d., https://www.nksc.lt/pranesti-spraga.html.

paskelbti viešai, kad kuo daugiau žmonių būtų įspėti ar pranešti kibernetinio saugumo subjektui ar NKSC ir tikėtis, kad greitu metu kažkas sureaguos.

Kaip ir Budapešto Konvencijoje, Direktyvoje 2013/40/EU įtvirtinta, jog visą parą, septynias dienas per savaitę veikiantys informaciniai punktai yra itin svarbūs tarpvalstybiniam bendradarbiavimui, kadangi reikalinga informacija suteikiama per trumpiausią įmanomą laiką. Nors ir pritariama, jog šis mechanizmas yra patobulintas, tačiau Direktyva 2013/40/EU susilaukia nemažai kritikos, kadangi nors ir Direktyva padėjo sukurti „bendrą kibernetinių nusikaltimų kalbą“, tačiau Direktyva nenumatė jokio veiksmingo tarpvalstybinio baudžiamojo persekiojimo mechanizmo, o visą procedūros įgyvendinimą iš esmės paliko valstybinių tarpusavio bendradarbiavimo mechanizmui, kuris ne visada užtikrina efektyvų vykdymą[42].

Pastaraisiais dešimtmečiais nuosekliai plėtojant tarptautinį teisinį reguliavimą, kompiuterinių nusikaltimų paplitimas ir jų daroma žala iki šiol išlieka itin didele problema. Nuo kompiuterinių nusikaltimų atsiradimo priimta nemažai svarbių tarptautinių teisės aktų, įskaitant konvencijas, rekomendacijas bei direktyvas – tai neabejotinai padarė teigiamą poveikį, kadangi valstybės suvienodino kompiuterinių nusikaltimų sąvoką, šias nusikalstamas veikas kriminalizavo bei bendromis jėgomis formavo tarptautinio lygmens prevencijos bei tyrimo standartus. Tačiau išanalizavus keletą, autorės nuomone, vienus svarbiausių teisės aktų, manoma, kad vien norminių teisės aktų gausa ar apskritai jų kūrimas neužtikrina kompiuterinių nusikaltimų užkardymo. Nusikaltėliai itin profesionaliai pasinaudoja informacinių technologijų teikiamomis galimybėmis, nuolat tobulina bei atnaujina nusikaltimų padarymo būdus ir metodus, tuo pačiu apsunkindami teisėsaugai šių nusikalstamų veikų atskleidimą ir ištyrimą. Taigi, tampa akivaizdu, kad kova su kompiuteriniais nusikaltimais negali būti grindžiama vien teisinio reguliavimo plėtra, kadangi būtinas kompleksinis požiūris, apimantis ne tik teisines, bet ir efektyvias technines prevencines priemones.

1.3. Kompiuterinių nusikalstamų veikų reglamentavimas Lietuvos Respublikos teisėje

1961 m. Lietuvoje galiojusiame baudžiamajame kodekse[43], (toliau – 1961 m. BK) kompiuterinių nusikalstamų veikų reglamentavimas nebuvo konkretus ir išsamus - tokios

[42] Elemegoius Mugamba, „Cross-border cybercrime enforcement and legislative harmonisation: a comparative study of EU Directive 2013/40/EU and non-EU jurisdictions”, *Research Gate,* 2025 m. spalio mėn., 2, https://www.researchgate.net/publication/398757570_CROSS-BORDER_CYBERCRIME_ENFORCEMENT_AND_LEGISLATIVE_HARMONISATION_A_COMPARATIVE_STUDY_OF_EU_DIRECTIVE_201340EU_AND_NON-EU_JURISDICTIONS.

[43] „Dėl Lietuvos tarybų socialistinės Respublikos baudžiamojo kodekso patvirtinimo“, Vyriausybės žinios, žiūrėta 2026 m. gegužės 9 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.20465/jxfupAglbe.

nusikalstamos veikos dar nebuvo išskirtos į atskirą baudžiamojo įstatymo skyrių. Kodekse buvo išskirtos tik šios nusikalstamos veikos, susijusios su kompiuteriniais nusikaltimais:

1. BK 135^2 straipsnis „tyčinis poveikis kompiuterinei informacijai ar jos apdorojimui“ numatė baudžiamąją atsakomybę už neteisėtos kompiuterinės programos sukūrimą, klaidingų duomenų įrašymą ar kitokį tyčinį poveikį kompiuterinei informacijai. Vis dėlto, atsakomybė grėsė tik tuomet, kai tokie veiksmai susiję su rinkimų ar referendumo rezultatų paveikimu.

2. 1961 m. BK 274 straipsnis „sukčiavimas“, kuriame numatyta baudžiamoji atsakomybė užvaldžius svetimą turtą ar apgaule įgijus teisę į turtą. Šiame straipsnyje numatyta alternatyva, kai nusikalstama veika padaroma sudarant žinomai neteisingą kompiuterinę programą, įrašant klaidingus duomenis ar kitaip paveikiant kompiuterinius duomenis.

3. 1961 m. BK 277 straipsnis „Turtinės žalos padarymas apgaule arba piknaudžiaujant pasitikėjimu“, kuriame numatyta baudžiamoji atsakomybė ir sudarant žinomai neteisingą kompiuterinę programą, įrašant klaidingus duomenis ar kitaip paveikiant kompiuterinius duomenis. Šie trys tuometinio baudžiamojo kodekso straipsniai priskirti skyriams „Nusikaltimai politinėms ir darbinėms piliečių teisėms“ ir „Nusikaltimai nuosavybei“ rodo, jog informacinės sistemos ir elektroniniai duomenys nebuvo laikomi kaip įstatymo saugoma vertybė, bet kaip priemonė nusikalstamoms veikoms daryti.

Vėliau, įsigaliojus 2003 m. BK[44], skyriuje „Nusikaltimai informatikai“ iki tol buvusius straipsnius pakeitė BK 196 straipsnis „kompiuterinės informacijos sunaikinimas ar pakeitimas“, 197 straipsnis „kompiuterinės programos sunaikinimas ar pakeitimas“ ir 198 straipsnis „kompiuterinės informacijos pasisavinimas ir skleidimas“. Skyriaus pavadinimas „Nusikaltimai informatikai“ buvo kritikuojamas. Lietuvių kalbos žodyną „informatika“ – tai „mokslo sritis, tirianti visų rūšių informacijos kūrimo, kaupimo, apdorojimo ir perdavimo techninėmis priemonėmis dėsnius ir būdus.“[45] Ši sąvoka neapima elektroninių duomenų ar informacinių sistemų sąvokų, tad ilgainiui pastebėta, kad toks skyriaus pavadinimas neatitinka įstatymo saugomos vertybės.

Budapešto Konvencija turėjo didelę reikšmę kompiuterinių nusikalstamų veikų teisinio reglamentavimo raidai Lietuvoje. Ši Konvencija įpareigojo valstybes savo nacionalinėje teisėje kriminalizuoti tam tikras su informacinėmis sistemomis ir elektroniniais duomenimis susijusias nusikalstamas veikas bei nustatyti veiksmingą baudžiamąją atsakomybę.[46] 2004 m. Ratifikavus

---

[44] „Lietuvos Respublikos baudžiamasis kodeksas (Žin., 2000, Nr. 89-2741)“ redakcija Nr. 1, Infolex, žiūrėta 2026 m. gegužės 4 d., https://www-infolex-lt.skaitykla.mruni.eu/ta/66150:ver1.

[45] „Informatika reikšmė“, lietuvių žodynas, žiūrėta 2023 m. spalio 16 d., https://www.lietuviuzodynas.lt/terminai/Informatika.

[46] Darius Sauliūnas, „Legislation On Cybercrime In Lithuania: Development and legal gaps in Comparison With The Convention On Cybercrime“, *Jurisprudencija* 4, 122 (2010): 207, https://ojs.mruni.eu/ojs/jurisprudence/article/view/1034/989.

Budapešto Konvenciją, baudžiamasis įstatymas[47] pasipildė dviem naujais straipsniais, t.y. neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo (198[1] str.) ir neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti (198[2] str.), toks pakeitimas lėmė, jog nėra būtini tokie padariniai kaip turtinės žalos atsiradimas, užtenka pačio fakto, jog kaip pavyzdys, asmuo neteisėtai prisijungė prie kito asmens duomenų. Taip pat, ratifikavus Budapešto Konvenciją baudžiamojo įstatymo XXX skyriuje įtvirtintos nusikalstamos veikos buvo pakoreguotos – beveik visi šiame skyriuje esantys straipsniai pasipildė nauja dalimi, kurioje išskiriama, jog yra taikoma atsakomybė su griežtesne sankcija tuomet, kai nusikalstamos veikos darymui panaudojama strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius elektroninius duomenis. Taip pat buvo išplėstos ir alternatyvių bausmių rūšys. Ilgainiui, BK XXX skyrius buvo pakeistas į „nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“, buvo atlikti svarbūs BK 198 straipsnio pakeitimai – terminą „pasisavina“ pakeitė „stebi, įrašo, perima, įgyja, saugo, pasisavina, platina ar kitaip naudoja“. Galiojantis baudžiamasis kodeksas numato, kad visos BK XXX skyriuje numatytos nusikalstamos veikos yra nesunkūs arba apysunkiai nusikaltimai, o baudžiamoji atsakomybė už kompiuterines nusikalstamas veikas gali būti taikoma ne tik fiziniam, bet ir juridiniam asmeniui.

Visgi, Budapešto Konvencijos veiksmingumas tam tikrais aspektais mažėja, kadangi sparčiai besikeičiant technologijoms, atsirado naujų kompiuterinių nusikaltimų būdų ir priemonių. Pavyzdžiui, sparčiai plinta virtualios erdvės pinigai – kriptovaliutos, kurios dažnai naudojamos išpirkos reikalaujančiose atakose, reikalaujant mokėti kriptovaliutomis. Daugelį kriptovaliutų tinklų veikia anonimiškumo principu, todėl juos yra sudėtinga atsekti ir konfiskuoti. Nors Budapešto Konvencijos 19 straipsnis apibrėžia kompiuterinių duomenų konfiskavimą, jis nėra pritaikytas skaitmeniniams pinigams.[48]

Apibendrinant, kompiuterinių nusikalstamų veikų teisinis reglamentavimas Lietuvoje formavosi palaipsniui, atsižvelgiant į informacinių technologijų paplitimą ir naujų nusikalstamų veikų atsiradimą. Iš pradžių, su informacinėmis technologijomis susijusios nusikalstamos veikos buvo integruojamos į tradicinių nusikalstamų veikų sudėtis, tačiau ilgainiui atsirado poreikis sukurti atskirą kompiuterinių nusikalstamų veikų reglamentavimą. Reikšmingą įtaką šiam procesui turėjo Budapešto Konvencijos ratifikavimas ir jos nuostatų perkėlimas į nacionalinę teisę, kurios sudarė prielaidą aiškesniam kompiuterinių nusikaltimų kriminalizavimui.

---

[47] „Lietuvos Respublikos baudžiamasis kodeksas (Žin., 2000, Nr. 89-2741)“, redakcija Nr. 4, *supra note, 30.*

[48] Francois Regis Nshimiyimana, „Adapting the Budapest Convention to Address Emerging Cyber Threats“, *Belugyi Szemle* 74, 1 (2026): 187, https://www.researchgate.net/publication/400408531_Adapting_the_Budapest_Convention_to_address_emerging_cyber_threats.

2. KOMPIUTERINIŲ NUSIKALTIMŲ RAIŠKA

Analizuojant kompiuterinių nusikaltimų raišką, svarbu įvertinti ne tik kiekybinius rodiklius, bet ir šių nusikaltimų struktūrą, jų daromą žalą bei pasiskirstymą, atsižvelgiant į kompiuterinių nusikaltimų latentiškumo lygį. Tokia analizė leidžia geriau suprasti vyraujančias tendencijas ir identifikuoti problemines sritis, kurios reikalauja didesnio teisėsaugos institucijų dėmesio. Atsižvelgiant į tai, toliau šiame skyriuje bus analizuojama kompiuterinių nusikaltimų paplitimas nacionaliniu ir tarptautiniu lygiu, kaip šie nusikaltimai su metais kinta, kokios jų pagrindinės rūšys bei kokia jų yra galima žala.

2.1. Paplitimas, struktūra ir dinamika Lietuvoje ir Europos Sąjungoje

Vienas pagrindinių kriminologinės informacijos šaltinių yra registruoto nusikalstamumo statistiniai duomenys. Analizuojant šiuos duomenis galima nustatyti nusikalstamų veikų paplitimą pasirinktu laikotarpiu (būklė), kaip plačiai ji yra paplitusi (paplitimas), nusikalstamų veikų pasiskirstymą pagal rūšis (struktūra) ir kaip jos keičiasi bėgant laikui (dinamika). Vertinant nusikalstamumo būklę, nereikėtų remtis vien tik oficialiais registruotais atvejais.[49] Ypatingai kalbant apie kompiuterinius nusikaltimus, kurie pasižymi aukštu latentiškumo laipsniu, kadangi tokius nusikaltimus sunkiau pastebėti ir nustatyti nei „tradicinius“, aukos vengia informuoti apie tai teisėsaugos institucijas[50], o ir teisėsaugos institucijos dėl didelių darbo krūvių, turimų žmogiškųjų ir techninių resursų trūkumo, vengia registruoti pranešimus apie padarytą nusikalstamą veiką, jog kuo mažiau reikėtų pradėti ikiteisminių tyrimų.[51] Nepaisant to, registruoto nusikalstamumo statistiniai duomenys leidžia objektyviau susidaryti nusikalstamų veikų „bendrą vaizdą“, stebėti tendencijas bei kurti prevencijos strategijas. Šiame skyriuje toliau pateikiama analizė apima 2020 – 2025 m. Lietuvoje registruotus kompiuterinius nusikaltimus.

Nagrinėjant kompiuterinių nusikaltimų būklę ir lygį Lietuvoje, atsižvelgiama į gyventojų skaičių bei demografinius rodiklius, kurie leidžia nusikalstamumo mastą įvertinti proporcingai. Oficialios statistikos duomenimis, laikotarpiu nuo 2020 metų iki 2025 metų Lietuvos gyventojų skaičius išaugo maždaug 78 tūkst. Gyventojų *(žr. 1 diagramą)*[52] arba 2,7 %. Norint kuo

---

[49] Alfredas Kiškis, „Nusikalstamumas Lietuvoje: ko neparodo oficialioji statistika?“, Mokslo darbai 11, 113 (2008): 114–123, https://www.researchgate.net/publication/289525848_Nusikalstamumas_Lietuvoje_ko_neparodo_oficialioji_statistika.

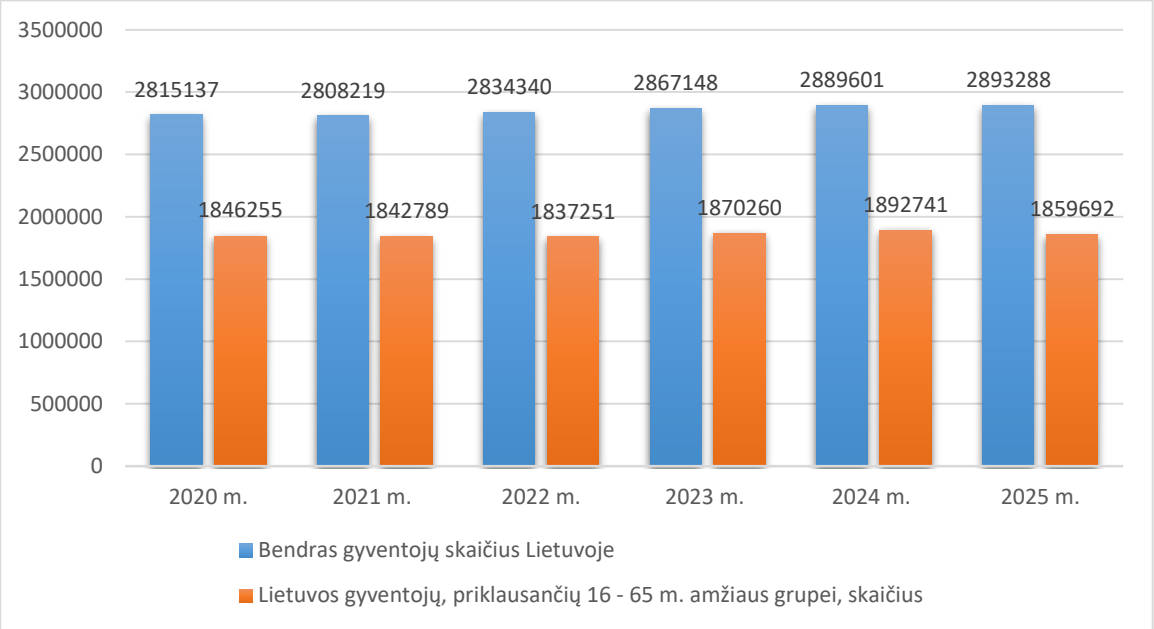
[50] Grigaitytė ir Mackevičiūtė, *supra note 28:* 288.

[51] Genovaitė Babachinaitė ir kt., *Kriminologija: vadovėlis* (Vilnius: Mykolo Romerio universitetas, 2010), 65-66.

[52], „Nuolatinių gyventojų skaičius metų pradžioje“, Oficialiosios statistikos portalas, žiūrėta 2026 m. kovo 22 d., https://osp.stat.gov.lt/statistiniu-rodikliu-analize?indicator=S3R166#/.

objektyviau įvertinti kompiuterinių nusikaltimų paplitimą analizuojamu laikotarpiu, svarbu atsižvelgti ir į Lietuvos gyventojų amžiaus grupę, todėl pasirenkama 16-65 metų amžiaus grupė, kadangi pagal baudžiamąjį kodeksą atsako asmuo, kuriam iki nusikaltimo ar baudžiamojo nusižengimo padarymo yra suėję 16 metų, o 65 metų riba pasirinkta atsižvelgiant į 2026 metų Lietuvos pensinį amžių.[53] Tiriamuoju laikotarpiu šios amžiaus grupės asmenys sudarė 65,2 % visų Lietuvos gyventojų.

1 diagrama. Gyventojų skaičius Lietuvoje 2020 – 2025 m. laikotarpiu.



Pagal užregistruotų visų nusikalstamų veikų Lietuvoje duomenis, 2020 m. užregistruota 46306 nusikalstamų veikų (t.y. 2508 nusikalstamos veikos tenkančios 100 tūkst. 16 – 65 m. amžiaus gyventojams), kai tuo tarpu per 2025 m. užregistruota 42961 nusikalstamų veikų (t.y. 2310 nusikalstamos veikos tenkančios 100 tūkst. 16 – 65 m. amžiaus gyventojams)[54]. Tokie duomenys rodo, jog užregistruotų nusikalstamų veikų rodikliai per pastaruosius 5 metus gerėjo – nusikalstamų veikų sumažėjo 7,2 %, o ir didėjant Lietuvoje gyventojų skaičiui, 7,9 % sumažėjo nusikalstamų veikų skaičius tenkantis 100 tūkst. gyventojų (16 – 65 m. amžiaus grupei).

[53] „Senatvės pensijos amžiaus lentelė“, Sodra, žiūrėta 2026 m. kovo 16 d., https://sodra.lt/senatves-pensijos-amziaus-lentele.

[54] Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos „Užregistruotos nusikalstamos veikos Lietuvoje“, Informatikos ir ryšių departamentas, žiūrėta 2026 m. kovo 16 d., https://www.ird.lt/lt/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos-3/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos-2/nusikalstamos-veikos-lietuvoje-2006-2025-metais-2.

1 lentelė. Užregistruotų Lietuvos Respublikos BK XXX skyriuje numatytų nusikalstamų veikų, skaičius 2020-2025 metų laikotarpyje.

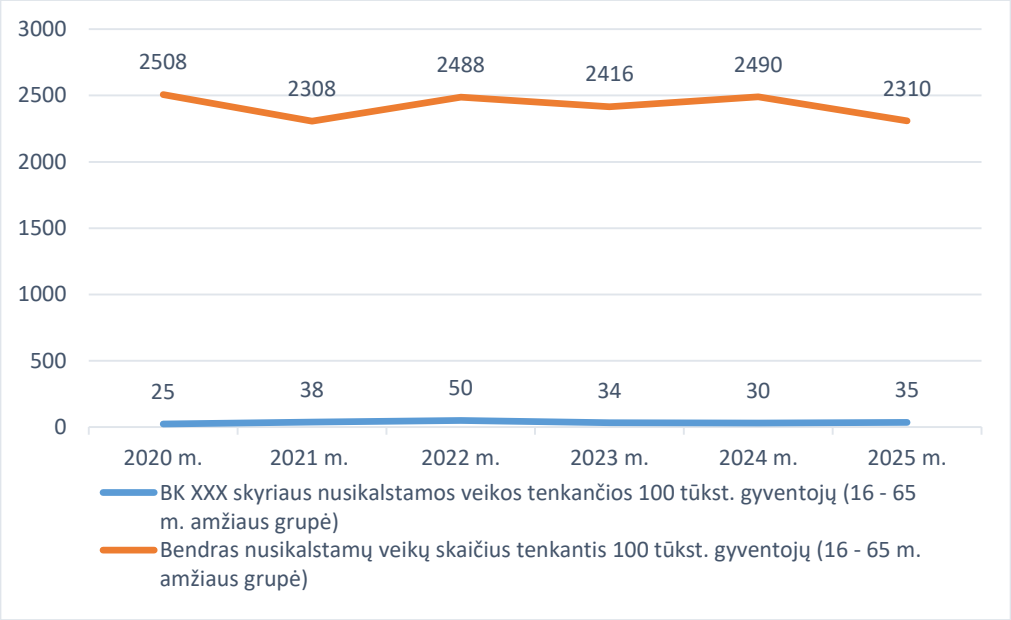
2020 Sausis- gruodis	2021 Sausis- gruodis	2022 Sausis- gruodis	2023 Sausis- gruodis	2024 Sausis- gruodis	2025 Sausis- gruodis
460	705	917	637	575	647

Analizuojant 2020 – 2025 m. Lietuvoje užregistruotų BK XXX skyriaus nusikalstamų veikų statistiką (žr. 1 lentelę.)[55], galima pastebėti, jog registruotų nusikalstamų veikų skaičius kito netolygiai. 2020 m. pasižymi mažiausiu, o 2022 m. didžiausiu registruotų nusikalstamų veikų skaičiumi (padidėjo 99,4 %). Tokį kompiuterinių nusikaltimų padidėjimą Lietuvoje, autorės nuomone, lėmė kelios priežastys. 2020 metais Lietuvoje prasidėjo COVID-19 pandemija, kuri pakeitė daugelio Lietuvos ir pasaulio žmonių įpročius. Kelis metus vyraujančią įtampą lėmusią karantino ribojimai, įvairūs draudimai, žmones paskatino plačiau naudotis kibernetine erdve – 2022 metais ženkliai padaugėjo nuotolinio darbo galimybių, padažnėjo internetiniai pirkimai, ugdymas ir laisvalaikis persikėlė į internetinę erdvę.[56] Taip pat, 2022 metais pasibaigus pandemijai, Europą, įskaitant ir Lietuvą, pasiekė dar viena geopolitinė situacija – Rusijos invazija į Ukrainą, kuri lėmė didesnę kibernetinių atakų bangą ir padidino kibernetinio saugumo riziką. Šios susidariusios globalios grėsmės sukūrė padidintą žmonių priklausomybę nuo informacinių technologijų, o būtent interneto, kas lėmė silpnesnę jo apsaugą, sumažėjusį žmonių budrumą ir paskatino nusikaltėlius išnaudoti atsiradusias spragas. Vis dėlto, nors 2023 m. registruotų nusikalstamų veikų skaičius mažėjo, 2025 m. matomas pakartotinis šių nusikalstamų veikų augimas, kuris lyginant su 2020 m. išaugo 40,7 %.

[55] Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, „Nusikalstamumo duomenų rinkiniai“, Informatikos ir ryšių departamentas, žiūrėta 2026 m. kovo 22 d., https://www.ird.lt/lt/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos/nusikalstamumo-duomenu-rinkiniai/dimension.BK?BK%5B%5D=XXX&DT%5B%5D=2025-11&SAV%5B%5D=LR&cols=DT.

[56] Lietuvos Respublikos Krašto apsaugos ministerija, *Nacionalinė kibernetinio saugumo ataskaita 2022*, (Lietuva: 2023), 51, https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf.

2 diagrama. Nusikalstamumo lygis 100 tūkst. gyventojų (16 – 65 m. amžiaus grupei) 2020 – 2025 m.



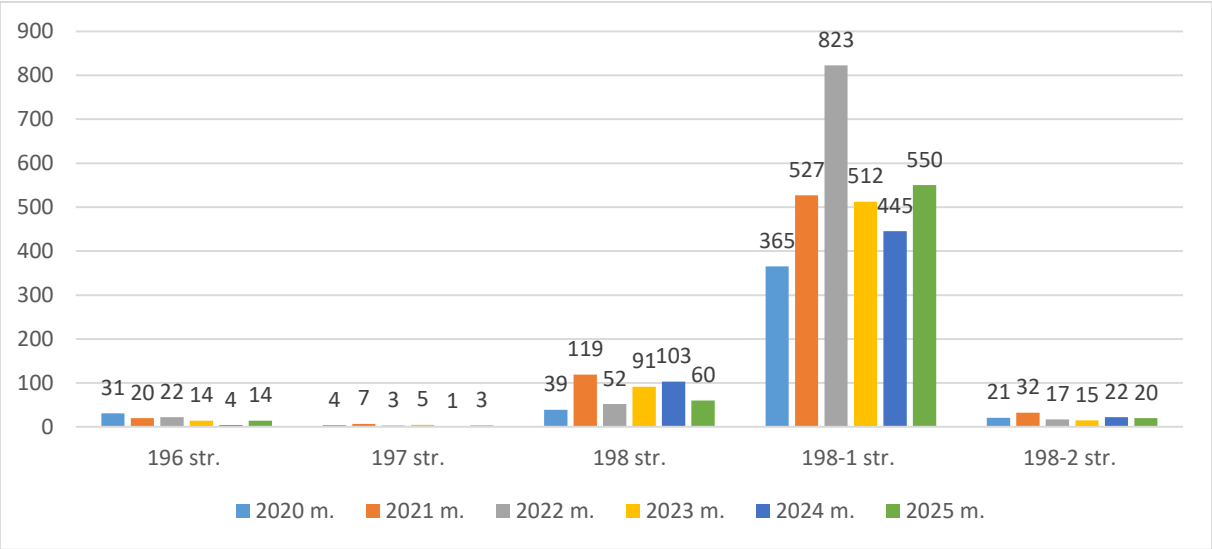
Lyginant BK XXX skyriuje numatytų nusikalstamų veikų lygį su bendru registruotų nusikalstamų veikų skaičiumi, tenkančiu 100 tūkst. 16 – 65 m. amžiaus gyventojų, matoma, kad kompiuteriniai nusikaltimai sudaro santykinai tik nedidelę bendro nusikalstamumo dalį (*žr. 2 diagramą*).[57] Analizuojamu laikotarpiu didžiausia kompiuterinių nusikaltimų dalis fiksuota 2022 m., kai šios nusikalstamos veikos sudarė 2,01 % visų registruotų nusikalstamų veikų. Kitais metais kompiuteriniai nusikaltimai kasmet sudarydavo 1 – 1,65 % visų registruotų nusikalstamų veikų, tenkančių 100 tūkst. 16 – 65 m. amžiaus gyventojų. Toks procentas yra sąlyginai nedidelis[58], tačiau tokio pobūdžio nusikaltimai labiausiai kelia grėsmę visuomenei ne dėl paplitimo, bet dėl galimos žalos ir padarinių (tai išsamiau aptariama 2.3. poskyryje).

Analizuojamu laikotarpiu daugiausiai užregistruota Lietuvos Respublikos BK 198[1] straipsnyje numatyta nusikalstama veika – neteisėtas prisijungimas prie informacinės sistemos *(žr. 3 diagramą)*[59]. Nagrinėjamu laikotarpiu BK 198[1] str. sudarydavo 74,8 – 89,8 % visų kompiuterinių nusikaltimų (mažiausiai užfiksuota 2021 m., o daugiausiai – 2022 m.) Neteisėtas prisijungimas prie informacinės sistemos nereikalauja tam skirtos išskirtinio pobūdžio technikos, taip pat potencialių taikinių skaičius yra didelis. Tokia nusikalstama veika gali pasireikšti tiek individualaus asmens veiksmais, neretai kylančiais iš buitinių santykių tarp pažįstamų asmenų, tiek organizuotu lygmeniu, kai neteisėtas prisijungimas yra naudojamas pavojingesnėms

[57] Informatikos ir ryšių departamentas, *supra note*, 55.
[58] Autorė pabrėžia, jog pateikti duomenys atspindi kompiuterinių nusikaltimų statistiką tik siaurąja prasme, t.y. tik tas nusikalstamas veikas, kurios įtvirtintos Lietuvos Respublikos BK XXX skyriuje. Jei šio nusikaltimo apibrėžimą vertintume plačiąja prasme, įtraukdami sukčiavimus, duomenų klastojimus ir kt., faktiškai registruotų atvejų skaičius procentaliai būtų žymiai didesnis.
[59] Informatikos ir ryšių departamentas, *op. cit.*

nusikalstamoms veikoms daryti, pavyzdžiui sukčiavimas ar šantažas.[60] Analizuojamu laikotarpiu neteisėto elektroninių duomenų perėmimo ir panaudojimo (BK 198) atvejų užregistruota 12,1 %, neteisėto disponavimo įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis (BK 198[2]) – 3,37 %, o neteisėto poveikio elektroniniams duomenimis (BK 196) užregistruota 2,84 % visų kompiuterinių nusikaltimų. Mažiausiai užregistruota neteisėto poveikio informacinei sistemai atvejų (BK 197) – 0,6 %.

3 diagrama. Lietuvos Respublikos baudžiamojo kodekso 196 - 198[2] straipsniuose numatytų nusikalstamų veikų registruotas skaičius 2020 – 2025 m. laikotarpiu.



Analizuojant Europos Sąjungos kibernetinio saugumo agentūros (toliau – ENISA) ataskaitas[61], matyti, kad Europos Sąjungoje kompiuterinių arba su duomenų panaudojimu susijusių nusikaltimų skaičius ne tik sparčiai didėja, bet ir sudėtingėja – nuo pavienių, mažesnio masto veikų pereinama prie koordinuotų ir sisteminių išpuolių, dažnai nukreiptų į didelės vertės taikinius, tokius kaip viešojo sektoriaus institucijas, finansų įstaigas. Analizuojamu laikotarpiu išryškėja tam tikros vyraujančios kompiuterinių nusikalstamų veikų kryptys. Didžiausią reikšmę įgauna duomenų vagystės, neteisėtas prisijungimas prie informacinių sistemų bei kenkėjiškų programų naudojimas – iš kurių didelė dalis buvo susijusi su paslaugų trikdymo (DDoS) atakomis[62]. Pastebima naujai auganti tendencija – pavogtais duomenimis ne tik pasinaudojama

[60] Vaidas Kalpokas, Renata Marcinauskaitė, „Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas“, *Teisės problemos* 3, 77 (2012): 30 - 52, https://teise.org/wp-content/uploads/2023/01/Kalpokas-Marcin.-TP2012_3.pdf.

[61] European Union Agency for Cybersecurity, „Enisa Threat Landscape reports 2020 – 2025”, ENISA, žiūrėta 2026 m. kovo 26 d., https://www.enisa.europa.eu/.

[62] DDoS ataka – viena dažniausiai pasitaikančių kibernetinių grėsmių, kurių metu robotų serija „atakuoja“ svetaines ar serverius. Puolamas tinklas bandydamas kovoti naudoja savo vidinius išteklius, dėl ko sistema sistema susilpnėja, tampa pažeidžiama duomenų vagystei arba visiškai nustoja veikti.

siekiant asmeninės naudos, o jais pradėta prekiauti nusikalstamose platformose. Tai tik įrodo, jog kompiuteriniai nusikaltimai vis labiau įgauna organizuoto nusikalstamumo bruožų.[63] ENISA ataskaitų analizė taip pat parodo, jog kompiuterinių nusikaltimų būklę ir paplitimą vertinti tarptautiniu mastu yra gan sudėtinga, dėl nevienodų nacionalinių teisinių sistemų ir nevienodų kompiuterinių nusikaltimų kvalifikavimo principų, dėl kurių statistiniai duomenys nėra tiesiogiai palyginami tarpusavyje.

Siekiant išsamiau atsikleisti kompiuterinių nusikaltimų struktūrą ir tendencijas tarptautiniu mastu, tikslinga pasitelkti skirtingus tarptautinės informacijos šaltinius. Vienas jų – JAV Federalinio tyrimo biuro (toliau – FBI) sudarytos metinės ataskaitos[64]. Per pastaruosius metus JAV fiksuojama kibernetinių incidentų augimo tendencija. 2020 m. JAV fiksuota maždaug 790 000 tūkst. kibernetinių incidentų, o 2024 m. – kibernetinių incidentų skaičius išaugo 8,8 % ir padidėjo iki 859 532 tūkst. kibernetinių incidentų. Visgi, per pastaruosius 5 metus kibernetinių nusikaltimų struktūra nesikeitė – daugiausiai užfiksuota fišingo (angl. *phising*) arba kitaip sakant sukčiavimo atvejų, kai apgaulės būdu yra išviliojama asmeninė informacija pavyzdžiui slaptažodžiai ar banko kortelės duomenys. Taip pat, vieni dažniausių nusikaltimų yra ir asmens duomenų neteisėtas atskleidimas (2020 m. fiksuota 45 330 atvejų, o 2024 m. šių nusikaltimų padidėjo 43,1 %). Statistika rodo, jog daugiausiai incidentų ir daugiausiai žalos 2024 m. padaryta sveikatos priežiūros įstaigoms, viešojo administravimo bei kitoms valstybinėms institucijoms, kas kelia susirūpinimą, nes šios institucijos yra itin svarbios valstybės funkcionavimui, o jų veiklos sutrikdymas gali sukelti rimtų pasekmių visuomenės saugumui ir viešajam interesui.

Atsižvelgiant į tai, kas išdėstyta, galima teigti, jog kompiuterinių nusikaltimų paplitimas tiek nacionaliniu, tiek tarptautiniu mastu pasižymi augimo tendencija ir didėjančiu sudėtingumu. Analizuojami duomenys leidžia daryti išvadą, jog šių nusikaltimų struktūroje dominuoja neteisėtas prisijungimas prie informacinių sistemų, neteisėtas duomenų pasisavinimas bei kenkėjiškų programų panaudojimas. Taip pat, nustatyta, kad šios nusikalstamos veikos vis dažniau nukreipiamos į valstybinius, strategiškai svarbius sektorius. Vis dėlto, pažymėtina, jog kompiuterinių nusikaltimų būklę ir paplitimą sunku įvertinti dėl kompiuterinių nusikaltimų latentiškumo bei nevienodo tarpvalstybinio šių veikų apibrėžimo, dėl ko sudėtinga objektyviai palyginti statistinius duomenis.

---

[63] European Union Agency for Cybersecurity, *supra note*, 61.

[64] Federal Bureau of Investigation, *Internet Crime Report 2024* (Washington: FBI, 2025), 4, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

2.2. Kompiuterinių nusikalstamų veikų žala

Kompiuteriniai nusikaltimai gali sukelti įvairaus pobūdžio žalą tiek fiziniams, tiek juridiniams asmenims. Šiame darbe žala suprantama kaip tiesioginis neigiamas tokių nusikalstamų veikų poveikis, pavyzdžiui finansiniai nuostoliai, o padariniai apima platesnes ir ilgalaikes pasekmes, tokias kaip asmens reputacijos pablogėjimas ar visuomenės pasitikėjimo institucijų teikiamomis paslaugomis, sumažėjimas. [65] Vis dėlto, praktikoje šie terminai glaudžiai susiję ir dažnai vartojami kaip sinonimai, todėl nagrinėjant kompiuterinių nusikaltimų žalą kartu bus atskleidžiami ir jų sukeliamai padariniai. Atsižvelgiant į tai, tikslinga išskirti pagrindines kompiuterinių nusikaltimų sukeliamas žalos rūšis.

Finansinė žala. Kompiuteriniai nusikaltimai kasmet padaro didelę finansinę žalą nukentėjusiesiems. Ši nusikalstama veika yra „nelabai rizikinga, didelį pelną duodanti nusikalstama veikla, kuri tampa vis labiau įprasta ir žalinga.“[66] Jungtinėse Amerikos Valstijose kompiuterinių nusikaltimų sukelta finansinė žala išaugo nuo 4,20 mlrd. dolerių 2020 m., iki 16,6 mlrd. dolerių 2024 m.[67] Tokia statistika atspindi tik tiesiogiai sukeltą finansinę žalą, tačiau neapima netiesioginės žalos, kuri susijusi su išlaidomis veiklos atstatymui, sistemų atkūrimui ar saugumo priemonių stiprinimui, dėl to, manoma, jog realioji finansinė žala, kurią sukelia kompiuteriniai nusikaltimai, yra žymiai didesnė. 2019 m. Jungtinių Amerikos Valstijų duomenimis, maždaug 60 % mažų ir vidutinio dydžio įmonių, nukentėjusių nuo kompiuterinių nusikaltimų (plačiąja prasme) yra priverstos uždaryti savo verslą per pusmetį nuo įvykusio incidento.[68]

Kompiuterinės nusikalstamos veikos, pavyzdžiui išpirkos reikalaujančios atakos, gali padaryti ne tik finansinę žalą, bet ir fizinę žalą, ypač kai šių nusikalstamų veikų taikinys yra ypatingos svarbos infrastruktrūra.[69] 2020 m. Vokietijos ligoninė patyrė išpirkos reikalaujančios

---

[65] James Lewis, *Economic Impact of Cybercrime—No Slowing Down Report*, CSIS (Santa Clara: McAfee LLC, 2018), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

[66] Europos Komisija, „Komisijos Komunikatas Tarybai ir Europos Parlamentui „Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su nusikalstamumu centro kūrimas/*COM/2012/0140 final */“, EUR-Lex, https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52012DC0140.

[67] Arianna E. Ortiz ir Rohitha Goonatilake, „Rise of Computer – Related Crimes: Loss of Data, Infrastructures and Monetary Assets“, *European Journal of Applied Sciences* 14, 1 (2026): 482, https://www.researchgate.net/publication/400598389_Rise_of_Computer-Related_Crimes_Loss_of_Data_Infrastructures_and_Monetary_Assets.

[68] Robert Johnson, „60 Percent Of Small Companies Close Within 6 Months Of Being Hacked“, *Cybercrime Magazine*, 2019 m. sausio 2 d., https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.

[69] Karine Bannelier, „Risks and Opportunities of the UN Cybercrime Convention for the UNTOC & The Fight Against Transnational Organized Crime: A First Assessment“, *Transnational Criminal Law Review* 4, 1 (2025): 142, https://www.researchgate.net/publication/394799916_Risks_and_Opportunities_of_the_UN_Cybercrime_Convention_for_the_UNDOC_the_Fight_Against_Transnational_Organised_Crime_A_First_Assessment?_tp=eyJjb250ZXh0IjoiZmFnZSI6ImhvbWUiLCJwYWdlIjoic2VhcmNoIiwicG9zaXRpb24iOiJwYWdlSGVhZGVyIn19.

programinės įrangos ataką, dėl kurios privalėjo laikinai uždaryti ligoninę. Dėl šios situacijos, sunkios būklės pacientas turėjo būti pervežtas į kitą artimiausią ligoninę, o pervežimo metu – mirė.[70] Tai tik parodo, kad jokia šalis ar institucija nėra apsaugota nuo kompiuterinių nusikalstamų veikų, o jų daroma žala kelia grėsmę visiems.

Kompiuterinių nusikaltimų daroma finansinė žala nuosekliai auga ir Lietuvoje. Nors, pastebima, jog tokia žala nėra tiksliai įvertinama, kadangi oficialūs šaltiniai nepateikia vieningos statistikos apie bendrą nuostolių dydį. Nacionalinės kibernetinio saugumo ataskaitos 2023 m. duomenimis iš fizinių ir juridinių asmenų sukčiavimo būdu bandyta pasisavinti 12,5 mln. Eur, o 2024 m. šis skaičius išaugo 28 %. Taip pat, pastebėta, jog 2024 m. didelės žalos incidentų (kai suma viršija 10 000 Eur) padaugėjo 36 % lyginant su 2023 m. - šis rodiklis daugiau nei 2 kartus viršija tokių sukčiavimo atvejų per 2020 – 2023 m. vidurkį.[71] Nors sukčiavimas yra tik dalis kompiuterinių nusikaltimų kalbant plačiąja prasme, tačiau tai tik parodo, jog elektroniniai nusikaltimai daro didelę finansinę žalą tiek fiziniams, tiek juridiniams asmenims.

Asmens duomenų saugumo pažeidimai. Analizuojant kompiuterinių nusikaltimų daromą žalą, asmens duomenų saugumo pažeidimai pasižymi išskirtiniu pavojingumu, kadangi gauti neteisėti duomenys gali būti naudojami pakartotinai, darant naujas nusikalstamas veikas, pavyzdžiui, sukčiavimas ar šantažas elektroninėje erdvėje. JAV duomenimis, fiksuojamas iš esmės nekintantis (arba nežymiai didėjantis) kasmetinis asmens duomenų apsaugos pažeidimų skaičius.[72] 2022 – 2024 m. laikotarpyje kasmet užfiksuota apie 60 000 tūkst. skundų dėl asmens duomenų pažeidimo atvejų – kasmet tai sudaro apie 1 mlrd. dolerių finansinės žalos. Tuo tarpu Lietuvoje, pastaraisiais metais matoma asmens duomenų saugumo pažeidimų mažėjimo tendencija, kadangi pažeidimų skaičius kasmet vis mažėja. Valstybinės duomenų apsaugos inspekcijos duomenimis,[73] 2025 m. Lietuvoje gauti 223 pranešimai dėl asmens duomenų saugumo pažeidimo, tai 18 % mažiau nei gauta pranešimų 2024 m. (273 pranešimai). Asmens duomenų pažeidimai kelia grėsmę tiek fiziniam asmeniui, kai jautri informacija tampa prieinama pašaliniams asmenims, tiek juridiniams asmenims – mažėja klientų pasitikėjimas, tenka naudoti papildomus resursus duomenų apsaugai, dėl ko juridinis asmuo patiria papildomus finansinius nuostolius.

Institucijų veiklos sutrikdymas ir reputacinė žala. Institucijos ir įstaigos saugo bei naudoja reikšmingą ir konfidencialią informaciją, įskaitant asmens duomenis, vidaus dokumentus ir net su nacionaliniu saugumu susijusią informaciją. Taip pat, teikiant viešąsias paslaugas institucijoms

---

[70] Alex Scroxton, „German authorities probe ransomware hospital death“, *Computer Weekly News,* 2020 m. rugsėjo 18 d., https://www.computerweekly.com/news/252489247/German-authorities-probe-ransomware-hospital-death.
[71] Lietuvos Respublikos Krašto apsaugos ministerija, *Nacionalinė kibernetinio saugumo ataskaita* 2024, (Lietuva: 2025), 64, https://kam.lt/wp-content/uploads/2025/07/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf.
[72] Federal Bureau of Investigation, *supra note*, 64: 18.
[73] „Asmens duomenų saugumo pažeidimai Lietuvoje 2025 m.“, *Valstybinė duomenų apsaugos inspekcija*, 2026 m. vasario 12 d., https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2025-m-lfX/.

yra svarbu užtikrinti svarbų ir nepertraukiamą darbą. Sutrikus sistemų veiklai gali būti apribotas ar visiškai sustabdytas paslaugų teikimas, pažeistiems duomenims iškyla rizika, jog duomenys bus neteisėtai sunaikinti arba nutekinti, todėl institucijų vadovai, susidūrę su pažeidimais, vis dažniau atkreipia dėmesį į sistemų saugumo stiprinimą. Visgi, institucijų vadovai teigia, jog nėra paprasta atkurti pažeistas sistemas, o tuo pačiu – atkurti klientų pasitikėjimo lygį, dažniausiai visiškas sistemų ir pasitikėjimo atkūrimas užtrukdavo ilgiau nei 100 dienų.[74] Tai parodo, jog kompiuterinių nusikaltimų padariniai yra ilgalaikis procesas, kurio metu bandant atstatyti patirtą žalą, institucijose sumažėja klientų paslaugų naudojimas (mažėja pelnas), papildomai investuojama į saugumo stiprinimo priemones (papildomos išlaidos). Ypatingą žalą institucijoms daro išpirkos reikalaujančios programos, ypač nukreiptos į svarbias valstybines institucijas, pavyzdžiui medicinos įstaigas. Sutrikdant įstaigos veiklą, vėluoja procedūros, sutrikdoma pacientų priežiūra, dėl ko tam tikrais atvejais institucijoms yra geriau susimokėti išpirką, kad galėtų tęsti savo veiklą, nei patirti užsitęsusių darbuotojų prastovų ir sistemų atkūrimo nuostolius, klientų praradimą ir nepasitikėjimą.[75] 2025 m. JAV atliktame tyrime, kuriame buvo apklausti 3470 institucijų vadovai, net 49 % vadovų patvirtino, jog sutrikus jų sistemoms dėl patirto kibernetinio incidento ar atakos, jie ketina papildomai investuoti pinigų į saugumą – daugiausiai į grėsmių aptikimo ir reagavimo technologijas (43 %), duomenų saugumo įrankius (37 %) , reagavimo į incidentus testavimą (35 %) bei darbuotojų mokymus (33 %). 2024 m. Europolo internetu organizuojamo nusikalstamumo grėsmių vertinimo ataskaitos (angl. – *Internet Organised Crime Threat Assessment*) duomenimis, daugiausiai kenkiama (ypatingai užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusais) smulkaus ir vidutinio verslo įmonėms, kadangi jos turi prasčiausiai išvystytą apsaugos sistemą.[76] Lietuvoje, fiksuojami atvejai, kai kibernetiniai nusikaltimai nukreipiami ir į valstybines institucijas, pavyzdžiui, 2024 m. pirmą kartą nusikaltėliai kenkėjiškus virusus panaudojo prieš finansų sektorių – įmonę atakavo „kombinuota elektroninių duomenų grobimo ir užšifravimo ataka“[77], dėl ko sutriko bankininkystės sistema, žmonės negalėjo disponuoti savo lėšomis, o tai lėmė, jog žmonės pasirinkdavo kitus, saugesnius bankus, kur saugoti savo pinigus.

---

[74] IBM, *Cost of a Data Breach Report 2025: The AI Oversight Gap* (JAV: IBM, 2025) 22, https://www.ibm.com/forms/mkt-53830.

[75] Budi Wibowo, Luqman Hafiz ir Taufik Hidayat, „Unveiling the Cybercrime Ecosystem: Impact of Ransomware – as – a – Service (RaaS) in Indonesia“, *International Journal of Science Education and Cultural Studies* 4, 1 (2025): 17, https://www.researchgate.net/publication/389501930_Unveiling_the_Cybercrime_Ecosystem_Impact_of_Ransomware-as-a-Service_RaaS_in_Indonesia.

[76] Europol, *Internet Organised Crime Threat Assessment 2025* (Luxembourg: Publications Office of the European Union, 2025), 13 – 15, https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.

[77] Krašto apsaugos ministerija, *supra note*, 71: 58.

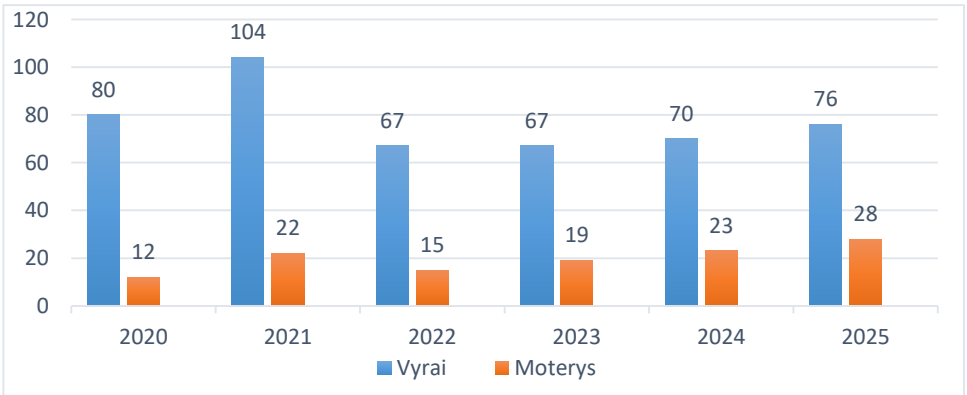
Apibendrinant galima teigti, jog kompiuterinių nusikaltimų daroma žala pasižymi kompleksiškumu, apimančiu tiek finansinius nuostolius, tiek asmens duomenų saugumo pažeidimus, institucijų veiklos sutrikdymą bei reputacinę žalą. Analizuoti duomenys rodo, jog šių nusikalstamų veikų poveikis yra ilgalaikis ir neapsiriboja tik vienkartiniais padariniais, o daugeliu atveju padariniai nėra lengvai išmatuojami ir paskaičiuojami, todėl realus kompiuterinių nusikaltimų daromos žalos mastas yra ženkliai didesnis nei rodo statistiniai duomenys. Taigi, kompiuteriniai nusikaltimai gali sukelti ne tik individualių pavienių nuostolių, bet ir turėti platesnį poveikį institucijų stabilumui, visuomenės pasitikėjimui bei valstybės saugumui.

3. NUSIKALTĖLIO CHARAKTERISTIKA IR JO RYŠYS SU AUKA

Analizuojant kompiuterinius nusikaltimus, svarbu įvertinti ne tik jų raišką, bet ir nusikaltėlio charakteristiką bei jo ryšį su auka, kadangi tai leidžia suprasti, kokie asmenys gali būti linkę daryti tokio pobūdžio nusikalstamas veikas, kokie jų motyvai. Tai ypač aktualu kompiuterinių nusikaltimų kontekste, kur nusikaltėliai dažnai veikia anonimiškai, nebendraudami su auka tiesioginio, fizinio kontakto būdu. Kompiuterinių nusikaltimų kontekste nusikaltėlio charakteristikos nustatymas dažniausiai yra grindžiamas oficialiosios statistikos duomenimis, dėl to, šiame skyriuje analizuojami BK XXX skyriaus padarytų nusikalstamų veikų, 2020 – 2025 m. laikotarpio įtariami (kaltinami) bei nukentėję asmenys pagal kelis kriterijus – lytį, amžių, išsilavinimą ir užimtumą.

Mokslinėje literatūroje pažymima, kad vyrai dažniau nei moterys įsitraukia į kibernetinį deviantį elgesį ir yra labiau linkę veikti kaip kompiuterinių nusikaltimų vykdytojai – tai siejama su įvairiais socialiniais, technologiniais ir psichologiniais veiksniais.[78] Vis dėlto, siekiant pagrįsti šias prielaidas oficialiosios statistikos duomenimis, išnagrinėti Lietuvoje įtariamų (kaltinamų) asmenų pagal BK XXX skyriaus nusikalstamų veikų pasiskirstymą pagal lytį 2020 – 2025 m. laikotarpiu *(žr. 4 diagramą)*[79]. Nagrinėjamu laikotarpiu didžiąją dalį nusikalstamas veikas padariusių asmenų sudarė vyrai. 2020 m. vyrai sudarė 87 %, o 2025 m. – 73,1 % visų įtariamų (kaltinamų) asmenų.

4 diagrama. Įtariamų (kaltinamų) asmenų, dėl BK XXX skyriaus nusikalstamų veikų, pasiskirstymas pagal lytį 2020 - 2025 m. laikotarpiu



Nors nagrinėjamu laikotarpiu vyrai padaro daugiau kompiuterinių nusikaltimų (bendrai vyrų dalis sudaro 79,6 %), moterų dalis tuo pačiu laikotarpiu augo – 2020 m. moterys sudarė 13 %, o 2025

[78] Li Li ir kt., „Do Men Have More Cyber- Deviant Behaviours? A Network Analysis Based on the Reciprocal Determinism Model“, *Deviant Behaviour* (2025): 2 - 3, https://www.tandfonline.com/doi/full/10.1080/01639625.2025.2562117?scroll=top&needAccess=true#d1e940.
[79] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.

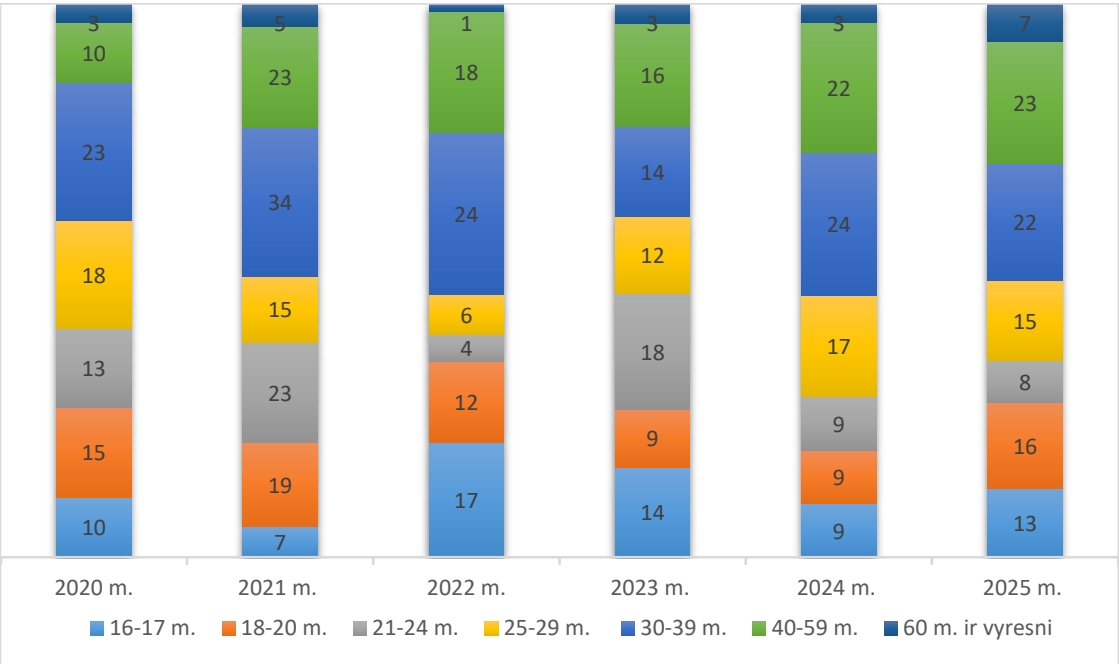
m. – 26,9 %. Tokie rezultatai gali būti siejami su vyrų didesniu įsitraukimu į technologijų sritį ir didesniu polinkiu rizikuoti, tačiau pastebima, kad kompiuteriniai nusikaltimai palaipsniui tampa mažiau būdingi vienai lyčiai ir galima daryti prielaidą, kad ilgainiui skirtumas tarp vyrų ir moterų gali mažėti.

Nagrinėjant kompiuterinius nusikaltimus darančių asmenų charakteristiką, svarbu analizuoti ir amžiaus kategorijas, kadangi skirtingos amžiaus grupės pasižymi nevienodu informacinių technologijų naudojimu bei nusikalstamų veikų darymu. Tarptautinių tyrimų 2025 m. rezultatais, net 82 % jaunimo (nuo 15 m. iki 24 m.) visame pasaulyje naudojasi internetu[80], tai lėmė ir padidėjusį jaunų asmenų įsitraukimą į neteisėtas veiklas internetinėje erdvėje.[81] Tokios veiklos internetinėje erdvėje jaunimo tarpe dažniausiai pasireiškia kaip paprastesnės, deviantinio elgesio formos (elektroninės patyčios, mažo pavojingumo neteisėtas turinio naudojimas ir kt.), o ne nusikalstamos veikos. Jaunesnio amžiaus asmenų įsitraukimas į neteisėtas veikas internetinėje erdvėje dažnai siejamas su smalsumu, noru eksperimentuoti bei siekiu išbandyti informacinių technologijų galimybes[82], todėl jų veiksmai dažniausiai neperžengia baudžiamosios teisės taikymo ribų.

Lietuvoje 2020 – 2025 m. laikotarpiu, daugiausiai kompiuterinių nusikaltimų padarė vidutinio amžiaus asmenys (žr. 5 diagramą)[83]. Didžiausią dalį sudaro 30 – 39 m. amžiaus grupė, kuri atskirai kiekvienais metais sudaro 16,3 – 29,3 % visų įtariamų (kaltinamų) asmenų (vidutiniškai 24,1 %). Reikšmingą dalį sudaro 25-29 m. amžiaus grupė – apie 7,3 – 21,95 % visų įtariamų (kaltinamų) asmenų (vidutiniškai 19,7 %) ir 40 – 59 m. amžiaus asmenys, kurių dalis sudaro 10,8 – 23,6 % kasmet visų įtariamų (kaltinamų) asmenų (vidutiniškai 19,2 %). Jaunesnių nei 18 m. ir vyresnių nei 60 m. amžiaus grupės sudaro itin mažą procentinę dalį.

[80] „Internet use remains highest among youth, yet the generational gap is shrinking“, International Telecommunication Union, žiūrėta 2026 m. balandžio 23 d., https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-youth-internet-use/.
[81] Mary Aiken, Julia Davidson ir Philip Amann, *Youth Pathways into Cybercrime* (Haga: 2016), 2 - 4, https://www.europol.europa.eu/cms/sites/default/files/documents/pathways-white-paper.pdf.
[82] *Ibid.,* 13.
[83] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.

5 diagrama. Įtariamų (kaltinamų) asmenų, dėl LR BK XXX skyriaus nusikalstamų veikų, pasiskirstymas pagal amžių 2020 - 2025 m. laikotarpiu



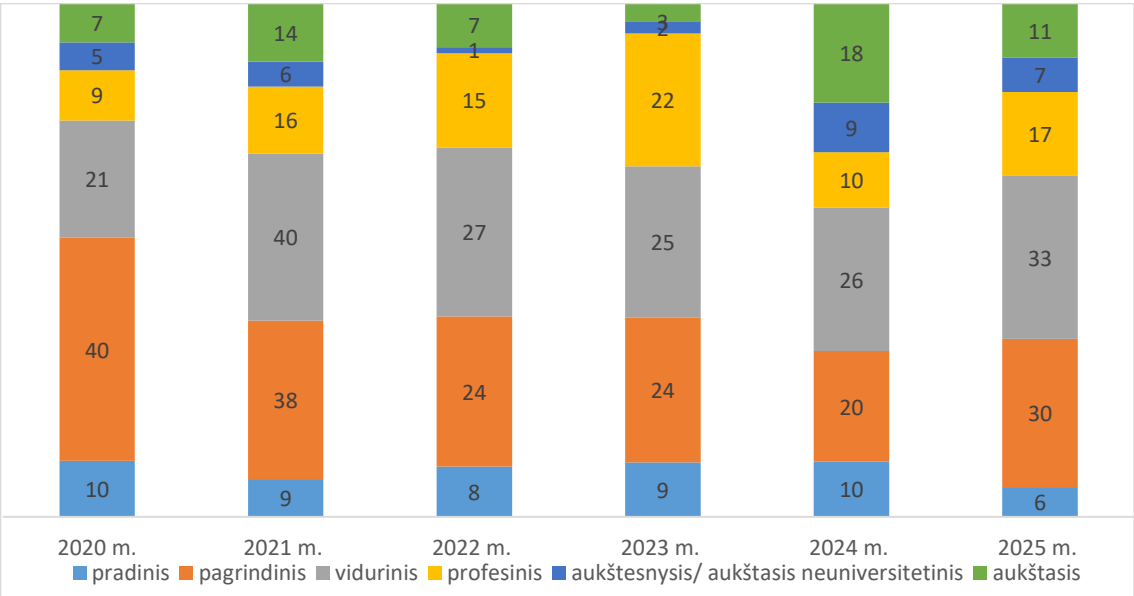
Jaunesnio amžiaus asmenys dažniau susitelkia į įvairius neteisėtus įsilaužimus (nagrinėjamu laikotarpiu nepilnamečiai asmenys daugiausiai padarė BK 198[1] str. nusikalstamų veikų) ar kitus mažesnio pavojingumo veiksmus, kurie, kaip minėta, dažnai neperžengia baudžiamosios atsakomybės ribų, o vyresnio amžiaus žmonės labiau linksta į finansiškai naudingą nusikalstamą veiką, kuri reikalauja didesnio planavimo ir techninių įgūdžių.[84] Tai, kad didžiausią dalį įtariamų (kaltinamų) asmenų sudaro 30 – 39 m. amžiaus asmenys, yra siejama su keliomis tarpusavyje susijusiomis aplinkybėmis. Pirmiausia, tokio amžiaus asmenys dažniau pasižymi gyvenimiška patirtimi ir gebėjimu planuoti veiksmus, neveikia impulsyviai ir yra labiau orientuoti į konkretų rezultatą (dažnu atveju finansinę naudą). Ilgametė patirtis leidžia nusikaltėliui veikti profesionaliai, užmaskuoti savo veiksmus – šie bruožai būdingi kompiuterinius nusikaltimus darančiam asmeniui.[85] Taip pat, šio amžiaus asmenys dažniausiai aktyviai dalyvauja darbo rinkoje, dėl to turi galimybę naudotis informacinėmis sistemomis, įvairiomis programomis, o taip pat turi prieigą prie tam tikrų duomenų ar vidinės informacijos – tai sudaro palankesnes sąlygas daryti kompiuterinius nusikaltimus.

Kompiuterinius nusikaltimus darantys asmenys dažnai siejami su aukštais informacinių technologijų gebėjimais ir žiniomis, todėl svarbu analizuoti kokį išsilavinimą turi šias

[84] Anamarija Pogorelec, „The people behind cyber extortion are often in their forties“, *Help Net Security*, 2026 m. kovo 10 d., https://www.helpnetsecurity.com/2026/03/10/cyber-extortion-cybercrime-age-profile/.
[85] Lietuvos Respublikos prokuratūra, *Lietuvos Respublikos prokuratūros veiklos 2023 metais ataskaita* (Lietuva: 2024), 15 – 16, https://www.prokuraturos.lt/data/public/uploads/2024/03/2023-m.-ataskaita-galutine.pdf.

nusikalstamas veikas darantys asmenys. Oficialiosios statistikos Lietuvoje duomenys rodo, kad nagrinėjamu laikotarpiu nuo 2020 m. iki 2025 m., didžiausią dalį įtariamų (kaltinamų) asmenų, padariusių kompiuterinį nusikaltimą, sudaro asmenys, turintys pagrindinį ir vidurinį išsilavinimą *(žr. 6 diagramą)*[86]. Pavyzdžiui, pagrindinį išsilavinimą turinčių asmenų dalis nagrinėjamu laikotarpiu sudaro 30,2 % vertinant visas išsilavinimo kategorijas. Tuo tarpu vidurinio išsilavinimo duomenys yra labai panašūs, fiksuojama, jog vidurinį išsilavinimą turintys asmenys nagrinėjamu laikotarpiu sudaro 29,4 %.

6 diagrama. Įtariamų (kaltinamų) asmenų, dėl LR BK 196 - 198[2] str. nusikalstamų veikų, pasiskirstymas, pagal išsilavinimą 2020 - 2025 m. laikotarpiu



Tuo tarpu, profesinį išsilavinimą turinčių asmenų skaičius yra mažesnis, kasmet neviršijantis 25 % ribos. Kiek mažesnę dalį kasmet sudaro asmenys, turintys tik pradinį išsilavinimą 5,7 % - 11 %, aukštąjį išsilavinimą turinčių asmenų skaičius kasmet sudaro 3,5 % - 10 %, o aukštesnįjį ar aukštąjį neuniversitetinį išsilavinimą sudaro 1,21 % - 10 %.

Tokia oficialioji statistika pagal išsilavinimo kriterijų sudaro prielaidą, jog kompiuterinių nusikaltimų vykdymui reikalingi įgūdžiai ir žinios dažnai įgyjamos ne formaliojo švietimo sistemose, o savarankiškai. Šiuolaikinėje skaitmeninėje erdvėje egzistuoja daug šaltinių ir viešai prieinamų erdvių (forumų, grupių), kuriose galima savarankiškai įgyti reikiamų žinių. Tokią prielaidą patvirtina ir Nacionalinė nusikaltimų agentūra (angl. – *National Crime Agency*), 2017 m. Jungtinėje Karalystėje atlikusi tyrimą[87], kurio metu buvo atliktos apklausos asmenų, dalyvavusių

[86] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.
[87] National Crime Agency, *Pathways Into Cyber Crime* (Jungtinė Karalystė: 2017), https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file.

kompiuteriniuose nusikaltimuose. Beveik visi apklausti asmenys nurodė, kad reikiamą informaciją norint daryti kompiuterinius nusikaltimus išmoko naršydami internete, o būtent - įsilaužimo mokančiuose forumuose (angl. – *Hackforums).*[88] Taip pat, apklausti asmenys pabrėžė, kad dažniausiai tokiuose forumuose pradėjo lankytis ir domėtis neteisėta veikla, dėl smalsumo, norėdami išplėsti savo žinias ar kažkam pajuokaujant pakenkti sutrikdant sistemų veiklą.[89] Tai leidžia daryti išvadą, kad kompiuterinių nusikaltimų kontekste didesnę reikšmę turi savarankiškai įgytos žinios ir informacija, o ne formalus išsilavinimas.

Analizuojant įtariamų (kaltinamų) asmenų pasiskirstymą Lietuvoje pagal užimtumą *(žr. 2 lentelę)*[90] matyti, kad 2020 – 2025 m. laikotarpiu didžiausią dalį sudaro nedirbantys ir bedarbiai asmenys – 34 %. Tuo tarpu dirbančių asmenų dalis yra mažesnė ir pasiskirsto tarp įvairių sektorių – daugiausiai nevalstybinių įstaigų ar įmonių darbuotojų (9,7 – 26,3 % kasmet). Besimokančių asmenų, t.y. mokinių ir studentų dalis sudaro 6,4 – 15,3 % kasmet, tačiau į besimokančių asmenų sąvoką įeina bendrojo lavinimo, profesinės mokyklos, aukštesniosios kolegijos, aukštosios ar kitos mokymosi įstaigos moksleiviai ir studentai.

[88] National Crime Agency, *supra note*, 87: 18.
[89] *Ibid.*, 11 – 18.
[90] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.

2 lentelė. Įtariamų (kaltinamų) asmenų, dėl LR BK XXX skyriaus nusikalstamų veikų, pasiskirstymas, pagal užimtumą 2020 - 2025 m. laikotarpiu

	2020 m.	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.
Užimtumas						
Dirba valstybės ar savivaldybės įstaigoje ar įmonėje		2		1	2	4
Pareigūnas: policijos						
Prokuratūros						
Valstybės saugumo departamento						
Valstybės sienos apsaugos tarnybos						
LR muitinės						
Finansinių nusikaltimų tyrimo tarnybos						
Priešgaisrinės apsaugos ir gelbėjimo departamento						
Specialiųjų tyrimų tarnybos						
LR Krašto apsaugos ministerijos						
Kalėjimų departamento						
Kitos valstybinės institucijos ar įmonės pareigūnas		1				
Valstybės tarnautojas						
Švietimo sistemos darbuotojas						
Nevalstybinėje įstaigoje ar įmonėje	9	17	14	15	24	24
Kita						
Mokosi: mokykloje						
Bendro lavinimo	3	5	12	9	7	5
Profesinėje	3	2	6			1
Aukštesniojoje/ kolegijoje	1			1	5	
Aukštojoje					1	
Kitoje mokymosi įstaigoje	5	1	1	1	1	4
Kita:						
Bedarbis	5	11	3	7	13	9
Nedirbantis	25	31	24	22	21	27
Neįgalus		1	2			1
Pensininkas	1	3		3	2	4
Nesimokantis			1			
Elgetaujantis				1		
Įkalintas laisvės atėmimo įstaigoje	19	18	3		2	4
Karys		1				1
Kita	21	33	16	26	15	20

Pastebėta, jog įkalintų laisvės atėmimo vietoje asmenų skaičius 2020 – 2025 m. laikotarpiu sumažėjo: 2020 m. fiksuota 19 asmenų, o 2025 m. tik 4 asmenys. Kitos užimtumo kategorijos, tokios kaip pensininkai, kariai ar kiti specifiniai statusai, nagrinėjamu laikotarpiu sudaro itin mažą dalį.

Šie duomenys leidžia daryti prielaidą, kad kompiuterinius nusikaltimus dažniausiai atlieka oficialiai nedirbantys asmenys, kurie gali turėti finansinių sunkumų ir didesnį norą užsidirbti ir dirbantys nevalstybinėse įstaigose ar įmonėse asmenys, turintys prieigą prie įvairių sistemų ar vidinės informacijos.

Analizuojant nusikaltėlio ir aukos ryšį, ypač reikšmingi duomenys yra ar nusikaltėlis buvo pažįstamas nukentėjusiajam. Mokslinėje literatūroje pažymima, jog kompiuterinių nusikaltimų nusikaltėlis savo auką pasirenka veikiamas šioms aplinkybėms – motyvacija, galimybėmis ir prasta apsauga.[91] Tai rodo, jog nusikaltėlis ruošiasi nusikaltimui motyvuotas konkrečiam tikslui – tai gali būti, pavyzdžiui, finansinė nauda ar noras išbandyti savo sugebėjimus. Kai nusikaltėlis turi konkretų tikslą, tuomet jis gali pasirinkti auką – ją renkasi atsitiktinai, dažniausiai asmeniškai jos nepažinodamas, tačiau atsižvelgdamas į esamas galimybes pasiekti auką – per socialinius tinklus ar kitas platformas. Galiausiai – nusikaltėlis atsižvelgia į aukos apsaugą, kuri pasireiškia tiek techninių saugumo priemonių trūkumu, tiek nepakankamu asmens budrumu. Šių trijų veiksnių visuma sudaro palankias sąlygas kompiuterinio nusikaltimo įvykdymui. Taigi, kompiuterinių nusikaltimų atveju nusikaltėlis savo auką pasirenka dažniausiai jos nepažinodamas, o atsižvelgdamas į esamas galimybes ir sistemų pažeidžiamumo aplinkybes bei asmeninius sugebėjimus ir tikslus. Todėl dauguma aukų net nesupranta, kodėl tapo nusikaltėlio taikiniu, dėl to aukos dažniau mano, kad joms tiesiog nepasisekė.[92] Pažengę nusikaltėliai dažnai naudoja socialinės inžinerijos metodus, kurie leidžia sukurti netikrą, trumpalaikį ryšį su auka (susirašinėjimai el. laiškais, trumposiomis žinutėmis ar skambučiai). Veikdami įtikinėjimo modeliu (paprastumas, susidomėjimas, prieštaravimas, pasitikėjimas, empatija)[93], nusikaltėliai įtikina žmones atskleisti asmens duomenis ar kitą naudingą informaciją.

Lietuvoje 2020 – 2025 m. laikotarpiu, daugiausiai nukentėjusiųjų nuo kompiuterinių nusikalstamų veikų, nukenčia nuo nepažįstamų asmenų – ši kategorija sudaro 49,5 % visų atvejų (*žr. 3 lentelę*)[94]. Reikšmingą dalį sudaro ir kategorija „kita“ (46,4 %), kuri apima detaliau neidentifikuotus ar į standartines santykių kategorijas nepatenkančius ryšius tarp nukentėjusiojo ir nusikalstamą veiką padariusio asmens. Mažiau nei 5 % aukų pažinojo asmenį nuo kurio neteisėtų veiksmų nukentėjo.

---

[91] Eric Rutger Leukfeldt ir Majid Yar, „Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis“, *Deviant Behavior* 37, 3 (2016): 3 – 4, https://www.researchgate.net/publication/286923434_Applying_Routine_Activity_Theory_to_Cybercrime_A_Theoretical_and_Empirical_Analysis.

[92] „Understanding the cyber crime and fraud victim journey“, Jungtinės Karalystės Vyriausybė, žiūrėta 2026 m. balandžio 28 d., https://www.gov.uk/government/publications/understanding-the-cyber-crime-and-fraud-victim-journey/understanding-the-cyber-crime-and-fraud-victim-journey.

[93] Al - Nafisa Shaden Ali ir Yahya Moubarak Khatabeh, „Social Engineering as an Intermediate Variable between Methods of Persuasion and Electronic Deception from the Point of View of Victims of Cybercrime, *Journal of Posthumanism* 5, 6 (2025): 1015 – 1016, https://www.researchgate.net/publication/392222941_Social_Engineering_as_an_Intermediate_Variable_between_Methods_of_Persuasion_and_Electronic_Deception_from_the_Point_of_View_of_Victims_of_Cybercrime.

[94] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.

3 lentelė. Nukentėjusių asmenų nuo LR BK XXX skyriaus nusikalstamų veikų, pasiskirstymas, pagal ryšį su nusikalstamą veiką padariusiu asmeniu 2020 - 2025 m. laikotarpiu.

	2020 m.	**2021 m.**	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**
Asmuo nukentėjo nuo:						
Sutuoktinio	2	2		1		
Sugyventinio	1			1		1
Buvusio sugyventinio	2	1				
Sūnaus				1		
Dukters				1		
Įsūnio			1			
Brolio				1		
Giminaičio	1	1		1		
Pažįstamo	2	9	1	6	2	4
Nepažįstamo	67	125	101	82	94	94
Darbdavio			1			2
Kita	172	200	73	30	161	28

Taip pat, nagrinėjamu laikotarpiu matyti, jog dažniausiai nuo kompiuterinių nusikaltimų nukenčia fiziniai asmenys (92 %), kadangi nukentėjusių juridiniai asmenys nagrinėjamu laikotarpiu sudaro 8 % visų aukų (*žr. 1 priedą*)[95]. Nacionalinio kibernetinio saugumo centro (toliau – NKSC) duomenimis[96], 2024 m. Valstybinė duomenų apsaugos inspekcija gavo net 273 pranešimus (7 % daugiau nei 2023 m.) apie asmens duomenų saugumo pažeidimus, kurie, kaip vėliau nustatyta, „33 % įvyko dėl kibernetinių nusikaltimų (duomenų užšifravimo ir išpirkos reikalaujančių atakų, neteisėtai gautos prieigos prie IT sistemų ir kt.).“[97] Didžioji dalis incidentų buvo nukreipta į juridinius asmenis, tačiau jų taikomos apsaugos priemonės dažnai padeda išvengti nuostolių, todėl tokie atvejai ne visada atsispindi oficialiojoje statistikoje.

Kompiuterinių nusikalstamų veikų aukomis dažniau tampa moterys – 57 % *(žr. priedą Nr. 2)*[98], o vertinant pagal amžių – didžiausią dalį sudaro 40 – 59 m. (42 %) asmenys *(žr. priedą Nr. 3)*[99]. Tokio amžiaus asmenys neretai pasižymi žemesniais skaitmeniniais įgūdžiais (lyginant su

[95] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.
[96] Krašto apsaugos ministerija, *supra note,* 71: 12.
[97] *Ibid.*
[98] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.
[99] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.

jaunesniais žmonėmis), dėl to gali sunkiau atpažinti įvairias grėsmes internetinėje erdvėje. Nuo kompiuterinių nusikalstamų veikų daugiausiai nukenčia aukštąjį išsilavinimą turintys asmenys *(žr. 4 priedą)*[100]

Apibendrinant galima teigti, kad kompiuterinius nusikaltimus darančių asmenų ir jų aukų charakteristikos reikšmingai skiriasi, o tai rodo, jog tokių nusikaltimų atveju nusikaltėlio ir aukos ryšys dažniausiai nėra grindžiamas asmeniniais ar socialiniais ryšiais. Kompiuterinių nusikaltimų aukomis dažnu atveju tampama dėl jų neatsargaus elgesio elektroninėje erdvėje ir techninių saugumo priemonių trūkumo, kadangi kompiuterinius nusikaltimus darantis asmuo veikia nuotoliniu būdu, neturėdamas tiesioginio fizinio kontakto su auka.

[100] Pagal užsakymą paruošti duomenys iš IRD prie LR VRM.

4. KOMPIUTERINIŲ NUSIKALSTAMŲ VEIKŲ VEIKSNIAI

Mokslinėje literatūroje pažymima, jog „dauguma individų nėra linkę nusikalsti, nors tam yra palankios sąlygos“[101], tai parodo, jog vien tik palankių aplinkybių buvimas nėra pakankama sąlyga atsirasti nusikalstamam elgesiui. Kriminologiniu požiūriu, asmens norą nusikalsti lemia tiek vidinės (savikontrolė, vertybės, moralė ir kt.), tiek išorinės (teisės, socialinės normos ir kt.) kontrolės elementai.[102] Kiekviena nusikalstama veika pasižymi nevienodais atsiradimo ir plitimo mechanizmais, todėl konkrečią nusikalstamą veiką lemiantys veiksniai taip pat gali skirtis. Ši aplinkybė ypač aktuali analizuojant kompiuterinius nusikaltimus, kurie dėl savo specifikos išsiskiria iš tradicinių nusikalstamų veikų.

Vienas svarbiausių kompiuterinius nusikaltimus skatinančių veiksnių laikytinas informacinių technologijų veiksnys, kuris apima informacinių technologijų naudojimo mastą ir prieinamumą bei sudaromas galimybes nusikalstamos veikoms atsirasti ir plisti. Per pastarąjį dešimtmetį informacinės technologijos priemonės sparčiai įsitvirtino kasdieniame gyvenime, populiarėjo socialiniai tinklai, todėl didelė dalis žmonių komunikavimo ir kitų veiklų vyksta skaitmeninėje erdvėje.[103] Jau 2023 m. pradžioje Lietuvoje visos gamybos ir paslaugų įmonės (kuriose dirbo 10 ar daugiau darbuotojų) naudojosi kompiuteriais ir internetu, iš kurių net 76,5 % turėjo internetinę svetainę, o 38,4 % įmonių turėjo įsigiję debesų kompiuterijos paslaugas.[104] Debesų kompiuterijos paslaugos leidžia saugoti ir valdyti duomenis nuotoliniuose serveriuose, todėl saugoma informacija gali būti pasiekiama iš bet kurios vietos. Nors tokios paslaugos teikėjai teigia, kad tokie duomenys išliks saugūs, tačiau pastebima, kad vis dažniau pasitaiko debesijos paslaugų pažeidimų. 2025 m. duomenimis, priešiškų šalių programišiai, pavyzdžiui, su Rusija siejama grupuotė APT29 geba įsilaužti į prastai apsaugotas debesijos paslaugų paskyras, taip įgydami ilgalaikę prieigą prie svetimų duomenų.[105] 2024 m. Lietuvoje įvyko duomenų nutekinimo incidentas, kai programišiai įsilaužė į „IGNITIS ON“ sistemą ir nutekino 20 tūkst. klientų duomenų, kuriuos vėliau pradėjo viešinti socialiniame tinkle „Telegram“. „IGNITIS ON“ vėliau savo internetiniame puslapyje pareiškė, kad programišiai gavo neteisėtą prieigą prie duomenų,

---

[101] Babacginaitė ir kt., *supra note,* 51: 175.
[102] *Ibid.*
[103] Maryja Šupa, „Socialiniai tyrimai apie elektroninius nusikaltimus: globalus temų diapazonas ir Lietuvoje atliktų tyrimų sisteminė analizė“, *Kriminologijos studijos* 9 (2021): 12 – 13, https://www.zurnalai.vu.lt/kriminologijos-studijos/lt/article/view/24959/24255.
[104] Lietuvos Respublikos Krašto apsaugos ministerija, *Nacionalinė kibernetinio saugumo būklės ataskaita 2020* (Lietuva: 2021), 64, https://kam.lt/wp-content/uploads/2022/02/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf.
[105] Lietuvos Respublikos valstybės saugumo departamentas, *Grėsmių nacionaliniam saugumui vertinimas 2025* (Vilnius: 2025), 48, https://kam.lt/wp-content/uploads/2025/03/2025-GR-LT-02-21-El-be-uzraso_.pdf.

kurie buvo saugomi debesyje.[106] Taigi, nors vis didesnis įmonių naudojimasis internetinėmis svetainėmis, debesų kompiuterijos paslaugomis, palengvina įmonių veiklą ir duomenų saugojimą, tačiau tuo pačiu tai tampa vis patrauklesniu taikiniu nusikalstamoms veikoms atlikti.

Kompiuterinius nusikaltimus darantys asmenys, dažnai naudoja kito asmens duomenis arba naudoja technines priemones, kurios leidžia paslėpti savo tapatybę ir buvimo vietą. Naudodami virtualius privačius tinklus (toliau – VPN) ar atviro kodo programinį tinklą (toliau – TOR), nusikaltėliai gali užšifruoti visus identifikavimo metodus – IP adresą, turinį ir naudotojo duomenis.[107] Kitas anonimiškumą užtikrinantis būdas yra dirbtinio intelekto naudojimas. Nusikaltėliai dirbtinio intelekto pagalba, kuria kenkėjiškas programas (kurias valdo ne pats nusikaltėlis, o dirbtinis intelektas), kurios išmokytos apeiti įprastas apsaugos sistemas. Veikdamas pagal nustatytus algoritmus, dirbtinis intelektas prisitaiko prie konkrečios situacijos, t.y. sukuria sukčiavimui ir duomenų pasisavinimui skirtus el. laiškus, imituoja realius pokalbius ar susirašinėjimus su žmonėmis.[108]

Kompiuterinių nusikaltimų paplitimą skatina ir interneto vartotojų nepakankamas dėmesys saugumui. Per pastaruosius metus pasaulyje ir Lietuvoje smarkiai išaugęs nutekintų duomenų kiekis siejamas su vartotojų naudojamais silpnais, lengvai atspėjamais ar pasikartojančiais slaptažodžiais, kurie naudojami keliose paskyrose,[109] taip pat dažnai asmenys slaptažodžius išsaugo naršyklėje, kad nereikėtų jo įvesti kiekvieną kartą, o tai palengvina neteisėtą prieigą prie jų duomenų.[110] Išanalizavus 2025 m. pranešimus Lietuvoje dėl asmens duomenų pažeidimų, matoma, jog net 58 % pažeidimų lėmė žmogiškieji veiksniai - klaidos, nepakankamas žinių lygis ir kt., o 29 % - kibernetiniai incidentai (neteisėtai gautos prieigos prie sistemų, kibernetinės ar išpirkos reikalaujančios atakos).[111] Technologiniai veiksniai turi reikšmingą įtaką kompiuterinių nusikaltimų atsiradimui ir plitimui, kadangi nuolatinis informacinių technologijų vystymasis ir tobulėjimas bei vartotojų neatsakingumas lemia kompiuterinių nusikaltimų vykdymo galimybes bei jų paplitimą.

---

[106] „Svarbu: „Ignitis ON" patyrė programišių ataką", Ignitis, 2024 m. vasario 12 d., https://ignitis.lt/verslui/naujienos/naujienos/svarbu-ignitis-patyre-programisiu-ataka.

[107] S. Kumar Reddy Mallidi ir Ravi Kiran Varma Penmatsa, „Optimizing Decision Tree for Multi – class VPN and Non – VPN Traffic Classification using BBFS – PSO", *PeerJ Computer Science* 12 (2026): 2 – 3, https://www.researchgate.net/publication/403538591_Optimizing_decision_trees_for_multi-class_VPN_and_non-VPN_traffic_classification_using_BBFS-PSO.

[108] Rupali Debbarma, „The Legal Framework And Challenges In Prosecuting Cybercrimes Including Hackings, Identity Theft, and Online Fraud, *Res Militaris* 13, 2 (2023): 22, https://www.researchgate.net/publication/399408186_The_Legal_Framework_And_Challenges_In_Prosecuting_Cybercrimes_Including_Hacking_Identity_Theft_And_Online_Fraud.

[109] Verizon, *2023 Data Breach Investigations Report* (New York: Verizon, 2023), 35, https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf.

[110] Krašto apsaugos ministerija, *supra note*, 104: 32.

[111] Valstybinė duomenų apsaugos inpekcija, *supra note,* 73.

Asmenų neteisėtus veiksmus kibernetinėje erdvėje skatina ir socialinio pripažinimo ir konkurencijos veiksnys. Kompiuteriniai nusikaltimai gali būti atliekami norint pademonstruoti savo įtaką ir galimybes.[112] Nusikaltėlis siekia visuomenei įrodyti, kad sugeba įveikti apsaugos sistemas ir taip įtvirtina savo statusą ir pranašumą prieš kitus. Xingan Li[113] teigia, kad tam tikrais atvejais nusikaltėlis siekia ne tik visuotinio pripažinimo, bet ir savo veiklą suvokia kaip asmeninį iššūkį sau – jiems svarbus ne tik galutinis rezultatas, bet ir pats procesas, kurio metu jie išbando savo sugebėjimus, išmoksta naujų dalykų, identifikuoja sistemų saugumo spragas ir tikrina savo ribas. Šūkis „Mano nusikaltimas yra smalsumas“ (angl. – *My crime is that of curiosity“)*[114], išpopuliarėjęs hakerių subkultūroje 1986 m., kai buvo suimtas žymus hakeris vadinęs save „Mentoriumi“, parodė, kad dalis kompiuterinių nusikaltimų grindžiamos siekiu suprasti informacines sistemas, būti geresniu už kitus ir protingesniu už sistemas.

Nigerijoje atlikto tyrimo[115] rezultatai parodė, kad pagrindiniai veiksniai, kurie lėmė jaunų asmenų įsitraukimą į kompiuterinius nusikaltimus, buvo finansinė nauda ir bendraamžių spaudimas. Jauni asmenys, turintys daug išlaidų, bet neturintys stabilaus pajamų šaltinio ieško internete būdų greitai užsidirbti papildomų pinigų. Kompiuteriniai nusikaltimai dažnai siejami su galimybe gauti finansinę naudą investuojant mažiau fizinių pastangų nei vykdant tradicines nusikalstamas veikas. Bendravimas su asmenimis, kurie jau vykdo tokio pobūdžio nusikalstamas veikas, gali formuoti požiūrį, kad tokia veikla, kuri atliekama internetinėje erdvėje, yra nepavojinga ir „mažiau bloga“, nei nusikalstamos veikos, kurios daromos fizinėje erdvėje. Atlikto tyrimo metu, tik keletas respondentų atsakė, kad kompiuterinius nusikaltimus darė tiesiog neturėdami ką veikti ir norėdami pasilinksminti.[116]

Kompiuterinių nusikaltimų paplitimą sąlygoja ir teisinės sistemos trūkumai. Pavyzdžiui, Indonezijoje kibernetinių nusikaltimų reguliavimas ir teisinis reglamentavimas kurį laiką buvo išskaidytas į skirtingus teisės aktus, o tai apsunkino nuoseklų ir efektyvų teisėsaugos institucijų darbą. Taip pat, šioje šalyje pastebimas su techninių priemonių ir specializuotų įrangų (pavyzdžiui, kibernetinių nusikaltimų laboratorijos), žmogiškųjų išteklių, specialistų kompetencijos,

---

[112] Martin C. Libicki, C*risis and Escalation in Cyberspace* (Santa Monica, RAND Corporation, 2012), 75 - 76, https://www.jstor.org/content/pdf/oa_book_monograph/10.7249/j.ctt24hrx7.pdf?refreqid=fastly-default%3A04b6dd4612bf0187868d714c17bd7ac9&ab_segments=&initiator=&acceptTC=1,
[113] Li, *supra note,* 14: 112 – 113.
[114] The Mentor, „The Hacker Manifesto, 8 January 1986“, žiūrėta 2026 m. gegužės 1 d., https://phrack.org/issues/7/3.
[115] Yetunde O. Ogunleye, U. Ojedokun ir A. A. Aderinto, „Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria“, *International Journal of Cyber Criminology* 13, 2 (2020): 309 – 310, https://www.researchgate.net/publication/339941723_Pathways_and_Motivations_for_Cyber_Fraud_Involvement_among_Female_Undergraduates_of_Selected_Universities_in_South-West_Nigeria.
[116] *Ibid.,* 315.

trūkumais.[117] Šios priežastys lėmė smarkiai padidėjusį ir sunkiai suvaldomą kibernetinių nusikaltimų skaičių Indonezijoje, kadangi nusikaltėliai nebijo būti sugauti, kadangi teisėsaugos institucijos neturės pakankamai išteklių tą padaryti.

Tuo tarpu Lietuvoje, susiduriama su kompiuterinių nusikaltimų ištyrimo ir kompetencijos trūkumo problema. 2020 m. Valstybinio audito ataskaitoje pažymima, jog policijos „specializuotų padalinių veiklos rezultatyvumas aukštas, kai į teismą perduodama ne mažiau 40 % visų baigtų bylų, tačiau šis procentas Lietuvoje nebuvo pasiektas 2016 – 2019 m. laikotarpiu (siekė 36 %)[118], o 2020 – 2025 m. laikotarpiu siekė vos 41,6 %[119] (nors atskirais metais ne visada pasiekė 40 % ribą). Nors per pastaruosius metus pavyko pasiekti 40 % ištyrimo ribą, atsižvelgiant, kad per 10 metų, Lietuvoje kompiuterinių nusikaltimų ištyrimas pagerėjo tik keliais procentais, autorės nuomone, šių nusikalstamų veikų tyrimai iki šiol susiduria su reikšmingais iššūkiais. 2020 – 2025 m. laikotarpiu iš viso užregistruota 3941 BK XXX skyriuje numatytų nusikalstamų veikų, dėl kurių net 1961 ikiteisminis tyrimas buvo sustabdytas, o tai sudaro 48,6 % *(žr. 3 lentelę)*[120]. Tokie duomenys rodo, kad kompiuterinių nusikaltimų tyrimai praktikoje išlieka sudėtingi, teisėsaugos institucijos susiduria su sunkumais nustatant ir identifikuojant nusikalstamą veiką padariusį asmenį.

3 lentelė. Užregistruotų BK XXX skyriaus nusikalstamų veikų ir sustabdytų ikiteisminių tyrimų skaičius 2020 – 2025 m. laikotarpiu.

	2020 m.	**2021 m.**	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**
Užregistruota nusikalstamų veikų	460	705	917	637	575	647
Sustabdyta ikiteisminių tyrimų pagal LR BPK 3^1 str.	124	228	317	443	439	365
Sustabdytų ikiteisminių tyrimų dalis (%)	27 %	32,3 %	34,6 %	69,5 %	76,5 %	56,4 %

Pastebima, jog iki šiol nėra sukurta kompiuterinių nusikaltimų tyrimų geroji praktika, trūksta reagavimo ir tyrimo algoritmų ir nemažai šios srities tyrėjų ir prokurorų neturi pakankamai

[117] Mujianto Mujianto, „Cybercrime Regulations as an Instrument of Legal Protection for Victims of Cybercrime in Indonesia“, pranešimas konferencijoje Proceeding of International Conference on the Law Development for Public Welfare, Indonezija, 2024 m., https://www.researchgate.net/publication/399221463_Cybercrime_Regulations_as_an_Instrument_of_Legal_Protection_for_Victims_of_Cybercrime_in_Indonesia.

[118] Aukščiausiojo audito institucija, „Ar veiksmingai kovojama su elektroniniais nusikaltimais“, Valstybės kontrolė, žiūrėta 2026 m. sausio 6 d., https://www.valstybeskontrole.lt/LT/Product/23926/ar-veiksmingai-kovojama-su-elektroniniais-nusikaltimais.

[119] Informatikos ir ryšių departamentas, *supra note*, 55.

[120] *Ibid;*.

kompetencijos tirti tokio pobūdžio nusikalstamas veikas.[121] Tokiai Lietuvos Respublikos prokuratūros nuomonei pritaria ir Aukščiausioji audito institucija, kuri nurodė, kad didelė problema yra tai, jog specializuotų pareigūnų trūkumas lemia, jog yra viršijamas vidutinis darbo krūvis (vienas tyrėjas turėtų tirti maždaug 6 bylas vienu metu, tačiau yra atvejų, kai pareigūno krūvis yra viršijamas net 3 kartus).[122] Dėl šios problemos tyrimai atliekami nepakankamai efektyviai ir nekokybiškai. Taigi, kvalifikuotų specialistų trūkumas bei sudėtingas šių nusikalstamų veikų išaiškinimas lemia, kad dalis nusikalstamų veikų lieka neišaiškintų, o įtariamieji – nenustatyti. Tokia situacija mažina nusikaltėlių rizikos suvokimą bei silpnina atgrasomąjį poveikį daryti kompiuterinius nusikaltimus, nusikaltėliai gali jaustis saugiau ir labiau rizikuoti, tikėdamiesi, kad jie nebus pagauti.

Apibendrinant, kompiuterinių nusikaltimų paplitimą lemia ne vienas atskiras veiksnys, o jų visuma. Spartus technologijų vystymasis, asmenų neatsakingumas, noras pademonstruoti savo galią ir žinias, finansinė nauda ir bendraamžių spaudimas ir teisinės spragos lemia kompiuterinių nusikaltimų paplitimą.

[121] Lietuvos Respublikos prokuratūra, *Lietuvos Respublikos prokuratūros veiklos 2024 metais ataskaita*, (Lietuva: 2025), https://www.prokuraturos.lt/data/public/uploads/2025/04/metine-prokuraturos-ataskaita-2024-final.pdf.
[122] Aukščiausiojo audito institucija, *supra note*, 118.

5. PREVENCIJA IR KONTROLĖ

Nusikalstamų veikų prevencija ir kontrolė yra vienas svarbiausių baudžiamosios politikos uždavinių.[123] Atsižvelgiant į kompiuterinių nusikaltimų paplitimą, sudėtingumą bei aukštą latentiškumo lygį, vien tik baudžiamosios atsakomybės taikymas nėra pakankamas siekiant efektyviai mažinti šių nusikalstamų veikų paplitimą. Kaip dar XVIII amžiuje teigė Š. Monteskjė, geras įstatymų leidėjas turėtų daugiau dėmesio skirti nusikaltimų prevencijai, o ne vien žmogaus nubaudimui už padarytus nusikaltimus.[124] Tad šiame darbo skyriuje bus siekiama išnagrinėti kompiuterinių nusikalstamų veikų taikomas prevencijos ir kontrolės priemones, ypatingą dėmesį skiriant nacionalinėms ir tarptautinėms strategijoms bei dirbtinio intelekto panaudojimui.

5.1. Nacionalinės ir tarptautinės strategijos

Nacionalinis kibernetinio saugumo centras (toliau – NKSC) – yra pagrindinė Lietuvos institucija atsakinga už kibernetinių incidentų stebėseną, analizę ir prevenciją Lietuvoje. Nors ši institucija nepradeda ikiteisminių tyrimų ir jų netiria, tačiau jos veikla turi netiesioginę, bet svarbią reikšmę kompiuterinių nusikaltimų prevencijai, nes leidžia laiku identifikuoti galimas grėsmes ir sumažinti jų žalą. NKSC daug dėmesio skiria ir visuomenės švietimui – nuolatos informuoja gyventojus apie galimas kibernetines grėsmes, taip pat, 2024 m. sukurti jų tinklapyje viešai prieinami kibernetinio saugumo mokymai, kurie pritaikyti skirtingoms grupėms: tiek senjorams, mokytojams ir jų mokiniams, darbuotojams ir paprastiems gyventojams, tiek įstaigų ir organizacijų vadovams, specialistams.[125] Vis didėjančio populiarumo sulaukusios NKSC organizuojamos pratybos „Kibernetinis skydas OpEx“,[126] kurios organizuojamos ne vienus metus – pratybų metu dalyvaujančios organizacijos virtualiame kibernetinių pratybų poligone gali pasitikrinti turimus kibernetinių incidentų valdymo planus, nes tenka susidurti su realiomis kibernetinėmis atakomis, jas identifikuoti ir neutralizuoti, tokiu būdu organizacijos stiprina savo kritinį mąstymą, mokosi tinkamai reaguoti ir susitvarkyti su iškilusiomis grėsmėmis.

---

[123] Gintautas Sakalauskas ir kt., *Baudžiamoji politika Lietuvoje: tendencijos ir lyginamieji aspektai* (Vilnius: Teisės institutas, 2012), 9, https://teise.org/wp-content/uploads/2012/10/Baudziamoji-politika-Lietuvoje.pdf.

[124] Charles de Montesquieu, *The Spirit of Laws* (Indianapolis: The online Library of Liberty, 1748), 115, https://oll-resources.s3.us-east-2.amazonaws.com/oll3/store/titles/837/Montesquieu_0171-01_EBk_v6.0.pdf.

[125] „NKSC Mokymai“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. gegužės 3 d., https://mokymai.nksc.lt/.

[126] „Atnaujintos svarbiausios NKSC pratybos „Kibernetinis skydas OpEx““, Nacionalinis kibernetinio saugumo centras, žiūrėta gegužės 3 d., https://www.nksc.lt/naujienos/nacionalinis_kibernetinio_saugumo_centras_eda46592.html.

Nacionalinės saugumo plėtros 2023 – 2030 m. programoje[127], išskiriami esami trūkumai kibernetinio saugumo sektoriuje, kuriuos siekiama išspręsti iškeliant šiuos uždavinius:

- Peržiūrėti ir atnaujinti esamus kibernetinio saugumo reikalavimus. Šis uždavinys bus įgyvendintas peržiūrėjus ir pakoregavus teisės aktus, kurie numato kibernetinio saugumo rizikų vertinimą, taip pat rekomendacijas mažoms ir vidutinėms įmonėms. Dabartiniai kibernetiniai saugumo reikalavimai nepakankamai išvysti nacionaliniu lygmeniu ir neapima nuolat naujai atsirandančių kibernetinių grėsmių;
- Suvienodinti kibernetinio atsparumo priemones viešajame sektoriuje (ypač ypatingos reikšmės informacinėse infrastuktūrose). Įvertinta, jog kibernetinio saugumo subjektai keliamus kibernetinio saugumo reikalavimus įgyvendina skirtingai, dažnu atveju tik iš dalies arba tik *de jure,* kadangi tai laikoma kaip biurokratinė našta[128], todėl saugos dokumentai rengiami formaliai - netiksliai, turinį apibrėžiant abstrakčiai. Dėl to būtina atlikti išsamias kibernetinio saugumo reikalavimų įgyvendinimo stebėsenas;
- Diegti naujas bendradarbiavimo platformas. Kibernetinio saugumo subjektas (toliau – KSS) turintis informacijos apie kibernetinę grėsmę ar incidentą, praneša apie tai NKSC arba Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI). NKSC ir VDAI, nustačiusios, jog yra nusikalstamos veikos požymių, perduoda informaciją policijai, kuri įvertinusi situaciją, nusprendžia pradėti ar nepradėti ikiteisminį tyrimą. Tačiau pastebėta, jog šios institucijos neatlieka tinkamo bendradarbiavimo: nustatyta, jog NKSC dažnai neperduoda reikiamos informacijos policijai, o nurodo KSS patiems kreiptis į policiją.[129] Toks bendradarbiavimo modelis mažina kibernetinių nusikaltimų kontrolės efektyvumą, kadangi ne visais atvejais nukentėjęs asmuo norės dar papildomai kreiptis į teisėsaugos institucijas, o jei ir kreipsis – tai lemia daug ilgesnį procesą ir galimybę nusikaltėliams atlikti kitas nusikalstamas veikas. Dėl to tikslinga diegti naujas platformas, kuriomis galima būtų bendradarbiauti tiek nacionaliniu, tiek tarptautiniu lygmeniu.
- Stiprinti valstybės institucijų personalo švietimą. Kasmet NKSC organizuoja tiek nacionalinio, tiek tarptautinio lygmens mokymų, siekiant stiprinti kibernetinį saugumą, tačiau matoma, kad maždaug tik penktadalis institucijų darbuotojų dalyvauja tokiuose mokymuose[130], todėl būtina sudaryti sąlygas ir skatinti darbuotojus dalyvauti tokio

[127] „Dėl 2023 – 2030 metų plėtros programos valdytojos Lietuvos Respublikos Krašto apsaugos ministerijos nacionalinė kibernetinio saugumo plėtros programos patvirtinimo“, Lietuvos Respublikos Krašto apsaugos ministerija, žiūrėta 2026 m. gegužės 4 d., https://kam.lt/pletros-programu-pazangos-priemones/.
[128] Lietuvos Respublikos Krašto apsaugos ministerija, *Nacionalinė kibernetinio saugumo ataskaita 2019* (Lietuva: 2020), https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf.
[129] Aukščiausioji audito institucija, *supra note,* 118.
[130] „2023 – 2030 metų plėtros programos valdytojos Lietuvos Respublikos Krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos pažangos priemonės Nr. 06-007-10-05-05 „Stiprinti kibernetinį atsparumą“

pobūdžio mokymuose. Lietuva siekdama stiprinti šalies kibernetinį saugumą, intensyviai ir nuolatos bendradarbiauja su užsienio šalimis, vienas sėkmingiausių Lietuvos inicijuotų projektų pradėtas dar 2018 metais – „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“[131]. Šis projektas, kurio tikslas sustabdyti kibernetines atakas ir nedelsiant reaguoti į įvykius kibernetinius incidentus, 2024 metais pirmą kartą buvo organizuotas Lietuvoje, Vilniuje, kurio metu vyko pajėgų pratybos, mokymai. Į šį projektą kasmet įsitraukia vis daugiau Europos Sąjungos šalių, kas manoma, ateityje, tik sustiprins kibernetinį saugumą ir tarpvalstybinį bendradarbiavimą. Taip pat, kibernetinis saugumas stiprinamas ir bendradarbiaujant su Jungtinėmis Amerikos Valstijomis (toliau – JAV). 2024 metų lapkritį patvirtintas Lietuvos ir JAV 2025-2029 m. bendradarbiavimo kibernetinio saugumo ir gynybos srityje planas, kuris užtikrins transatlantinį bendradarbiavimą vykdant 2024 metais įsteigtą Lietuvos kariuomenės Kibernetinės gynybos valdybą. [132]

- Didinti kibernetinio saugumo specialistų skaičių. Esant dideliam kibernetinio saugumo specialistų trūkumui[133], daugelis įmonių neturi vien už kibernetinį saugumą atsakingų specialistų, todėl būtina bendradarbiaujant su aukštųjų mokyklų atstovais, ruošti kuo daugiau būsimų specialistų, didinti visuomenės informuotumą apie šią profesiją, jos perspektyvas ir reikšmę.

Lietuvos Respublikos Krašto apsaugos ministerijos 2026 – 2028 m. veiklos plane[134] yra numatytas vienas iš prioritetinių tikslų – stiprinti kibernetinį saugumą. Šiam tikslui įgyvendinti iškeliami šie uždaviniai:

- kurti saugumo operacijų centrus, kurie veiktų atskirose organizacijose (ne visose) ir užtikrintų nuolatinę sistemų stebėseną ir reaguotų į grėsmes;

---

aprašo pagrindimas“, Lietuvos Respublikos Krašto apsaugos ministerija, žiūrėta 2026 m. gegužės 4 d., https://kam.lt/pletros-programu-pazangos-priemones/.

[131] „Lietuvos vadovaujamos ES kibernetinės greitojo reagavimo pajėgos- atsakas į incidentus tiek ES viduje, tiek remiant ES partnerius ir karines misijas“, Lietuvos Respublikos Krašto apsaugos ministerija, 2023 m. kovo 30 d., https://kam.lt/lietuvos-vadovaujamos-es-kibernetines-greitojo-reagavimo-pajegos-atsakas-i-incidentus-tiek-es-viduje-tiek-remiant-es-partnerius-ir-karines-misijas/.

[132] „Lithuanian Cyber Defence Command opened“, Lietuvos Respublikos Krašto apsaugos ministerija, 2025 m. sausio 3 d., https://kam.lt/en/lithuanian-cyber-defence-command-opened/.

[133] Linas Bukauskas, Agnė Brilingaitė ir Kęstutis Ikamas, *Lietuvos kibernetinio saugumo kompetencijų žemėlapis (ataskaita)* (Vilnius: Vilniaus universitetas, 2022), 142, https://cs.vu.lt/projects/P-REP-21- 2/ataskaita.pdf.

[134] „Įsakymas dėl Lietuvos Respublikos Krašto apsaugos ministro valdymo sričių 2026 – 2028 metų strateginio veiklos plano patvirtinimo“, Lietuvos Respublikos Krašto apsaugos ministerija, žiūrėta 2026 m. gegužės 4 d., https://kam.lt/wp-content/uploads/2026/03/2026-2028-m.-SVP-2026-02-26-Nr.-V-172.pdf.

- įgyvendinti Lietuvos kibernetinio miestelio (angl. – *Cyber Campus LT)* koncepciją. Šis uždavinys bus įgyvendintas suburiant viešojo, privataus ir mokslo sektorių bendradarbiavimo tinklą, kuris skatintų žinių sklaidą, švietimą ir inovacijas;
- į švietimo programas (bendrajame, profesiniame mokyme ir aukštajame moksle) integruoti kibernetinio saugumo ugdymą;
- parengti valstybės perėjimo prie postkvantinės kriptografijos planą[135].

Šiuos iškeltus uždavinius paskatino 2023 m. Europos Sąjungos priimta Direktyva 2022/2555[136], kuria buvo išplėstas subjektų, kuriems taikomi kibernetinio saugumo reikalavimai, ratas, tuo pačiu nustatomi griežtesni rizikos valdymo ir incidentų reagavimo įpareigojimai bei didinama organizacijų atsakomybė už kibernetinio saugumo pažeidimus. Krašto apsaugos ministerija koordinavo šios direktyvos įtvirtinimą į Lietuvos teisės aktus – buvo atnaujintas Kibernetinio saugumo įstatymas, pakoreguoti kiti reikšmingi nacionaliniai teisės aktai bei apie pokyčius informuoti kibernetinio saugumo subjektai.[137]

Prevencine veikla aktyviai užsiima ir Lietuvos policija, kuri nuolat organizuoja susitikimus su prižiūrimų teritorijų bendruomenės nariais, kurių metu skleidžia informaciją apie kibernetinį saugumą ir kaip apsisaugoti nuo galimų grėsmių, dalina prevencinius šviečiamojo pobūdžio lankstinukus. Per 2024 m. daugiau nei 1840 įvykdyta tokių susitikimų. Nuolat bendradarbiaujama su privataus sektoriaus atstovais, mobiliojo ryšio operatorių atstovais, pinigų plovimo prevencijos kompetencijų centru.[138] Taip pat, Europos Sąjungos teisėsaugos bendradarbiavimo agentūra – Europol, kartu su policija išskiria šias pagrindines, apsisaugojimo nuo kibernetinių nusikaltimų, priemones:[139]

- Saugotis netikėtų prašymų. Gavus el. laišką, žinutę ar skambutį skubiai pateikti kažkokius asmeninius duomenis, iš pradžių būtina patikrinti ar tai nėra apsimetėliai. Pavyzdžiui, sulaukus skambučio iš mobilaus ryšio operatoriaus, rasti oficialųjį jų numerį internete ir susisiekti su jais, siekiant išsiaiškinti ar tikrai jie jums skambino;

---

[135] Prognozuojama, jog per ateinantį dešimtmetį bus sukurti pakankamai galingi kvantiniai kompiuteriai, gebantys nulaužti algoritmus, kurie dabar naudojami apsaugai pasirašant elektroniniu parašu, jungiantis prie elektroninės bankininkystės ir kt. Postkvantinė kriptografija – naujas kriptografijos metodas, kuris būtų atsparus kvantinių kompiuterių atakoms.

[136] „Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)“, Official Journal of the European Union, žiūrėta 2026 m. gegužės 4 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

[137] Krašto apsaugos ministerija, *supra note*, 71: 7.

[138] *Ibid.*, 70.

[139] „Sukčiavimui atspari mąstysena: paprasti apsisaugoti padedantys įpročiai“, Europol, žiūrėta 2026 m. gegužės 4 d., https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/scam-aware-mindset-simple-habits-to-stay-protected:lt.

- Saugoti savo asmeninius duomenis ir informaciją. Telefoninio pokalbio metu geriausia yra neteikti jokios asmeninės informacijos apie save ar savo duomenis, nebent esate įsitikinęs su kuo šnekate.
- Atkreipti dėmesį į klaidas. Apsimetėliai dažnai siųsdami laiškus ar nuorodas, ant kurių prašo paspausti, įvelia rašybos klaidų, taip pat dažnai el. paštas iš kurio siunčiamas laiškas gali atrodyti kaip tikras, tačiau jo siuntėjo adrese bus papildomų skaičių ar simbolių. Oficialius el. paštus ir kontaktus dažniausiai galima pasitikrinti internete, o kilus įtarimui, geriau laiško ar jame esančių nuorodų – neatidarinėti. Taip pat ir su QR kodų nuskaitymais. Nuskaičius klaidingą QR kodą rizikuojama atskleisti savo privačius duomenis arba užkrėsti savo įrenginį virusu.
- Skirti laiko savo saugumui. Siekiant išvengti kibernetinių grėsmių, būtina reguliariai atnaujinti savo įrenginio programinę įrangą, naudoti sudėtingus slaptažodžius, o jei įmanoma – dvielementį tapatumo nustatymą.

Tarptautinėse ataskaitose pabrėžiama[140], jog didelę dalį kibernetinių incidentų lemia žmogiškasis faktorius – nusikaltėliai išnaudoja vartotojų neatsargumą, todėl viena svarbiausių kibernetinių grėsmių prevencijos krypčių yra visuomenės informuotumo didinimas. Europos Sąjungos kibernetinio saugumo agentūra periodiškai konsultuoja Lietuvą ir kitas valstybes nares dėl kibernetinio saugumo priemonių, esamų ir būsimų teisės aktų kūrimo bei atnaujinimo, tačiau pabrėžia, jog vien techninių prevencijos priemonių neužtenka, jei vartotojai elgiasi neatsakingai.

Apibendrinant, prevencija ir kontrolė kibernetinio saugumo srityje įgyvendinama vadovaujantis tarptautinėmis rekomendacijomis ir teisės aktais, kurie nustato pagrindines kryptis ir prioritetus. Tiek tarptautiniu, tiek nacionaliniu lygmeniu ypatingas dėmesys skiriamas visuomenės švietimui, informuotumo didinimui bei saugaus elgesio internete skatinimui. Tačiau ne mažiau svarbu vaidmenį atlieka ir techninės bei organizacinės priemonės, tokios kaip informacinių sistemų sauga, rizikų valdymas ir stebėsena.

5.2. Dirbtinio intelekto panaudojimas kovoje su kibernetinėmis grėsmėmis

Tobulėjant dirbtiniam intelektui (toliau – DI), nusikaltėliai vis dažniau naudojasi DI galimybėmis, kad atliktų automatizuotas ir sudėtingesnes atakas, lengviau gautų priėjimą prie

[140] ENISA, *Raising Awareness of Cybersecurity*: *A Key Element of National Cybersecurity* (Graikija: 2021), 9 – 12, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Raising%20awareness%20of%20cybersecurity%20as%20a%20key%20element%20of%20NCSS.pdf.

asmens duomenų.[141] Tačiau tuo pačiu, vis daugiau dėmesio yra skiriama DI pritaikymui kovoje su kibernetinėmis grėsmėmis. Dėl savo gebėjimo nuolatos mokytis, analizuoti ir sisteminti didelius informacijos srautus, DI yra pritaikytas aptikti galimas grėsmes ar pažeidimus, automatiškai reaguoti į kilusią grėsmę. Viena iš sričių, kurioje dirbtinis intelektas plačiai taikomas pasauliniu mastu yra debesų kompiuterijos aplinkoje saugomų duomenų apsauga.

Kaip minėta ankstesniame skyriuje, tam tikri nusikaltėliai jau sugeba įveikti saugomą debesijos tinklą. DI naudingas tuom, kad įdiegus Nulinio Pasitikėjimo Architektūros sistemą (angl. – *Zero Trust Architecture)*, kuri užuot pasitikėjusi prisijungti bandančiais vartotojais pagal jų tinklo vietą, ši sistema užtikrina visų vartotojų ir jų įrenginių tikrinimą pagal tris kriterijus: tapatybė, elgesys ir rizikos profilis.[142] DI padeda analizuoti vartotojų elgseną, aptikti anomalijas ir priimti sprendimus dėl prieigos suteikimo. Iš esmės, DI sistemos pasižymi gebėjimu mokytis iš konkrečios organizacijos duomenų ir prisitaikyti prie jos veiklos ypatumų ir gali atlikti šiuos veiksmus:[143]

- nuolatinė stebėsena ir duomenų surinkimo (apdorojimo) procesai;
- anomalijų aptikimo mechanizmai realiu laiku;
- dirbtiniu intelektu pagrįsti sprendimų modeliai, skirti grėsmių klasifikavimui;

Tad DI veikdamas kartu su kitomis apsaugos sistemomis gali identifikuoti grėsmę dar iki jai pasiekiant kritinį lygmenį ir padarant žalą. Įvairios įmonės DI pasitelkia aptinkant kenkėjiškas programas, atrenkant grėsmę keliančius el. laiškus, kuriuose gali būti siunčiami virusai, kad to nereikėtų daryti rankiniu būdu.

Visiems gerai žinomos įmonės, tokios kaip „Google“, „Microsoft“ ar „IBM“ per pastaruosius metus pradėjo viešai reklamuoti jų kuriamas DI sistemas ir net skatinti jų panaudojimą apsaugos sistemose. „Google“ teigia, kad generatyvinis DI prisidėjo prie aukštesnės kokybės incidentų rezultatų analizės ir tuo pačiu sutaupė 51 % specialistų laiko skirto užduotims atlikti.[144] Taip pat, DI gali iš anksto nuspėti galimą grėsmę kenkėjiškų interneto adresų (angl. – *Uniform Resource Locator*) rinkiniu. Pavyzdžiui, „VirusTotal“ – „Google“ sukurta grėsmių

---

[141] Premanand Narasimhan ir Kala Baskar, „Securing the Metaverse: AI – Driven Solutions for Cyber Security, Privacy and User Trust“, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 10, 6 (2024): 1891 – 1892, https://www.researchgate.net/publication/387377644_Securing_the_Metaverse_AI-Driven_Solutions_for_Cyber_Security_Privacy_and_User_Trust.

[142] Rajesh Adepu, „Autonomous Cyber Defense Systems Powered by AI for Enterprise Cloud Enviroments“, *International Journal of Computer Engineering and Technology* 17, 2 (2026): 25 – 26, https://www.researchgate.net/publication/403909469_AUTONOMOUS_CYBER_DEFENSE_SYSTEMS_POWERED_BY_AI_FOR_ENTERPRISE_CLOUD_ENVIRONMENTS.

[143] *Ibid.*, 26.

[144] Polona Car ir Tristan Marelin, „Artificial Intelligence and Cybersecurity”, European Parliament, žiūrėta 2026 m. gegužės 5 d., 2, https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA(2024)762292_EN.pdf.

analizės platforma, DI pagalba leidžia patikrinti įtartinus failus, nuorodas ar IP adresus (domenus). Nors analizės atliekamos naudojant antivirusines sistemas, tačiau tuo pačiu DI pagalba informacija yra tikrinama jau žinomų grėsmių duomenų bazėse ir vertinant failų ir nuorodų elgseną.[145]

Dirbtinio intelekto technologijos naudojamos kai kuriose šalyse ir vykdant atvirųjų šaltinių žvalgybą (angl. – *Open Source Intelligence)*[146]. Dirbtinis intelektas pagrįstas mašininiu mokymosi ir natūralios kalbos apdorojimu, gali rasti ir apdoroti tokią informaciją, kurios žmogaus protas nesugebėtų atpažinti ir perprasti.[147] Tai ypač naudinga analizuojant tamsiajame internete vykstančius procesus, nustatant neteisėta veikla užsiimančius asmenis ir numatant galimas grėsmes ir nusikaltėlių taikinius. Naujai sukurta dirbtinio intelekto sistema *(*angl. – *Vigilante),* atlikdama išsamią teksto analizę anonimizuotuose tamsiojo interneto kanaluose, identifikuoja anomalijas ir riziką keliančius asmenis. Po daugybės testavimų ir mašininio mokymosi, dirbtinio intelekto sistemos užfiksuojama informacija atitiko teisėsaugos institucijų naudojamus nustatymo kriterijus.[148] Tokios dirbtiniu intelektu paremtos sistemos mažina žmogiškųjų išteklių poreikį identifikuojant galimas kompiuterinių nusikaltimų grėsmes.

Generatyvinis dirbtinis intelektas Lietuvoje sparčiai plinta įvairiose įmonėse. Jis taikomas prevenciškai apsaugant sistemas nuo kibernetinių grėsmių be žmogaus įsikišimo (aptinka ir pašalina kenkėjiškas programas, blokuoja pavojingus IP adresus, nuspėja galimus pažeidimus ar silpnąsias sistemų vietas, analizuoja vartotojų elgsenos modelius ir kt.). Tačiau DI naudojimas vis dar išlieka ribotas, ypač viešojo saugumo sektoriuje, kadangi DI sistemų diegimas reikalauja didelių finansinių investicijų, taip pat DI sistemų efektyvumas priklauso nuo jo mokymo proceso, nuolatinio tobulinimo, o tai reikalauja laiko ir žmogiškųjų išteklių.[149] Dėl šių priežasčių DI prevencinės priemonės dažniausiai taikomos kaip pagalbinė priemonė, tačiau ilgalaikėje perspektyvoje jų vaidmuo kibernetinio saugumo srityje taps vis reikšmingesnis.

Apibendrinant, kibernetinio saugumo užtikrinimas šiais laikais nebegali būti grindžiamas vien pavienėmis priemonėmis – vis didesnę reikšmę įgauna kompleksinis ir į prevenciją orientuotas požiūris. Nors tradicinės prevencijos ir kontrolės priemonės išlieka svarbios, jų

---

[145] Car ir Marelin, *supra note,* 144: 2.
[146] Atvirųjų šaltinių žvalgyba – tai vienas iš informacijos rinkimo būdų naudojant viešai prieinamus duomenis. Tokia informacija renkama iš socialinių tinklų, naujienų portalų, viešų forumų, svetainių ar registrų.
[147] Nitin Soni ir Rakesh Poonia, „AI – Driven Open – Source Intelligence in Digital Forensics for Cybercrime Investigation“, *Journal of Collective Sciences and Sustainability* 1 (2025): 2 – 3, https://www.researchgate.net/publication/393924645_AI-driven_open-source_intelligence_in_digital_forensics_for_cybercrime_investigation.
[148] Vamshidhar Reddy Vemula, „AI – Powered Framework for Proactive Monitoring of Dark Web Marketplaces and Prediction of Emergent Cybercrime Trends“, *FMDB Transactions on Sustainable Computer Letters* 3, 3 (2025): 127, https://www.researchgate.net/publication/397563566_AI-Powered_Framework_for_Proactive_Monitoring_of_Dark_Web_Marketplaces_and_Prediction_of_Emergent_Cybercrime_Trends.
[149] „Ar Dirbtinis Intelektas Perims Kibernetinį Saugumą“, Solix Technologies, žiūrėta 2026 m. gegužės 5 d., https://www.solix.com/lt/blog/learning/will-ai-take-over-cyber-security/.

efektyvumas neretai priklauso ir nuo visuomenės sąmoningumo ir atsargaus elgesio, todėl ypatingas dėmesys skiriamas būtent šiai sričiai. Taip pat, šiame kontekste išryškėja dirbtinio intelekto panaudojimo svarba, stiprinant prevenciją ir atliekant kontrolę, nors jo taikymas vis dar susiduria su tam tikrais iššūkiais.

6. EMPIRINIS TYRIMAS

6.1. Tyrimo metodologija

Šio darbo tikslui ir uždaviniams pasiekti atliktas empirinis tyrimas – 9 ikiteisminio tyrimo tyrėjų, dirbančių Lietuvos policijoje, kokybinis tyrimas interviu būdu. Ikiteisminio tyrimo tyrėjai parinkti pagal jų specializuotą darbo kryptį, susijusią su kompiuterinių nusikalstamų veikų tyrimais.

Atliekant empirinį tyrimą buvo laikomasi mokslinių tyrimų etikos principų. Tyrimo dalyviai buvo informuoti apie tyrimo tikslą, dalyvavimo savanoriškumą. Taip pat, buvo užtikrintas tyrimo dalyvių anonimiškumas ir duomenų konfidencialumas. Tyrimas buvo vykdytas laikotarpiu nuo 2026 m. gegužės 15 d. iki 21 d. Su tyrimo dalyviais bendrauta elektroniniu paštu. Jiems buvo užduodami 7 atviri klausimai *(priedas Nr. 5*).

Empirinio tyrimo rezultatai pateikiami nurodant tyrėjo klausimą (tyrėjo klausimas žymimas – T) ir kiekvieno iš respondentų atsakymą (respondentai įvardijami nuo R1 iki R9).

6.2. Tyrimo rezultatų analizė

T. Kiek metų tiriate nusikalstamas veikas, numatytas BK XXX skyriuje (nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui)?

R1. 5 metai.

R2. Specializuojuosi 8 metus.

R3. Nusikalstamas veikas, numatytas BK XXX skyriuje, tiriu apie kelerius metus. Praktikoje dažniausiai tenka susidurti su neteisėtu prisijungimu prie informacinių sistemų, duomenų pasisavinimu, sukčiavimais elektroninėje erdvėje.

R4. Nusikalstamas veikas, numatytas BK XXX skyriuje, t. y. nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui, tiriu apie 7 metus.

R5. Nuo 2026-01-23 Vilniaus apskrities vyriausiojo policijos komisariato Kriminalinės policijos nusikaltimų nuosavybei tyrimo valdybos 1-ojo skyriaus vyresnioji tyrėja.

R6. 3 metus.

R7. Nusikalstamas veikas, numatytas BK XXX skyriuje, tiriu jau keletą metų.

R8. Greitai bus 3 metai.

R9. 1 metus.

T. Kaip per pastaruosius kelerius metus pasikeitė kompiuterinių nusikaltimų pobūdis ir mastas Jūsų praktikoje?

R1. Nepastebėjau, kad būtų išaugęs nusikalstamų veikų, numatytų aukščiau nurodytame skirsnyje, skaičius. Per minėtą tarnybos laikotarpį, jis išlieka panašus. Kaip pvz. šiuo metu, specializuotame padalinyje, kuris tiria nusikalstamas veikas, padarytas elektroninėje erdvėje, nusikaltimai, numatyti BK XXX skyriuje sudaro 37 proc. visų šiuo metu atliekamų ikiteisminių tyrimų, kurie pagal 2024-02-14 Nr. 10-IL-2870 Lietuvos policijos generalinio komisaro patvirtintas Policijos įstaigų padalinių kompetencijų atlikti ikiteisminius tyrimus aprašą priskirti šiam skyriui. Žinoma reikia paminėti dėl nusikalstamų veikų, numatytų LR BK 198-1 str. „Neteisėtas prisijungimas prie informacinės sistemos". Ši nusikalstama veika dažnai padaroma kartu su nusikalstama veika, numatyta LR BK 182 str. „Sukčiavimas". Pastaruoju metu šių nusikalstamų veikų skaičius žymiai išsaugo, palyginus su ankstesniais metais. Šiuo metu vyrauja nusikalstamos veikos, kuomet nusikalstamą veiką vykdantys asmenys atlieka apgaulingus skambučius, prisistatydami telekomunikacijų, banko darbuotojais, policijos pareigūnais, įgaudami asmenų pasitikėjimą, gauna prieigą prie jų el. banko duomenų ir atlieka neteisėtus prisijungimus prie interneto banko bei atlieka neteisėtas finansines operacijas. Taip pat vyrauja nusikalstamos veikos, kuomet nusikalstamą veiką vykdantys asmenys siunčia nuorodą, skirtą išgauti prisijungimo prie interneto banko duomenis ir inicijuoti finansinę operaciją.

R2. Per pastaruosius kelerius metus kompiuterinių nusikaltimų pobūdis ir mastas ženkliai pasikeitė. Nusikaltimai tapo labiau organizuoti, profesionalūs. Labiausiai paplito išpirkos reikalaujantys išpuoliai, duomenų vagystės ir prisijungimų perėmimas. Sukčiavimo atakos tapo labiau personalizuotos ir įtikinamos, dažnai pasitelkiant dirbtinį intelektą. Taip pat padaugėjo tikslinių atakų prieš įmones ir valstybines institucijas. Apskritai kibernetiniai nusikaltimai tapo globalesni, dažnesni ir techniškai sudėtingesni.

R3. Per pastaruosius metus kompiuterinių nusikaltimų mastas akivaizdžiai išaugo. Nusikaltimai tapo sudėtingesni, dažniau naudojami anonimiškumo įrankiai, dirbtinis intelektas, socialinė inžinerija. Taip pat daugėja atvejų, susijusių su finansiniu sukčiavimu internete.

R4. Per pastaruosius kelerius metus kompiuterinių nusikaltimų pobūdis pastebimai pasikeitė. Nusikalstamos veikos tapo labiau organizuotos, techniškai sudėtingesnės ir dažniau vykdomos naudojant tarptautinę infrastruktūrą: užsienio IP adresus, VPN, tarpinius serverius, anonimizavimo priemones, kriptovaliutas, netikras paskyras bei socialinės inžinerijos metodus. Taip pat padidėjo tokių nusikalstamų veikų mastas. Praktikoje dažniau susiduriama ne su pavieniais atvejais, o su platesnėmis schemomis, kai nukentėjusieji yra keli ar net daug asmenų, o nusikalstama veikla vykdoma per skirtingas platformas, banko sąskaitas, elektronines pinigines ar socialinius tinklus.

Pastebima, kad techninis įsilaužimas dažnai derinamas su apgaule, psichologiniu poveikiu nukentėjusiajam ir neteisėtu duomenų panaudojimu.

R5. Sukčiavimams vykdyti vis dažniau naudojami ir kuriami įtikinami el. laiškai, SMS žinutės, net netikri balso ar vaizdo įrašai, nuorodos. Apgaulingi el. laiškai ar žinutės, tokiu būdu bandoma išvilioti prisijungimus prie banko sąskaitų**.** Daugėja išpuolių prieš mobiliuosius įrenginius, taikomasi į senesnius telefonus ir neatsinaujinusias sistemas. Taip pat prieš el. paštų serverius, kai sistemos nėra apsaugomos ar atnaujinamos dėl saugumo.

R6. Nepasakyčiau, jog būčiau pastebėjus labai padidėjusį BK XXX skyriaus nusikalstamų veikų skaičių, bet sakyčiau, šios nusikalstamos veikos tapo sudėtingesnės. Sudėtingesnės ta prasme, kad nemažai nusikalstamą veiką padariusių asmenų yra užsieniečiai, kurie trumpam atvyksta į Lietuvą, todėl dažnai apie juos praktiškai jokių duomenų neturim (kur gyvena, kokį telefono numerį naudoja ir pnš.), todėl sunkiau juos surasti ir sulaikyti. Tuo pačiu ir pačios nusikalstamos veikos sudėtingėja, nes nusikaltėliai naudoja vis sudėtingesnes technines priemones, kurias net mums patiems, tyrėjams, kartais sunku perprasti. Šie nusikaltimai vis dažniau nėra „paprastų“ žmonių atliekamos pavienės nusikalstamos veikos, o vis dažnėja organizuotų grupuočių, kurias yra gan sunku nustatyti.

R7. Per pastaruosius kelerius metus kompiuterinių nusikaltimų pobūdis tapo gerokai sudėtingesnis ir profesionalesnis. Anksčiau dažniau pasitaikydavo pavieniai neteisėti prisijungimai ar paprastesnės sukčiavimo schemos, o dabar daugėja organizuotų, tarptautiniu mastu veikiančių grupuočių vykdomų nusikaltimų. Taip pat sparčiai išaugo socialinės inžinerijos, „phishing“, investicinio sukčiavimo bei išpirkos reikalaujančių virusų atvejų skaičius. Nusikaltėliai aktyviai naudojasi anonimiškumo priemonėmis, kriptovaliutomis ir užsienio serveriais, todėl tyrimai tampa sudėtingesni.

R8. Kompiuterinių nusikaltimų pobūdis sudėtingėja. Vis daugiau šias nusikalstamas veikas padaro šios srities „profesionalai“, kurie naudoja sudėtingą techniką, leidžiančią užšifruoti savo banko sąskaitas, telefono numerius, IP adresus. Be to, kiek pati pastebėjau ir kiek kolegos sakė, šios nusikalstamos veikos buvo paprastesnės, pavienių asmenų atliekami „smulkūs“ veiksmai. Su metais, jau ir dabar pastebiu, kad šias nusikalstamas veikas daro asmenys organizuotai, kurie siekia trikdyti informacinių sistemų veiklą, finansiškai pasipelnyti. Padaugėjo ir atvejų kai nusikaltėliai naudoja dirbtinį intelektą, kuris padeda dar labiau paslėpti savo veiksmus ir tapatybę.

R9. Kompiuterinių nusikaltimų tyrimų pradedama nemažai, jų vis daugėja. Vėliau, daugelis tyrimų būna nutraukiama arba sustabdoma, nes nepavyksta nustatyti asmens, padariusio nusikalstamą veiką. Todėl galima sakyti, kad kompiuterinių nusikaltimų pobūdis tikrai pasikeitė – nusikaltimai tapo sudėtingesni, labiau apgalvoti, nusikaltėliai greitai išmoksta paslėpti savo neteisėtus veiksmus, todėl tyrėjams bendradarbiaujant su prokurorais yra sunku nustatyti nusikalstamą veiką

padariusį asmenį. BK XXX skyriaus nusikalstamos veikos dažnai padaromos su kitomis veikomis, pavyzdžiui sukčiavimas.

T. Kokie, Jūsų nuomone, yra pagrindiniai veiksniai, lemiantys kompiuterinius nusikaltimus?

R1. Nusikalstamas veikas vykdančių asmenų žinios informacinių technologijų srityse, leidžiančios įvykdyti šiuos nusikaltimus, kuomet yra galimybė nuslėpti savo tapatybę ir apsunkinti jos nustatymą. Nėra reikalingas tiesioginis („gyvas“) kontaktas su nukentėjusiuoju, mažiau rizikos dėl galimybės, kad būsi „užkluptas“ nusikaltimo padarymo vietoje, bei dėkingos technologijų išplitimo aplinkybės, leidžiančios labai gerai paslėpti nusikalstamos veikos „pėdsakus“ elektroninėje erdvėje (VPN paslaugos, „TOR“ naršyklės[150], „SIM spiečių“[151] naudojimas skambučių atlikimui, IP telefonija, finansinių operacijų atlikimas virtualiomis valiutomis ir kt.). Taip pat būtina pažymėti, kad tokias nusikalstamas veikas, gali atlikti būdamas bet kurioje pasaulio vietoje ir jos gali būti nukreiptos į bet kurios šalies gyventojus.

R2. Pagrindiniai veiksniai, lemiantys kompiuterinius nusikaltimus, yra technologinė pažanga, didėjantis interneto naudojimas ir skaitmeninių paslaugų plėtra. Nusikaltimus taip pat skatina silpnas kibernetinis saugumas, vartotojų neatsargumas. Taip pat įtakos turi globalizacija, leidžianti veikti anonimiškai ir iš bet kurios pasaulio vietos. Pastaruoju metu nusikaltimų augimą skatina ir dirbtinio intelekto technologijų panaudojimas.

R3. Pagrindiniai veiksniai – technologijų prieinamumas, nepakankamas žmonių informuotumas apie kibernetinį saugumą, galimybė veikti anonimiškai bei finansinė nauda nusikaltėliams.

R4. Pirmiausia – spartus technologijų naudojimo augimas ir didelė visuomenės priklausomybė nuo elektroninių paslaugų, bankininkystės, socialinių tinklų bei mobiliųjų įrenginių. Antra – nepakankamas gyventojų skaitmeninis raštingumas ir saugumo įpročiai: silpni slaptažodžiai, daugkartinis tų pačių slaptažodžių naudojimas, neatidumas nuorodoms, sukčiavimo žinutėms ar netikriems prisijungimo puslapiams. Taip pat reikšmingas veiksnys yra nusikaltimų anonimiškumas ir tarptautinis pobūdis. Nusikaltėliai dažnai veikia iš užsienio, naudoja technines priemones savo tapatybei slėpti, todėl išaiškinimas tampa sudėtingesnis. Be to, dalis nusikaltimų yra finansiškai labai patrauklūs, nes nedidelėmis sąnaudomis galima pasiekti daug potencialių aukų.

[150] „Tor“ naršyklė – interneto naršyklė, kuri nukreipia interneto srautą per kelis tarpinius užšifruotus serverius, dėl ko tampa sudėtingiau nustatyti naudotojo tapatybę, buvimo vietą ar atliekamą veiksmą internete.

[151] „SIM spiečiai“ – didelio kiekio tarpusavyje sujungtų SIM kortelių sistema, leidžianti vienu metu valdyti daugybę telefono numerių, siųsti didelius kiekius trumpųjų žinučių, atlikti skambučius. Ši sistema taip pat naudojama siekiant išvengti tapatybės patvirtinimo mechanizmus kuriant anonimines paskyras ar vykdant automatizuotą registraciją socialiniuose tinkluose.

R5. Spartus technologijų vystymasis; Silpnas kibernetinis saugumas; Žemas vartotojų sąmoningumas, nes neatpažįsta kenkėjiškų laiškų, paspaudžia nuorodas, dalijasi asmenine informacija, perleidžia savo banko sąskaitų prisijungimus ar PIN kodus.

R6. Žinoma, pirmoje vietoje yra informacinių sistemų platus naudojamas, daug kas šiais laikais yra skaitmenizuota, pirkimai telefonu, nuotolinis darbas. Nusikaltėliams tai labai paranku, nes labai daug taikinių yra. Taip pat, žmonės gal yra nepakankamai informuojami, kad saugotųsi ar gal tiesiog žmonės kažkaip nepakankamai saugosi, nes nusikaltėliams pavyksta kartais paprasčiausiais būdais išvilioti asmens duomenis, kuriuos vėliau gali panaudoti.

R7. Pagrindiniai veiksniai, lemiantys kompiuterinius nusikaltimus, yra spartus technologijų vystymasis, visuomenės priklausomybė nuo skaitmeninių paslaugų bei nepakankamas gyventojų kibernetinio saugumo raštingumas. Taip pat svarbų vaidmenį turi finansinė motyvacija, nes dauguma tokių nusikaltimų siekiama neteisėtos finansinės naudos. Nusikalstamumą skatina ir galimybė veikti anonimiškai bei tarptautinis interneto pobūdis.

R8. Asmenims yra "patogu" daryti kompiuterinius nusikaltimus, nes sumažėja rizika būti pagautiems, nei, kad darytų nusikalstamą veiką realiai, fizinėje erdvėje. Nusikaltėliai išmoko paslėpti savo veiksmus, dėl ko yra sunku nustatyti nusikalstamą veiką padariusį asmenį. Taip pat, vis labiau plečiasi ir tobulėja dirbtinis intelektas, kurį nusikaltėliai panaudoja kaip priemonę, nusikalstamoms veikoms atlikti. Nukentėti nuo šių nusikalstamų veikų gali vos ne kiekvienas, kadangi gyvename tokiais laikais, kai visi naudojames išmaniaisiais įrenginiais, kompiuteriais tiek namuose, tiek darbe. Taip pat, vienas iš veiksnių yra prastas kibernetinis saugumas – žmonės naudoja prastas apsaugos sistemas arba jų išvis nenaudoja, susidūrus su grėsme nemoka jos identifikuoti, paspaudžia ant įtartinų el. laiškų ar nuorodų, nepatikrina svetainės tikslaus pavadinimo, susilaukę skambučių iš „teisėsaugos institucijų" ar telekomunikacijos tinklų operatorių iškart atskleidžia jiems asmeninę informaciją.

R9. Pagrindinis veiksnys, lemiantis kompiuterinius nusikaltimus yra finansinė nauda. Taikinių skaičius yra didelis, kadangi daug žmonių naudoja internetą, perka internetu ar dirba nuotoliu, todėl nusikaltėliams reikia tiesiog rasti tinkamą asmenį, kuris galbūt turi prastesnes apsaugos sistemas, ar prastesnį suvokimą apie kompiuterinius nusikaltimus. Informacinės technologijos sparčiai plečiasi, taip pat ir dirbtinis intelektas, kurio pagalba galima daryti sudėtingesnes ir sunkiau susekamas nusikalstamas veikas.

T. Ar Jūsų nuomone, Lietuvos policijai pakanka techninių ir žmogiškųjų išteklių ir kvalifikacijos, tiriant kompiuterinius nusikaltimus?

R1. Manau, kad šiuo laikotarpiu Lietuvos policijai labiau nepakanka žmogiškųjų išteklių, nei techninių išteklių ar kvalifikacijos. Pareigūnai vyksta į įvairius mokymus, kurie vyksta tiek Lietuvoje, tiek įvairiose užsienio šalyse bei nuotoliu. Žinoma, darbą apsunkina ir tam tikrų techninių išteklių neturėjimas, pačių šių nusikalstamų veikų latentiškumas, sunkumai gaunant informaciją iš užsienio institucijų, tarptautinio bendradarbiavimo terminai.

R2. Mano nuomone, Lietuvos policija turi gana stiprią kibernetinių nusikaltimų tyrimo kompetenciją ir pastaraisiais metais ji nuolat tobulinama. Yra specializuoti padaliniai, dirbantys su skaitmeniniais įrodymais ir sudėtingomis IT bylomis. Tačiau kibernetinių nusikaltimų mastas ir sudėtingumas auga greičiau nei institucijų resursai, todėl tam tikrais atvejais vis dar jaučiamas specialistų ir techninių priemonių trūkumas. Taip pat reikalingas nuolatinis darbuotojų kvalifikacijos kėlimas dėl greitai besikeičiančių technologijų. Apibendrinant galima teigti, kad ištekliai yra pakankami baziniam lygiui, tačiau ilgalaikėje perspektyvoje juos būtina stiprinti.

R3. Mano nuomone, išteklių ir specialistų vis dar trūksta, ypač atsižvelgiant į sparčiai augantį tokių nusikaltimų kiekį. Tačiau kvalifikacija gerėja, vyksta mokymai, stiprinamos specializuotos pajėgos.

R4. Lietuvos policijoje yra kvalifikuotų pareigūnų, turinčių patirties tiriant kompiuterinius nusikaltimus, tačiau atsižvelgiant į šių nusikaltimų mastą ir techninį sudėtingumą, išteklių ne visada pakanka. Tokie tyrimai reikalauja specifinių žinių, nuolatinio kvalifikacijos kėlimo, techninių priemonių, greitos prieigos prie duomenų ir gebėjimo analizuoti didelės apimties skaitmeninę informaciją. Praktikoje juntamas didesnis specializuotų pareigūnų, analitikų, skaitmeninės kriminalistikos specialistų ir techninių įrankių poreikis. Kadangi nusikaltimų metodai nuolat keičiasi, kvalifikacijos kėlimas turėtų būti nuolatinis, o ne epizodinis.

R5. Nepakanka, nes Lietuvos policija taip greit netobulėja, kaip šiuo metu sparčiai vystosi technologijos.

R6. Labiausiai trūksta žmogiškųjų išteklių. Turime daug kvalifikuotų, išsilavinusių pareigūnų, bet kai taip smarkiai plečiasi ir tobulėja kompiuteriniai nusikaltimai (ir tuo pačiu sudėtingėja), atrodo, reikia vis daugiau ir daugiau specialistų, gerai išmanančių kompiuterinius nusikaltimus. Tyrėjų kompetencija yra nuolat tobulinama, organizuojami įvairūs mokymai, žinoma, ne visada visiems tyrėjams pavyks nuvykti į tuos mokymus, dėl didelio darbo krūvio.

R7. Mano nuomone, Lietuvos policijos pajėgumai kompiuterinių nusikaltimų srityje gerėja, tačiau iššūkių vis dar yra. Technologijos sparčiai tobulėja, todėl būtina nuolat investuoti į specialistų kvalifikacijos kėlimą, techninę įrangą ir programinę įrangą. Taip pat jaučiamas kvalifikuotų

specialistų trūkumas, nes privatų sektorių dažnai vilioja didesni atlyginimai. Nepaisant to, tyrėjų kompetencija ir bendradarbiavimas su kitomis institucijomis nuosekliai stiprėja.

R8. Manau Lietuvos policijos situacija tiriant kompiuterinius nusikaltimus nėra prasta, bet tikrai yra daug kur tobulėti. Kvalifikuotų specialistų nuolat trūksta, kadangi šių nusikalstamų veikų tyrimai yra sudėtingi ir ilgai trunkantys, todėl sunku pritraukti tyrėjus į šią sritį. Šių nusikalstamų veikų kiekis yra nemažas, jų tyrimai reikalauja sudėtingų veiksmų, bendradarbiavimo su užsienio ir Lietuvos insitucijomis, todėl ne visada pavyksta kiekvieną tyrimą atlikti išsamiai ir kokybiškai. Taip pat, sparčiai tobulėjant informacinėms technologijoms, tyrėjams yra būtina nuolat atnaujinti savo žinias ir įgūdžius, prisitaikant prie vis naujai atsirandančių kompiuterinių nusikaltimų rūšių.

R9. Daugiausiai trūksta mokymų ikiteisminio tyrimo tyrėjams. Dirbu jau apie metus, tačiau dar nedalyvavau mokymuose susijusiuose su kompiuteriniais nusikaltimais, todėl daugiausiai patirties įgyjama iš kolegų ir tiesiog tiriant kompiuterinius nusikaltimus. Tuo pačiu, trūksta ir pačių tyrėjų, kadangi policijoje darbuotojų kaita vyksta nuolatos, o tyrimai vis sudėtingėja, reikalauja daugiau laiko vien susipažinti su ikiteisminio tyrimo medžiaga.

T. Ar praktikoje susiduriate su sunkumais bendradarbiaujant su kitomis įstaigomis (nacionaliniu ir tarptautiniu lygmeniu)? Jei taip, kokiais?

R1. Susiduriama su tarptautinio bendradarbiavimo problematika, t. y. ilgais vykdymo terminais. Dažnu atveju, pateikiant Teisinės pagalbos prašymą ar Europos tyrimo orderį, prašomų duomenų laukiama ilgą laiką, dėl ko prarandama galimybė gauti ir kitus duomenis. Kaip ir minėta aukščiau, aptariami nusikaltimai vykdomi iš įvairių pasaulio šalių ir tų, su kuriomis Lietuva net neturi tarptautinio bendradarbiavimo sutarčių. Pažymėtina, kad skirtingose užsienio šalyse skiriasi duomenų saugojimo (telefonu priklausomybių, IP priklausomybių) terminai, dėl ko pasitaiko atvejai, kuomet prašomi duomenys jau nėra išlikę. Žinoma darbą apsunkina ir privačių įstaigų teikiamos informacijos ribojimai, pvz. įmonės, kurios teikia VPN paslaugas, dažnu atveju neteikia duomenis apie klientus, kurie užsisakė VPN (*Virtual Private Network* – virtualus privatus tinklas) paslaugą.

R2. Taip, praktikoje kartais susiduriama su tam tikrais sunkumais bendradarbiaujant tiek nacionaliniu, tiek tarptautiniu lygmeniu. Nacionaliniu mastu iššūkių gali kilti dėl skirtingų institucijų informacinių sistemų nesuderinamumo ar lėtesnio informacijos apsikeitimo. Taip pat kartais trūksta aiškesnio procesų koordinavimo tarp skirtingų institucijų. Tarptautiniu lygmeniu pagrindiniai sunkumai susiję su skirtingais teisiniais reglamentais, duomenų perdavimo ribojimais ir skirtingu tyrimų prioritetų nustatymu. Be to, bendradarbiavimą gali apsunkinti kalbos barjerai ir laiko skirtumai. Nepaisant to, per pastaruosius metus bendradarbiavimas gerėja, ypač per Europolo ir kitų tarptautinių organizacijų mechanizmus.

R3. Taip, praktikoje pasitaiko sunkumų, ypač bendradarbiaujant tarptautiniu mastu. Dažniausios problemos – ilgas informacijos gavimo procesas iš užsienio platformų ar institucijų, jurisdikcijų skirtumai ir duomenų apsaugos ribojimai.
R4. Taip, praktikoje tokių sunkumų pasitaiko. Nacionaliniu lygmeniu dažniausiai susiduriama su duomenų gavimo terminais, skirtinga įstaigų praktika, techninių duomenų saugojimo terminais ir ne visada pakankamai greitu informacijos pateikimu. Kai kuriuose tyrimuose laikas yra labai svarbus, nes elektroniniai duomenys, prisijungimų žurnalai, IP adresų naudojimo informacija ar kiti techniniai duomenys gali būti saugomi ribotą laiką. Tarptautiniu lygmeniu sunkumų kelia tai, kad daug paslaugų teikėjų, platformų, serverių ar finansinių tarpininkų veikia užsienyje. Duomenų gavimas priklauso nuo konkrečios valstybės teisinio reguliavimo, tarptautinės teisinės pagalbos procedūrų, platformų vidinių taisyklių ir atsakymo terminų. Dėl to tyrimai gali užtrukti, o kai kurie duomenys gali būti jau ištrinti arba nepasiekiami.

R5. Ne, tik bendradarbiavimas nacionaliniu ar tarptautiniu lygmeniu užtrunka ilgiau.
R6. Taip, daugiausiai sunkumų atsiranda bendradarbiaujant su kitų šalių institucijomis, kadangi informacijos keitimasis užtrunka tikrai ilgai.
R7. Praktikoje dažnai kyla sunkumų bendradarbiaujant tarptautiniu mastu. Dalis duomenų saugomi užsienio serveriuose, todėl informacijos gavimas užtrunka dėl skirtingų valstybių teisinių procedūrų. Taip pat problemų kelia skirtingas valstybių požiūris į duomenų apsaugą bei ribotos galimybės greitai identifikuoti anoniminius asmenis internete. Nacionaliniu lygmeniu bendradarbiavimas dažniausiai vyksta sklandžiau, tačiau kartais trūksta operatyvaus keitimosi informacija tarp institucijų.
R8. Taip. Dažnai tenka bendradarbiauti tarptautiniu lygmeniu, kadangi kompiuterinius nusikaltimus asmenys gali atlikti iš viso pasaulio. Siekiant gauti tyrimui reikšmingos informacijos iš užsienio, tenka labai ilgai laukti, pavyzdžiui Europos tyrimo orderio tenka laukti daugiau nei pusę metų. Tyrimams svarbi informacija (telefono numerio išklotinės, IP adresai) saugomi tik tam tikrą laiką, todėl visada yra rizika prarasti reikšmingus duomenis, laukiant ilgai atsakymo iš kitų užsienio institucijų. Nacionaliniu lygmeniu tarp institucijų bendradarbiauti yra paprasčiau.
R9. Vienintelis iššūkis tai, kad bendradarbiavimas su užsienio šalimis yra gan sudėtingas, dėl skirtingų jurisdikcijų, duomenų apsaugos taisyklių. Be to, tai yra ilgas procesas.

T. Kaip vertinate Lietuvoje vykdomas prevencines priemones, siekiant sumažinti kompiuterinių nusikaltimų skaičių? Ar, Jūsų nuomone, jos yra veiksmingos ir ar jų yra pakankamai?
R1. Lietuvoje vykdomas prevencines priemones vertimu teigiamai, tačiau kaip rodo praktika, mano aukščiau minėtų nusikalstamų veikų, kurios šiuo metu vyrauja (LR K 182 str. ir 198^1 str.),

sumažejimui šiam momentui didelės įtakos nėra. Matyti, kad nusikalstamas veikas vykdantys asmenys prisitaiko prie pokyčių, kurie įvyksta ir bet kokiu atveju suranda „spragas“, kurios leidžia jiems įvykdyti nusikaltimą. Manau, kad nėra pakankamas vien Lietuvos policijos įdirbis prevencijoje, prie to turi prisijungti ir finansų įstaigos, telekomunikacijos tinklų operatoriai.

R2. Lietuvoje vykdomos prevencinės priemonės, skirtos kompiuterinių nusikaltimų mažinimui, mano nuomone, yra gana įvairios ir nuosekliai tobulinamos. Vykdomos informacinės kampanijos, švietimas apie kibernetinį saugumą, taip pat stiprinamas institucijų bendradarbiavimas ir incidentų prevencija. Šios priemonės prisideda prie visuomenės sąmoningumo didinimo ir padeda sumažinti dalį paprastų sukčiavimo atvejų. Tačiau, atsižvelgiant į sparčiai augantį kibernetinių nusikaltimų mastą ir jų sudėtingumą, prevencinių priemonių ne visada pakanka. Ypač trūksta nuolatinio visuomenės švietimo ir platesnio verslo sektoriaus įtraukimo.

R3. Prevencinės priemonės vykdomos, tačiau jų vis dar nepakanka. Informacinės kampanijos ir visuomenės švietimas yra naudingi, tačiau dalis gyventojų vis tiek išlieka pažeidžiami sukčiavimo schemoms. Prevencija turėtų būti aktyvesnė ir labiau orientuota į praktinį žmonių mokymą.

R4. Prevencines priemones vertinu teigiamai, tačiau manyčiau, kad jų nepakanka. Lietuvoje vykdomos įvairios informacinės kampanijos, policija ir kitos institucijos viešina įspėjimus apie sukčiavimo schemas, teikia rekomendacijas dėl saugaus elgesio internete. Tokios priemonės yra reikalingos ir daliai visuomenės padeda atpažinti grėsmes. Vis dėlto praktikoje matyti, kad nusikaltėliai labai greitai prisitaiko, keičia schemas, naudoja vis įtikinamesnius pranešimus, netikras svetaines, suklastotas paskyras ir psichologinį spaudimą. Todėl vienkartinių ar bendro pobūdžio kampanijų neužtenka. Prevencija turėtų būti nuosekli, nuolat atnaujinama ir orientuota į konkrečias rizikos grupes – vaikus, vyresnio amžiaus asmenis, verslą, viešąjį sektorių ir aktyvius elektroninės bankininkystės naudotojus.

R5. Šiuo metu Lietuvoje vykdomos prevencinės priemonės prieš kompiuterinius nusikaltimus tapo profesionalesnės. Dabar jau po truputi tampa kryptingos ir iš dalies veiksmingos, tačiau dar nėra visiškai pakankamos, nes kibernetinės grėsmės auga greičiau nei visuomenės ir organizacijų pasirengimas. Nors anksčiau tikrai nebuvo vykdomos prevencinės priemonės dėl kompiuterinių nusikaltimų.

R6. Vertinu teigiamai, bet, mano nuomone, trūksta didesnio visuomenės švietimo, informavimo apie savo duomenų saugojimą, saugumo taisykles internete. Tiek vyresnio, tiek jaunesnio amžiaus asmenis būtina nuolat informuoti būti atsargiems.

R7. Lietuvoje vykdomos prevencinės priemonės, tokios kaip visuomenės informavimo kampanijos, įspėjimai apie sukčiavimo būdus, mokymai bei institucijų bendradarbiavimas, yra

naudingos ir reikalingos. Vis dėlto jų vis dar nepakanka, nes dalis visuomenės išlieka nepakankamai informuota apie kibernetines grėsmes. Prevencijos efektyvumą būtų galima didinti aktyviau šviečiant gyventojus nuo ankstyvo amžiaus ir dažniau organizuojant praktinius mokymus.

R8. Juridiniai asmenys, ypač valstybinės institucijos manau gan atsakingai žiūri į kibernetinį saugumą ir taiko aukščiausio standarto saugumo priemones. Lietuvos policija, bankai, žiniasklaida ir kitos institucijos tikrai dažnai informuoja piliečius apie kibernetinio saugumo grėsmes ir kaip nuo jų apsisaugoti. Nuolatos kuriami straipsniai šia tema, bankai asmeniškai savo klientams nuolat siunčia įspėjimus ir priminimus saugoti savo asmeninius duomenis, neatskleisti jų tretiesiems asmenims. Šios priemonės yra labai gerai, nes piliečiams visada yra primenama būti atsargiems. Bet šių priemonių manau yra nepakankamai ir jos nepakankamai intensyviai vykdomos, kadangi vis tiek žmonių informuotumas apie kompiuterinius nusikaltimus, jų grėsmes, yra nepakankamas.

R9. Lietuvos policija dažnai užsiima švietėjiška veikla, tiek socialiniuose tinkluose, tiek fiziškai, nuolat stengiamasi informuoti visuomenę apie galimas grėsmes, sukčiavimo būdus. Taip pat, bankai, mobilaus ryšio operatoriai nuolat siunčia priminimus apie sukčiavimo atvejus ir kaip nepakliūti į sukčių pinkles. Prevencijos priemones Lietuvoje vertinu teigiamai, tačiau jų yra nepakankamai, nes nusikalstamų veikų vis tiek daugėja, jos tampa vis profesionaliau atliekamos, todėl būtina investuoti daugiau resursų į prevenciją.

T. Kokias priemones, Jūsų nuomone, reikėtų taikyti Lietuvoje siekiant stiprinti kompiuterinių nusikaltimų prevenciją?

R1. Skatinti asmenų sąmoningumą, ugdyti kompiuterinį raštingumą, įprotį laikytis saugumo priemonių (laikytis duomenų privatumo, sunkesnių slaptažodžių naudojimo, nesilankyti įtartinuose svetainėse). Skatinti bendradarbiavimą tarp institucijų dėl operatyvaus apsikeitimo informacija bei galimo nusikaltimų užkardymo. Griežtinti finansų įstaigų veiklos reglamentavimą.

R2. Siekiant stiprinti kompiuterinių nusikaltimų prevenciją Lietuvoje, pirmiausia reikėtų didinti visuomenės kibernetinį raštingumą, nuolat vykdant švietimo kampanijas mokyklose, viešajame sektoriuje ir tarp vyresnio amžiaus žmonių. Taip pat svarbu stiprinti įmonių ir valstybinių institucijų kibernetinio saugumo standartus, diegiant pažangesnes apsaugos technologijas ir reguliariai atliekant sistemų saugumo auditus. Be to, reikėtų plėsti specialistų rengimą kibernetinio saugumo srityje ir užtikrinti nuolatinį jų kvalifikacijos kėlimą. Svarbi priemonė yra ir glaudesnis nacionalinių bei tarptautinių institucijų bendradarbiavimas, greitesnis keitimasis informacija apie grėsmes.

R3. Reikėtų stiprinti visuomenės švietimą apie kibernetinį saugumą nuo ankstyvo amžiaus, dažniau organizuoti prevencines kampanijas, investuoti į specialistų rengimą bei technines priemones. Taip pat svarbu stiprinti tarptautinį bendradarbiavimą ir greitesnį keitimąsi informacija.

R4. Reikėtų stiprinti visuomenės skaitmeninį raštingumą ir praktinį mokymą, kaip atpažinti sukčiavimo schemas, netikras nuorodas, suklastotus prisijungimo puslapius, investicinio sukčiavimo požymius ir kitus pavojus. Prevencija turėtų būti ne teorinė, o paremta realiais pavyzdžiais iš praktikos. Taip pat reikėtų daugiau dėmesio skirti mokykloms, senjorams, smulkiajam verslui ir viešojo sektoriaus darbuotojams. Svarbu skatinti dviejų veiksnių autentifikavimą, saugių slaptažodžių naudojimą, reguliarius duomenų atsarginių kopijų darymus, atsargumą naudojantis elektronine bankininkyste ir socialiniais tinklais. Be to, būtų tikslinga stiprinti institucijų, bankų, elektroninių ryšių paslaugų teikėjų, platformų ir policijos bendradarbiavimą, kad į įtartinus veiksmus būtų reaguojama greičiau. Reikalingos ir aiškesnės procedūros, leidžiančios operatyviai išsaugoti reikšmingus elektroninius duomenis, kol jie dar nėra ištrinti. Prevencija turėtų būti nuolatinis procesas, o ne tik reakcija į jau įvykusius nusikaltimus.

R5. Labai reikia stiprinti visuomenės švietimą, gerinti specialistų rengimą, gerinti ar modernizuoti įrangas, stiprinti įmonių ir institucijų apsaugą, investuoti į modernias technologijas. tobulinti įstatymus.

R6. Užtikrinti, kad įmonės turėtų geresnes ir patikimesnes apsaugos sistemas, kad grėsmę pavyktų identifikuoti iš anksto, o ne tada, kai žala jau yra padaryta. Daugiau informuoti visuomenę kaip apsisaugoti nuo kompiuterinių nusikaltimų.

R7. Siekiant stiprinti kompiuterinių nusikaltimų prevenciją Lietuvoje, reikėtų daugiau investuoti į visuomenės skaitmeninį raštingumą ir specialistų rengimą. Taip pat svarbu stiprinti tarptautinį bendradarbiavimą, modernizuoti technines tyrimo priemones ir užtikrinti greitesnį informacijos apsikeitimą tarp institucijų. Be to, naudinga būtų dažniau vykdyti prevencines kampanijas apie sukčiavimo schemas, socialinę inžineriją bei saugų elgesį internete.

R8. Reikėtų jau mokyklinio amžiaus asmenims diegti žinias apie kibernetinį saugumą, plėsti žinias kaip apsisaugoti nuo intenete esančių grėsmių. Įmonėms organizuoti daugiau mokymų apie kibernetinį saugumą. Šviesti žmones apie antivirusinių programų naudojimą, sudėtingų slaptažodžių naudojimą. Įmonės ir institucijos turėtų nuolatos atlikti sistemų saugumo testavimus, investuoti į specialistų rengimą, darbuotojų mokymus. Didelį dėmesį skirti vyresnio amžiaus asmenimis, kurie dažnai nukenčia nuo įvairių sukčiavimo atvejų.

R9. Tiek fiziniams, tiek juridiniams asmenims organizuoti daugiau mokymų paremtų praktika, o ne teorija, skatinti žmonių budrumą internetinėje erdvėje, gilinti žmonių žinias kaip atliekami kompiuteriniai nusikaltimai.

Apibendrinant respondentų atsakymus, tik keli ikiteisminio tyrimo tyrėjai teigė pastebėję išaugusį kompiuterinių nusikaltimų skaičių, tačiau visi tyrėjai akcentavo, kad kompiuterinių nusikaltimų pobūdis per pastaruosius metus pasikeitė – šios nusikalstamos veikos tapo sudėtingesnės, profesionalesnės ir labiau organizuotos. Taip pat, padaugėjo išpirkos reikalaujančių išpuolių, duomenų vagysčių ir prisijungimo perėmimo atvejų, o nusikaltėliai vis dažniau naudoja anonimiškumą užtikrinančias priemones, socialinės inžinerijos metodus bei netikras paskyras, dėl ko šių nusikalstamų veikų tyrimas tampa sudėtingesnis.

Visi ikiteisminio tyrimo tyrėjai vieningai pabrėžė spartų informacinių technologijų vystymąsi kaip vieną pagrindinių veiksnių, lemiančių kompiuterinių nusikaltimų plitimą. Tyrėjų nuomone, nuolat tobulėjančios informacinės technologijos ne tik sudaro palankesnes sąlygas nusikalstamų veikų vykdymui, bet ir sudaro galimybes jiems veikti sudėtingesniais ir efektyvesniais būdais. Dauguma tyrėjų taip pat pabrėžė ir finansinę naudą, kuri skatina nusikaltėlius atlikti tokio pobūdžio nusikalstamas veikas, globalizaciją – kuri suteikia galimybę kompiuterinius nusikaltimus daryti iš bet kurios pasaulio vietos bei neatsargų interneto vartotojų elgesį ir nepakankamą jų informuotumą apie šias nusikalstamas veikas. Tik keli tyrėjai išskyrė dirbtinio intelekto įtaką, nurodydami, kad ši sritis pasitelkiama sudėtingesnėms nusikalstamoms schemos vykdyti bei socialinės inžinerijos metodams tobulinti.

Dauguma tyrėjų Lietuvos policijos ikiteisminio tyrimo tyrėjų kompetenciją tiriant kompiuterinius nusikaltimus įvertino teigiamai ir pabrėžė, kad kvalifikacija yra nuolat tobulinama dalyvaujant įvairiuose mokymuose bei kvalifikacijos kėlimo programose. Beveik visi tyrėjai akcentavo, kad didžiausia problema yra ne techninių galimybių ar pareigūnų kvalifikacijos stoka, bet nepakankamas kvalifikuotų tyrėjų skaičius.

Respondentų atsakymai atskleidė, kad praktikoje bendradarbiaujant su kitomis institucijomis sunkumų dažniausiai kyla tarptautiniu lygmeniu. Didžioji dalis tyrėjų pagrindinę problemą išskyrė ilgą informacijos gavimo procesą, skirtingus valstybių teisinius reglamentus, duomenų apsaugos ribojimus. Nacionaliniu lygmeniu bendradarbiavimas vyksta sklandžiau ir greičiau, susiduriama tik su pavienėmis organizacinio pobūdžio problemomis ar ilgesniu informacijos gavimo procesu.

Visi respondentai Lietuvoje taikomas kompiuterinių nusikaltimų prevencijos priemones vertina teigiamai. Tyrėjų nuomone, pastaraisiais metais prevencinės priemonės tapo aktyvesnės ir nuosekliau vystomos – organizuojami įvairūs mokymai, visuomenės informavimas tapo dažnesnis. Tačiau visi respondentai akcentavo, kad taikomų prevencijos priemonių vis dar

nepakanka. Tyrėjai pabrėžė, kad didžiausias dėmesys turėtų būti skiriamas visuomenės švietimui ir skaitmeninio raštingumo stiprinimui, kadangi kompiuterinių nusikaltimų prevencija pirmiausia turi būti grindžiama visuomenės gebėjimu atpažinti galimas kibernetines grėsmes bei mokėjimu saugiai elgtis elektroninėje erdvėje. Todėl prevencijos priemonės turi būti ne vienkartinės, o tęstinio pobūdžio, o saugaus elgesio igūdžiai internete formuojami nuo ankstyvo amžiaus

IŠVADOS

1. Kompiuterinių nusikaltimų sąvoka mokslinėje literatūroje ir teisės aktuose aiškinama nevienodai, tačiau Lietuvos įstatymuose, kompiuteriniai nusikaltimai apibrėžiami Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“. Kompiuterinių nusikaltimų teisinis reglamentavimas Lietuvoje formavosi palaipsniui, o reikšmingą įtaką jo raidai turėjo Budapešto Konvencija bei Europos Sąjungos teisės aktai.

2. Kompiuterinių nusikaltimų skaičius 2020 – 2025 m. laikotarpiu Lietuvoje išaugo 40,7 %. Didžiausią dalį registruotų kompiuterinių nusikalstamų veikų sudarė neteisėtas prisijungimas prie informacinės sistemos. Kompiuterinių nusikaltimų augimo tendencijos pastebimos ir pasauliniu mastu.

3. Remiantis Lietuvoje registruotų kompiuterinių nusikaltimų 2020 – 2025 m. statistiniais duomenimis, tipinis asmuo, padaręs kompiuterinį nusikaltimą yra vyras, 30 – 39 m. amžiaus asmuo, pagrindinį ir vidurinį išsilavinimą turintis asmuo bei nedirbantis ar bedarbis.

2020 – 2025 m. statistiniais duomenimis, kompiuterinių nusikaltimų aukomis dažniausiai tampa moterys, 40 – 59 m. amžiaus asmenys, turintys aukštąjį išsilavinimą asmenys. Tokių nusikalstamų veikų atveju nusikaltėlio ir aukos ryšys dažniausiai nėra grindžiamas asmeniniais ar socialiniais ryšiais. Nusikaltėlis dažniausiai pasirenka savo auką atsižvelgdamas į esamas galimybes, motyvaciją ir techninę apsaugą.

4. Svarbiausias kompiuterinių nusikaltimų veiksnys yra sparčiai besivystančios informacinės technologijos. Didėjantis kompiuterių, interneto ir skaitmeninių paslaugų naudojimas sudaro galimybes nusikaltėliams pasiekti didelį potencialių aukų skaičių, o nuolatinė technologinė pažanga, įskaitant dirbtinį intelektą, suteikia galimybes vykdyti sudėtingesnes ir įvairiasnes kompiuterines nusikalstamas veikas.

5. Veiksminga kompiuterinių nusikaltimų prevencija ir kontrolė reikalauja kompleksinių priemonių taikymo. Lietuvos teisėsaugos institucijos ir kitos įstaigos labiausiai orientuotos į visuomenės švietimą, informavimą apie galimas grėsmes, saugų elgesį elektroninėje erdvėje ir dažniausiai taikomus kompiuterinių nusikaltimų metodus.

PASIŪLYMAI

Švietimo, mokslo ir sporto ministerijai:

Bendrojo ugdymo mokyklose į informatikos programas įtraukti atskiras temas apie saugių slaptažodžių kūrimą, fišingo atpažinimą, asmens duomenų apsaugą ir saugų naudojimąsi socialiniais tinklais.

Lietuvos policijos departamentui:

Nustatyti privalomus periodinius kvalifikacijos kėlimo mokymus kompiuterinių nusikalstamų veikų tyrėjams ne rečiau kaip kartą per metus.

Viešojo ir privataus sektoriaus subjektams:

Įdiegti dviejų veiksnių autentifikavimo priemones darbuotojų naudojamose sistemose bei ne rečiau kaip kartą į metus organizuoti praktinius darbuotojų mokymus

LITERATŪRA

Teisės aktai:

1. „2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų (Žin., 2004, Nr. 36-1188)“. Infolex. Žiūrėta 2025 m. rugsėjo 15 d. https://www-infolex-lt.skaitykla.mruni.eu/ta/84371#B_0.
2. „Lietuvos Respublikos baudžiamasis kodeksas (Žin., 2000, Nr. 89-2741)“. Redakcija Nr. 4. Infolex. Žiūrėta 2025 m. rugsėjo 15 d. https://www-infolex-lt.skaitykla.mruni.eu/ta/66150:ver4.
3. „Lietuvos Respublikos baudžiamasis kodeksas (Žin., 2000, Nr. 89-2741), redakcija Nr. 121. Infolex. Žiūrėta 2025 m. rugsėjo 15 d. https://www-infolex-lt.skaitykla.mruni.eu/ta/66150:ver121.
4. „2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš
   informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR“. EUR – Lex. Žiūrėta 2026 m. sausio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32013L0040.
5. „Dėl Lietuvos tarybų socialistinės Respublikos baudžiamojo kodekso patvirtinimo“. Vyriausybės žinios. Žiūrėta 2026 m. gegužės 9 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.20465/jxfupAglbe.
6. „Lietuvos Respublikos baudžiamasis kodeksas (Žin., 2000, Nr. 89-2741)“. 1 Redakcija. Infolex. Žiūrėta 2026 m. gegužės 4 d. https://www-infolex-lt.skaitykla.mruni.eu/ta/66150:ver1.
7. „Įsakymas dėl Lietuvos Respublikos Krašto apsaugos ministro valdymo sričių 2026 – 2028 metų strateginio veiklos plano patvirtinimo“. Lietuvos Respublikos Krašto apsaugos ministerija. Žiūrėta 2026 m. gegužės 4 d. https://kam.lt/wp-content/uploads/2026/03/2026-2028-m.-SVP-2026-02-26-Nr.-V-172.pdf.
8. „Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)“. Official Journal of the European Union. Žiūrėta 2026 m. gegužės 4 d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

Specialioji literatūra:

9. Petrauskas, Rimantas ir Darius Štitilis. *Kompiuteriniai nusikaltimai ir jų prevencija: mokomasis leidinys parengtas pagal Tempus Phare projektą „Valstybės pareigūnų rengimas teisinės sistemos reformai Lietuvoje*. Vilnius: LTA Leidybos centras, 2000.
10. Kalpokas, Vaidas. „Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos“, *Teisės problemos* 1, 63 (2009). https://teise.org/wp-content/uploads/2023/01/2009-1-kalpokas.pdf.
11. Starkus Saulius. „Kriminologiniai Kompiuterizacijos Aspektai”. *Jurisprudencija* 20 (2001): 85-92. https://talpykla.elaba.lt/elaba-fedora/objects/elaba:2706487/datastreams/MAIN/content.
12. Štitilis, Darius. *Elektroniniai nusikaltima*i. Vilnius: Mykolo Romerio universitetas, 2011.
13. Marcinauskaitė, Renata. „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 1981 straipsniai)“. Daktaro disertacija, Mykolo Romerio universitetas, 2013.
14. Marcinauskaitė, Renata. *Nusikalstamos veikos elektroninėje erdvėje :elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje: monografija*. Vilnius: Registrų centras, 2019. https://cris.mruni.eu/cris/entities/publication/c9e5a17d-3878-4db2-ae66-89f31fb5bbc5.
15. Holt, Thomas J. ir Adam M. Bossler. *Cybercrime in Progress: Theory and Preventon of Technology – Enabled Offenses.* Niujorkas: Routledge, 2016. https://www.taylorfrancis.com/books/mono/10.4324/9781315775944/cybercrime-progress-thomas-holt-adam-bossler.
16. Brewer, Russell, Mellisa de Vel – Palumbo, Alice Hutchhings ir David Maimon. *Cybercrime Prevention: Theory and Applications.* Palgrave, 2019. https://www.researchgate.net/publication/337296521_Cybercrime_Prevention_Theory_and_Applications.
17. Li, Xingan. „A Review of Motivations of Illegal Cyber Activities“. *Kriminologija ir socialinė integracija* 25, 1 (2017). https://hrcak.srce.hr/file/266976.
18. Karne, Rahul, Akhil Dudhipala ir Pavan Kumar Pativada. „Cybercrime in India: Legal Frameworks, Emerging Threats, and the Role of AI in Detection and Defence“. *International Journal of Novel Research and Development* 10, 4 (2025). https://www.researchgate.net/publication/392367232_CYBERCRIME_IN_INDIA_LEGAL_FRAMEWORKS_EMERGING_THREATS_AND_THE_ROLE_OF_AI_IN_DETECTION_AND_DEFENCE.

19. AllahRakha, Naeem. „Legal Frameworks for AI – Driven Cybercrime Prevention“. *Uzbek Journal of Law and Digital Policy* 2, 6 (2024). https://www.researchgate.net/publication/399194690_Challenges_in_Regulating_and_Prosecuting_AI_Model_Poisoning_as_Cybercrime.
20. Syed, Shoeb Ali. „AI – Powered Cybercrime: The New Frontier of Digital Threats“. *International Journal of Engineering Technology Research & Management* 6, 2 (2022). https://www.researchgate.net/publication/390441717_AI-POWERED_CYBERCRIME_THE_NEW_FRONTIER_OF_DIGITAL_THREATS.
21. Leverett, Eireann ir Aaron Kaplan. „Towards Estimating the Untapped Potential: A Global Malicious DDoS Mean Capacity Estimate“. *Journal of cyber policy* 2, 2 (2017). https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1362020.
22. Rajput, Nikhil ir Dhaval Chudasama. „Protecting Ourselves from Digital Crimes“. *National Journal of Cyber Security Law* 4, 1 (2021). https://www.researchgate.net/publication/352507646_Protecting_Ourselves_from_Digital_Crimes.
23. Kiškis, Mindaugas, Rimantaa Petrauskas, Irmantas Rotomskis ir Darius Štitilis. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006.

    Higgins, George. *Cybercrime. An introduction to an Emerging Phenomenon.* New York: McGraw-Hill, 2010.
24. Littlejohn Shinder, Debra. *Scene of the Cybercrime: Computer forensics handbook*. Rockland: Syngress Publishing, 2002.
25. Grigaitytė, Ugnė ir Miglė Mackevičiūtė. „Nusikaltimai virtualioje erdvėje- šiuolaikiniai iššūkiai ir prevencijos galimybės“. *Teisės mokslo pavasaris* Nr. 4, (2020): 276. https://www.zurnalai.vu.lt/openseries/article/view/21070/20214.
26. Asghar, Muhammad Umar, Muhammad Hassan Javed ir Sumia Azhar. „The regulation of Cybercrime in Internation Law: Discussing the Legal Frameworks and Challenges in Regulating Cybercrime“. *Indus Journal of Social Sciences* 3, 2 (2025): 418. https://www.researchgate.net/publication/391623650_The_Regulation_of_Cybercrime_in_International_Law_Discussing_the_Legal_Frameworks_and_Challenges_in_Regulating_Cybercrime.
27. Bucaj, Enver ir Kenan Idrizaj. „The need for cybercrime regulation on a global scale by the international law and cyber convention“. *Multidisciplinary Reviews* 8, 1 (2024): 4. https://www.researchgate.net/publication/385089998_The_need_for_cybercrime_regulation_on_a_global_scale_by_the_international_law_and_cyber_convention.

28. Sauliūnas, Darius. „Legislation On Cybercrime In Lithuania: Development and legal gaps in Comparison With The Convention On Cybercrime“. *Jurisprudencija* 4, 122 (2010): 207. https://ojs.mruni.eu/ojs/jurisprudence/article/view/1034/989.
29. Kiškis, Alfredas. „Nusikalstamumas Lietuvoje: ko neparodo oficialioji statistika?“. *Mokslo darbai* 11, 113 (2008): 114–123. https://www.researchgate.net/publication/289525848_Nusikalstamumas_Lietuvoje_ko_neparodo_oficialioji_statistika.
30. Babachinaitė, Genovaitė, Alfredas Kiškis, Jūratė Galinaitytė, Gitana Jurgelaitienė, Aistė Kuolaitė, Brigita Palavinskienė, Arūnas Paukštė, Artūras Petkus, Aida Raudonienė, Tomas Rudzkis ir Rokas Uscila. *Kriminologija: vadovėlis.* Vilnius: Mykolo Romerio universitetas, 2010.
31. Kalpokas, Vaidas ir Renata Marcinauskaitė. „Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas“. *Teisės problemos* 3, 77 (2012): 30-52. https://teise.org/wp-content/uploads/2023/01/Kalpokas-Marcin.-TP2012_3.pdf.
32. Ortiz, Arianna E. ir Rohitha Goonatilake. „Rise of Computer – Related Crimes: Loss of Data, Infrastructures and Monetary Assets“. *European Journal of Applied Sciences* 14, 1 (2026): 482. https://www.researchgate.net/publication/400598389_Rise_of_Computer-Related_Crimes_Loss_of_Data_Infrastructures_and_Monetary_Assets.
33. Li, Li, Zhimin Niu, Liangqing Wang, Mark Griffiths ir Songli Mei. „Do Men Have More Cyber- Deviant Behaviours? A Network Analysis Based on the Reciprocal Determinism Model“. *Deviant Behaviour*, (2025): 2-3. https://www.tandfonline.com/doi/full/10.1080/01639625.2025.2562117?scroll=top&needAccess=true#d1e940.
34. Aiken, Mary, Julia Davidson ir Philip Amann. *Youth Pathways into Cybercrime.* Haga: 2016. https://www.europol.europa.eu/cms/sites/default/files/documents/pathways-white-paper.pdf.
35. Leukfeldt, Eric Rutger ir Majid Yar. „Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis“. *Deviant Behavior* 37, 3 (2016): 3 – 4. https://www.researchgate.net/publication/286923434_Applying_Routine_Activity_Theory_to_Cybercrime_A_Theoretical_and_Empirical_Analysis.
36. Ali, Al - Nafisa Shaden ir Yahya Moubarak Khatabeh. „Social Engineering as an Intermediate Variable between Methods of Persuasion and Electronic Deception from the Point of View of Victims of Cybercrime. *Journal of Posthumanism* 5, 6 (2025): 1015 – 1016.

https://www.researchgate.net/publication/392222941_Social_Engineering_as_an_Intermediate_Variable_between_Methods_of_Persuasion_and_Electronic_Deception_from_the_Point_of_View_of_Victims_of_Cybercrime.

37. Maryja Šupa. „Socialiniai tyrimai apie elektroninius nusikaltimus: globalus temų diapazonas ir Lietuvoje atliktų tyrimų sisteminė analizė“. *Kriminologijos studijos* 9 (2021): 12 – 13. https://www.zurnalai.vu.lt/kriminologijos-studijos/lt/article/view/24959/24255.
38. Mallidi, S. Kumar Reddy ir Ravi Kiran Varma Penmatsa. „Optimizing Decision Tree for Multi – class VPN and Non – VPN Traffic Classification using BBFS – PSO“. *PeerJ Computer Science* 12 (2026): 2 – 3. https://www.researchgate.net/publication/403538591_Optimizing_decision_trees_for_multi-class_VPN_and_non-VPN_traffic_classification_using_BBFS-PSO.
39. Debbarma, Rupali. „The Legal Framework And Challenges In Prosecuting Cybercrimes Including Hackings, Identity Theft, and Online Fraud. *Res Militaris* 13, 2 (2023): 22. https://www.researchgate.net/publication/399408186_The_Legal_Framework_And_Challenges_In_Prosecuting_Cybercrimes_Including_Hacking_Identity_Theft_And_Online_Fraud.
40. Libicki, Martin C. C*risis and Escalation in Cyberspace.* Santa Monica, RAND Corporation, 2012. https://www.jstor.org/content/pdf/oa_book_monograph/10.7249/j.ctt24hrx7.pdf?refreqid=fastly-default%3A04b6dd4612bf0187868d714c17bd7ac9&ab_segments=&initiator=&acceptTC=1,
41. Ogunleye, Yetunde O., U. Ojedokun ir A. A. Aderinto. „Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria“. *International Journal of Cyber Criminology* 13, 2 (2020): 309 – 310. https://www.researchgate.net/publication/339941723_Pathways_and_Motivations_for_Cyber_Fraud_Involvement_among_Female_Undergraduates_of_Selected_Universities_in_South-West_Nigeria.
42. Sakalauskas, Gintautas, Skirmantas Bikelis, Vaidas Kalpokas ir Aušra Pocienė. *Baudžiamoji politika Lietuvoje: tendencijos ir lyginamieji aspekta* Vilnius: Teisės institutas. https://teise.org/wp-content/uploads/2012/10/Baudziamoji-politika-Lietuvoje.pdf.

43. Narasimhan, Premanand ir Kala Baskar. „Securing the Metaverse: AI – Driven Solutions for Cyber Security, Privacy and User Trust“. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 10, 6 (2024): 1891 – 1892. https://www.researchgate.net/publication/387377644_Securing_the_Metaverse_AI-Driven_Solutions_for_Cyber_Security_Privacy_and_User_Trust.
44. Adepu, Rajesh. „Autonomous Cyber Defense Systems Powered by AI for Enterprise Cloud Enviroments“. *International Journal of Computer Engineering and Technology* 17, 2 (2026): 25 – 26. https://www.researchgate.net/publication/403909469_AUTONOMOUS_CYBER_DEFENSE_SYSTEMS_POWERED_BY_AI_FOR_ENTERPRISE_CLOUD_ENVIRONMENTS.
45. Soni, Nitin ir Rakesh Poonia. „AI – Driven Open – Source Intelligence in Digital Forensics for Cybercrime Investigation“. *Journal of Collective Sciences and Sustainability* 1 (2025): 2 – 3. https://www.researchgate.net/publication/393924645_AI-driven_open-source_intelligence_in_digital_forensics_for_cybercrime_investigation
46. Nshimiyimana, Francois Regis. „Adapting the Budapest Convention to Address Emerging Cyber Threats“. *Belugyi Szemle* 74, 1 (2026): 187. https://www.researchgate.net/publication/400408531_Adapting_the_Budapest_Convention_to_address_emerging_cyber_threats.
47. Bannelier, Karine. „Risks and Opportunities of the UN Cybercrime Convention for the UNTOC & The Fight Against Transnational Organized Crime: A First Assessment“. *Transnational Criminal Law Review* 4, 1 (2025): 142. https://www.researchgate.net/publication/394799916_Risks_and_Opportunities_of_the_UN_Cybercrime_Convention_for_the_UNDOC_the_Fight_Against_Transnational_Organised_Crime_A_First_Assessment?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6ImhvbWUiLCJwYWdlIjoic2VhcmNoIiwicG9zaXRpb24iOiJwYWdlSGVhZGVyIn19.
48. Wibowo, Budi, Luqman Hafiz ir Taufik Hidayat. „Unveiling the Cybercrime Ecosystem: Impact of Ransomware – as – a – Service (RaaS) in Indonesia“. *International Journal of Science Education and Cultural Studies* 4, 1 (2025): 17. https://www.researchgate.net/publication/389501930_Unveiling_the_Cybercrime_Ecosystem_Impact_of_Ransomware-as-a-Service_RaaS_in_Indonesia.
49. Vemula, Vamshidhar Reddy. „AI – Powered Framework for Proactive Monitoring of Dark Web Marketplaces and Prediction of Emergent Cybercrime Trends“. *FMDB Transactions on Sustainable Computer Letters* 3, 3 (2025): 127. https://www.researchgate.net/publication/397563566_AI-

Powered_Framework_for_Proactive_Monitoring_of_Dark_Web_Marketplaces_and_Prediction_of_Emergent_Cybercrime_Trends

Statistiniai duomenys:

50. „Nuolatinių gyventojų skaičius metų pradžioje“. Oficialiosios statistikos portalas. Žiūrėta 2026 m. kovo 22 d. https://osp.stat.gov.lt/statistiniu-rodikliu-analize?indicator=S3R166#/.
51. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos. „Užregistruotos nusikalstamos veikos Lietuvoje”. Informatikos ir ryšių departamentas. Žiūrėta 2026 m. kovo 16 d. https://www.ird.lt/lt/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos-3/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos-2/nusikalstamos-veikos-lietuvoje-2006-2025-metais-2.
52. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos. „Nusikalstamumo duomenų rinkiniai“. Informatikos ir ryšių departamentas. Žiūrėta 2026 m. kovo 22 d. https://www.ird.lt/lt/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos/nusikalstamumo-duomenu-rinkiniai/dimension.BK?BK%5B%5D=XXX&DT%5B%5D=2025-11&SAV%5B%5D=LR&cols=DT.
53. „Internet use remains highest among youth, yet the generational gap is shrinking“. International Telecommunication Union. Žiūrėta 2026 m. balandžio 23 d. https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-youth-internet-use/.

Kiti šaltiniai:

54. Lietuvos statistika. *Skaitmeninė ekonomika ir visuomenė Lietuvoje*. Vilnius: 2022. https://osp.stat.gov.lt/documents/10180/10362936/Skaitmenin%C4%97+ekonomika+ir+visuomen%C4%97+Lietuvoje+%282022+m.+leidimas%29.pdf/14d6c6c8-db09-4fb2-9427-3c6104db448a.
55. „Lietuvos kibernetinių grėsmių paveikslas: ar valstybė pasiruošusi apsaugoti virtualią erdvę?“. *Lietuvos Respublikos Krašto apsaugos ministerija,* 2025 m. spalio 7 d. https://kam.lt/lietuvos-kibernetiniu-gresmiu-paveikslas-ar-valstybe-pasiruosusi-apsaugoti-virtualia-erdve/.
56. „2025 Internet Crime Report“. Federal Bureau of Investigation. Žiūrėta 2025 m. rugsėjo 15 d. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

57. „The Evolving Threat Landscape: How Encryption, Proxies and AI are Expading Cybercrime 2026“. Europol. Žiūrėta 2026 m. rugsėjo 15 d. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf.
58. „Kibernetiniai nusikaltėliai sukūrė tikrą ‚darbo biržą‘ – išpirkos reikalauti gali bet kas“. *LRT,* 2017 m. gegužės 15 d. https://www.lrt.lt/naujienos/mokslas-ir-it/11/173003/kibernetiniai-nusikalteliai-sukure-tikra-darbo-birza-ispirkosreikalauti-gali-bet-kas.
59. National Criminal Justice Information and Statistics Service. *Criminal Justice Resource Manual* (U.S.: 1979*).* https://www.ojp.gov/pdffiles1/Digitization/61550NCJRS.pdf. Kemp, Simon. „Digital 2026: Internet Ussers Pass The 6 Billions Mark“ *Datareportal,* 2025 m. spalio 15 d. https://datareportal.com/reports/digital-2026-six-billion-internet-users.
60. „Chart of signatures and ratifications of Treaty 185“. Council of Europe Portal. Žiūrėta 2025 m. gruodžio 26 d. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.
61. „574 arrests and USD 3 million recovered in coordinated cybercrime operation across Africa“. Interpol. Žiūrėta 2025 m. gruodžio 26 d. https://www.interpol.int/News-and-Events/News/2025/574-arrests-and-USD-3-million-recovered-in-coordinated-cybercrime-operation-across-Africa.
62. „From Framework to Fieldwork: INTERPOL‘s Role in Advancing the UN Cybercrime Convention“. United Nations Office on Drugs and Crime. Žiūrėta 2025 m. gruodžio 27 d. https://hanoiconvention.org/side-event/from-framework-to-fieldwork-interpols-role-in-advancing-the-un-cybercrime-convention/.
63. European Committee on Crime Problems. *Computer – Related Crime, Recommendation No. R(89)9 on computer - related crime and final report of the European Committee on Crime Problems.* Strasbourg, Council of Europe, 1990. https://www.oas.org/juridico/english/89-9&final%20Report.pdf.
64. Council of Europe. *Recommendation No. R(95) 13, of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law Connected with Information Technology.* Strasbourg: Council of Europe, 1995. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76.
65. „Pranešti apie spragą“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. sausio 2 d. https://www.nksc.lt/pranesti-spraga.html.
66. Mugamba, Elemegoius. „Cross-border cybercrime enforcement and legislative harmonisation: a comparative study of EU Directive 2013/40/EU and non-EU

jurisdictions". *Research Gate,* 2025 m. spalio mėn., 2. https://www.researchgate.net/publication/398757570_CROSS-BORDER_CYBERCRIME_ENFORCEMENT_AND_LEGISLATIVE_HARMONISATION_A_COMPARATIVE_STUDY_OF_EU_DIRECTIVE_201340EU_AND_NON-EU_JURISDICTIONS.

67. „Informatika reikšmė". Lietuvių žodynas. Žiūrėta 2023 m. spalio 16 d. https://www.lietuviuzodynas.lt/terminai/Informatika.
68. „Senatvės pensijos amžiaus lentelė". Sodra. žiūrėta 2026 m. kovo 16 d. https://sodra.lt/senatves-pensijos-amziaus-lentele.
69. Lietuvos Respublikos Krašto apsaugos ministerija. *Nacionalinė kibernetinio saugumo ataskaita 2022*. Lietuva: 2023. https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf.
70. European Union Agency for Cybersecurity. "Enisa Threat Landscape reports 2020 – 2025". ENISA. Žiūrėta 2026 m. kovo 26 d. https://www.enisa.europa.eu/.
71. ENISA. *Raising Awareness of Cybersecurity*: *A Key Element of National Cybersecurity*. Graikija: 2021. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Raising%20awareness%20of%20cybersecurity%20as%20a%20key%20element%20of%20NCSS.pdf.
72. Federal Bureau of Investigation. *Internet Crime Report 2024*. Washington: FBI, 2025. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
73. Lewis, James. *Economic Impact of Cybercrime—No Slowing Down Report*. Santa Clara: McAfee LLC, 2018. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.
74. Europos Komisija. „Komisijos Komunikatas Tarybai ir Europos Parlamentui „Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su nusikalstamumu centro kūrimas/*COM/2012/0140 final */". EUR-Lex. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52012DC0140.
75. Lietuvos Respublikos Krašto apsaugos ministerija. *Nacionalinė kibernetinio saugumo ataskaita* 2024. Lietuva: 2025. https://kam.lt/wp-content/uploads/2025/07/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf.
76. Lietuvos Respublikos Krašto apsaugos ministerija. *Nacionalinė kibernetinio saugumo ataskaita 2020*. Lietuva: 2021. https://kam.lt/wp-content/uploads/2022/02/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf.

77. „Asmens duomenų saugumo pažeidimai Lietuvoje 2025 m.“. *Valstybinė duomenų apsaugos inspekcija*, 2026 m. vasario 12 d. https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2025-m-lfX/.
78. IBM. *Cost of a Data Breach Report 2025: The AI Oversight Gap.* JAV: IBM, 2025. https://www.ibm.com/forms/mkt-53830.
79. Pogorelec, Anamarija. „The people behind cyber extortion are often in their forties“. *Help Net Security*, 2026 m. kovo 10 d. https://www.helpnetsecurity.com/2026/03/10/cyber-extortion-cybercrime-age-profile/.
80. Lietuvos Respublikos prokuratūra. *Lietuvos Respublikos prokuratūros veiklos 2023 metais ataskaita*. Lietuva: 2024. https://www.prokuraturos.lt/data/public/uploads/2024/03/2023-m.-ataskaita-galutine.pdf.
81. Lietuvos Respublikos prokuratūra. *Lietuvos Respublikos prokuratūros veiklos 2024 metais ataskaita*“. Lietuva: 2025. https://www.prokuraturos.lt/data/public/uploads/2025/04/metine-prokuraturos-ataskaita-2024-final.pdf.
82. „Understanding the cyber crime and fraud victim journey“. Jungtinės Karalystės Vyriausybė. Žiūrėta 2026 m. balandžio 28 d. https://www.gov.uk/government/publications/understanding-the-cyber-crime-and-fraud-victim-journey/understanding-the-cyber-crime-and-fraud-victim-journey.
83. Lietuvos Respublikos valstybės saugumo departamentas. *Grėsmių nacionaliniam saugumui vertinimas 2025.* Vilnius: 2025. https://kam.lt/wp-content/uploads/2025/03/2025-GR-LT-02-21-El-be-uzraso_.pdf.
84. „Svarbu: „Ignitis ON” patyrė programišių ataką”. Ignitis, 2024 m. vasario 12 d. https://ignitis.lt/verslui/naujienos/naujienos/svarbu-ignitis-patyre-programisiu-ataka.
85. Verizon. *2023 Data Breach Investigations Report.* New York: Verizon, 2023. https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf.
86. The Mentor. „The Hacker Manifesto, 8 January 1986“. Žiūrėta 2026 m. gegužės 1 d. https://phrack.org/issues/7/3.
87. Mujianto, Mujianto. „Cybercrime Regulations as an Instrument of Legal Protection for Victims of Cybercrime in Indonesia“. Pranešimas konferencijoje Proceeding of International Conference on the Law Development for Public Welfare, Indonezija, 2024 m. https://www.researchgate.net/publication/399221463_Cybercrime_Regulations_as_an_Instrument_of_Legal_Protection_for_Victims_of_Cybercrime_in_Indonesia.

88. Aukščiausiojo audito institucija. „Ar veiksmingai kovojama su elektroniniais nusikaltimais“. Valstybės kontrolė. Žiūrėta 2026 m. sausio 6 d. https://www.valstybeskontrole.lt/LT/Product/23926/ar-veiksmingai-kovojama-su-elektroniniais-nusikaltimais.
89. Charles de Montesquieu. *The Spirit of Laws.* Indianapolis: The online Library of Liberty, 1748. https://oll-resources.s3.us-east-2.amazonaws.com/oll3/store/titles/837/Montesquieu_0171-01_EBk_v6.0.pdf.
90. „NKSC Mokymai“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. gegužės 3 d. https://mokymai.nksc.lt/.
91. „Atnaujintos svarbiausios NKSC pratybos „Kibernetinis skydas OpEx““. Nacionalinis kibernetinio saugumo centras. Žiūrėta gegužės 3 d. https://www.nksc.lt/naujienos/nacionalinis_kibernetinio_saugumo_centras_eda46592.html.
92. „Dėl 2023 – 2030 metų plėtros programos valdytojos Lietuvos Respublikos Krašto apsaugos ministerijos nacionalinė kibernetinio saugumo plėtros programos patvirtinimo“. Lietuvos Respublikos Krašto apsaugos ministerija. Žiūrėta 2026 m. gegužės 4 d. https://kam.lt/pletros-programu-pazangos-priemones/.
93. „2023 – 2030 metų plėtros programos valdytojos Lietuvos Respublikos Krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos pažangos priemonės Nr. 06-007-10-05-05 „Stiprinti kibernetinį atsparumą“ aprašo pagrindimas“. Lietuvos Respublikos Krašto apsaugos ministerija. Žiūrėta 2026 m. gegužės 4 d. https://kam.lt/pletros-programu-pazangos-priemones/.
94. Lietuvos Respublikos Krašto apsaugos ministerija. *Nacionalinė kibernetinio saugumo ataskaita 2019.* Lietuva: 2020. https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf
95. „Lietuvos vadovaujamos ES kibernetinės greitojo reagavimo pajėgos- atsakas į incidentus tiek ES viduje, tiek remiant ES partnerius ir karines misijas“. Lietuvos Respublikos Krašto apsaugos ministerija, 2023 m. kovo 30 d. https://kam.lt/lietuvos-vadovaujamos-es-kibernetines-greitojo-reagavimo-pajegos-atsakas-i-incidentus-tiek-es-viduje-tiek-remiant-es-partnerius-ir-karines-misijas/.
96. „Lithuanian Cyber Defence Command opened“. Lietuvos Respublikos Krašto apsaugos ministerija, 2025 m. sausio 3 d. https://kam.lt/en/lithuanian-cyber-defence-command-opened/.

97. Bukauskas, Linas, Agnė Brilingaitė ir Kęstutis Ikamas. *Lietuvos kibernetinio saugumo kompetencijų žemėlapis (ataskaita*). Vilnius: Vilniaus universitetas, 2022. https://cs.vu.lt/projects/P-REP-21- 2/ataskaita.pdf.
98. „Sukčiavimui atspari mąstysena: paprasti apsisaugoti padedantys įpročiai“. Europol. Žiūrėta 2026 m. gegužės 4 d. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/scam-aware-mindset-simple-habits-to-stay-protected:lt.
99. Car, Polona ir Tristan Marelin. „Artificial Intelligence and Cybersecurity”. European Parliament. Žiūrėta 2026 m. gegužės 5 d. https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA(2024)762292_EN.pdf.
100. „Ar Dirbtinis Intelektas Perims Kibernetinį Saugumą“. Solix Technologies. Žiūrėta 2026 m. gegužės 5 d. https://www.solix.com/lt/blog/learning/will-ai-take-over-cyber-security/.
101. Johnson, Robert. „60 Percent Of Small Companies Close Within 6 Months Of Being Hacked“. *Cybercrime Magazine,* 2019 m. sausio 2 d. https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.
102. Scroxton, Alex. „German authorities probe ransomware hospital death“. *Computer Weekly News,* 2020 m. rugsėjo 18 d. https://www.computerweekly.com/news/252489247/German-authorities-probe-ransomware-hospital-death
103. Europol. *Internet Organised Crime Threat Assessment 2025.* Luxembourg: Publications Office of the European Union, 2025. https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.
104. National Crime Agency. *Pathways Into Cyber Crime*. Jungtinė Karalystė: 2017). https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file.

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

Anotacija lietuvių kalba

Reikšminiai žodžiai: kompiuteriniai nusikaltimai, elektroninė erdvė, informacinės technologijos, prevencija.

Magistro baigiamojo darbo „Kompiuterinių nusikaltimų Lietuvoje kriminologiniai aspektai“ tikslas – ištyrus kompiuterinių nusikaltimų Lietuvoje kriminologinius aspektus pateikti siūlymų jų prevencijai.

Baigiamajame darbe atskleidžiama kompiuterinių nusikaltimų sampratą, analizuojamas šių nusikalstamų veikų tarptautinis teisinis reguliavimas bei teisinis reglamentavimas Lietuvos Respublikos teisėje. Didelis dėmesys skiriamas kompiuterinius nusikaltimus darančių asmenų charakteristikai, jų ryšiui su auka, bei kompiuterinių nusikaltimų raiškai 2020 – 2025 m. laikotarpiu, atskleisti. Nagrinėjami veiksniai lemiantys kompiuterinių nusikaltimų nusikalstamumą, pabrėžiant technologinių, socialinių, ekonominių ir teisinių veiksnių įtaką kompiuterinių nusikaltimų paplitimui. Analizuojamos Lietuvoje taikomos prevencijos ir kontrolės priemonės kovai su kompiuteriniais nusikaltimais, akcentuojant visuomenės švietimo ir informavimo, dirbtinio intelekto panaudojimo, naudą. Atliktas ikiteisminio tyrimo tyrėjų, atliekančių kompiuterinių nusikaltimų tyrimus, kokybinio tyrimo interviu būdu gautų atsakymų analizė. Susisteminus tyrimo metu gautą informaciją, pateikiamos išvados ir pasiūlymai kompiuterinių nusikaltimų prevencijos ir kontrolės tobulinimui.

Annotation in English

Key words: computer crime, cyberspace, information technology, prevention.

The aim of the Master‘s thesis „Criminological aspects of computer crime in Lithuania“ is to examine the criminological aspects of cybercrime in Lithuania ant to provide proposals for its prevention. The thesis reveals the concept of the computer crimes, analyses the international legal regulation of these criminal acts , as well as their legal regulation in the law of Republic of Lithuania. Considerable attention is devoted to the characteristics of persons committing cybercrimes, their relationship with the victim and the manifestation of cybercrime during the period of 2020 – 2025. The thesis examines the factors contributing to cybercrime, emphasizing the influence of technological, social, economic, and legal factors on the spread of cybercrime. It also analyses the prevention and control measures applied in Lithuania in combating cybercrime, highlighting the benefits of public education and awareness – raising and the use of artificial

intelligence. A qualitative study was contucted by analysing responses obtained through interviews with pre – trial investigators carrying out cybercrime investigations. After systematising the information obtained during the research, conclusions and proposals for improving cybercrime prevention and control are presented.

SANTRAUKA LIETUVIŲ KALBA

Šiuolaikiniame pasaulyje, informacinės technologijos yra neatsiejama mūsų gyvenimo dalis. Tobulėjant šioms technologijoms, kartu didėja ir kompiuterinių nusikaltimų skaičius. Šie nusikaltimai tampa vis labiau sudėtingesni, tarptautiniu pobūdžiu padaromi dideli nuostoliai tiek fiziniams, tiek juridiniams asmenims, todėl kompiuterinius nusikaltimus svarbu analizuoti kriminologiniu požiūriu: tyrinėti šių nusikalstamų veikų paplitimą, nusikaltėlio charakteristiką, veiksnius, skatinančius nusikalstamumą bei prvencijos priemones.

Magistro baigiamojo darbo „Kompiuterinių nusikaltimų Lietuvoje kriminologiniai aspektai“ tikslas – ištirti kompiuterinių nusikaltimų kriminologinius aspektus ir pateikti siūlymų jų prevencijai. Pagrindiniai uždaviniai – išanalizuoti kompiuterinių nusikaltimų sampratą, tarptautinį teisinį reguliavimą bei nacionalinį teisinį reglamentavimą; išanalizuoti kompiuterinių nusikaltimų raišką 2020 – 2025 m. laikotarpiu; atskleisti asmenų, padariusių kompiuterinius nusikaltimus, charakteristiką ir jo ryšį su auka; atskleisti veiksnius, lemiančius kompiuterinių nusikaltimų atsiradimą ir plitimą; apžvelgti kompiuterinių nusikaltimų prevencijos ir kontrolės priemones bei pateikti siūlymus prevencijos ir kontrolės gerinimui; atskleisti ikiteisminio tyrimo tyrėjų, atliekančių kompiuterinių nusikaltimų tyrimus, požiūrį į šių nusikalstamų veikų pobūdį, veiksnius ir prevencijos priemones.

Pirmajame skyriuje analizuojama kompiuterinių nusikaltimų samprata, atribojant ją nuo elektroninių nusikaltimų sąvokos. Analizuojamas kompiuterinių nusikaltimų tarptautinis teisinis reguliavimas, bei koks yra Lietuvoje šių nusikalstamų veikų teisinis reglamentavimas.

Antrajame skyriuje pateikiama 2020 – 2025 m. laikotarpio kompiuterinių nusikaltimų raiška bei galima žala. Registruotų nusikalstamų veikų, numatytų LR BK XXX skyriuje, skaičius padidėjo.

Trečiajame skyriuje analizuojama kompiuterinius nusikaltimus darančių asmenų charakteristika. 2020 – 2025 m. laikotarpiu kompiuterinius nusikaltimus dažniau padaro vyrai, pagrindinį ir vidurinį išsilavinimą turintys asmenys, dažniausiai 30 – 39 m. amžiaus bei nedirbantys ir bedarbiai asmenys.

Ketvirtajame skyriuje atskleidžiami veiksniai, lemiantys kompiuterinių nusikaltimų atsiradimą ir plitimą, pabrėžiant technologinių, socialinių, ekonominių ir teisinių veiksnių įtaką kompiuterinių nusikaltimų paplitimui.

Penktajame skyriuje apžvelgiami kompiuterinių nusikaltimų prevencijos ir kontrolės priemonės. Pabrėžiama visuomenės sąmoningumo ugdymo nuo mažens ir dirbtinio intelekto panaudojimo, nauda.

Šeštajame skyriuje pateikiami ir analizuojami ikiteisminio tyrimo tyrėjų, atliekančių kompiuterinių nusikaltimų tyrimus, kokybinio tyrimo interviu būdu gauti duomenys, atskleidžiamas tyrėjų požiūris į šių nusikalstamų veikų pobūdį, veiksnius bei prevencijos priemones.

SUMMARY

The aim of the Master‘s thesis „Criminological aspects of cybercrime in Lithuania“ is to examine the criminological aspects of cybercrime and to provide proposals for its prevention. The main objectives of the thesis: to analyse the concept of cybercrime, international legal regulation and national legal framework; to examine the manifestation of cybercrime during the period of 2020 – 2025; to reveal the characteristics of persons committing cybercrimes and their relationship with the victim; to identify the factors contributing to the emergence and spread of cybercrime; to review cybercrime prevention and control measures and provide proposals for improving prevention and control; to reveal the attitudes of pre – trial investigators conducting cybercrime investigators towards the nature, causes and prevention measures of these criminal offences.

The first chapter analyses the concept of cybercrime and distinguishes it from the concept of electronic crime. It also examines the international legal regulation of cybercrime and legal framework governing these criminal offences in Lithuania.

The second chapter presents the manifestation of cybercrime during the period of 2020 – 2025 and the potential damage caused by such offences. The number of registered criminal offences provided in Chapter XXX of the Criminal Code of the Republic of Lithuania increased during the analysed period.

The third chapter analyses the characteristics of the persons committing cybercrimes. During the period of 2020 – 2025, cybercrimes were more frequently committed by males, persons with primary or secondary education, individuals aged 30 – 39 and unemployed persons.

The fourth chapter reveals the factors contributing to the emergence and spread of cybercrime, emphasizing the influence of technological, social, economic and legal factors on the prevalence of cybercrime.

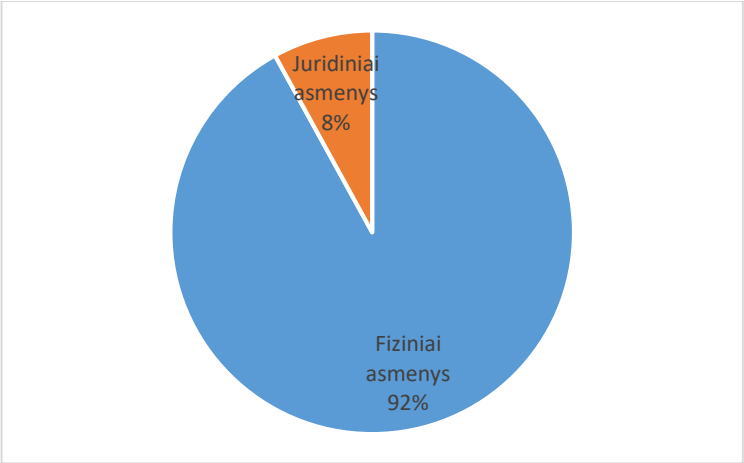
The fifth chapter reviews cybercrime prevention and control measures. Particular emphasis is places on the benefits of raising public awareness from an early age and the us of artificial intelligence.

The sixth chapter presents and analyses the data obtained through qualitative interviews with pre – trial investigators conducting cybercrime investigations, revealing investigators attitudes towards the nature of these criminal offences, the factors contributing to them and the prevention measures applied.

PRIEDAI

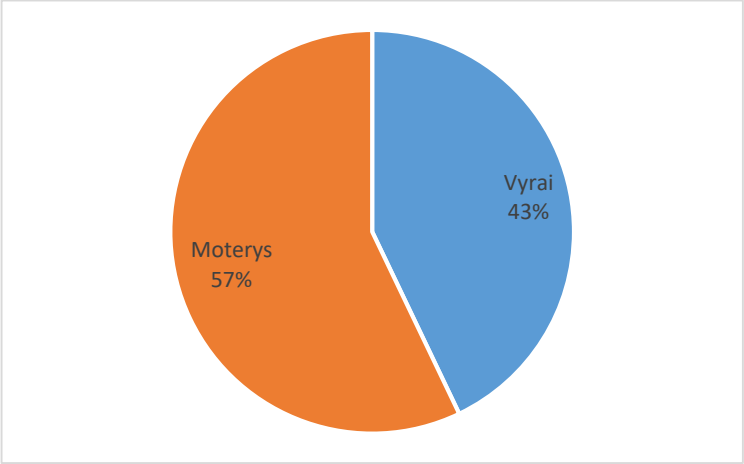
Priedas Nr. 1.

Nukentėjusių asmenų nuo LR BK XXX skyriaus nusikalstamų veikų, pasiskirstymas 2020 - 2025 m. laikotarpiu



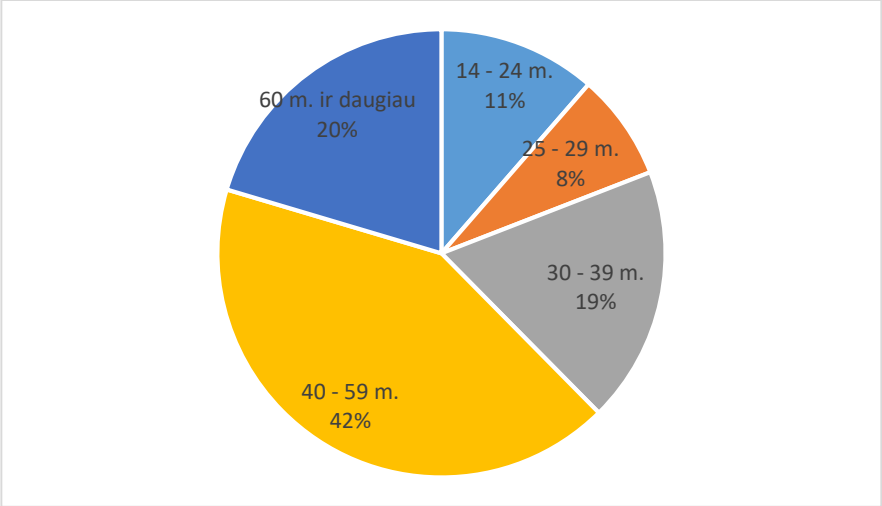
Priedas Nr. 2

Nukentėjusių asmenų nuo LR BK XXX skyriaus nusikalstamų veikų, pasiskirstymas pagal lytį 2020 - 2025 m. laikotarpiu



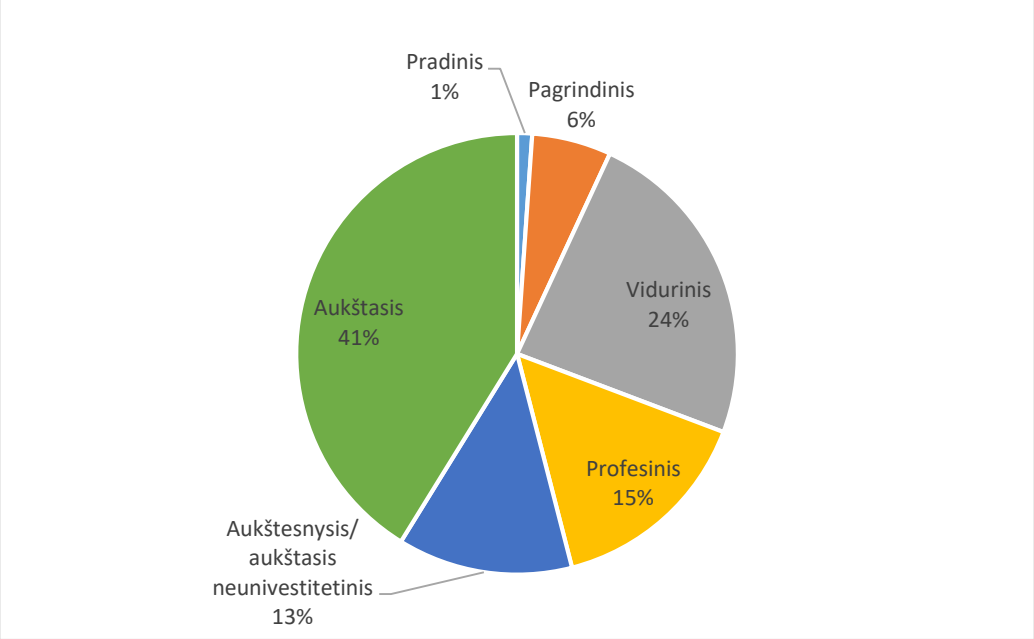
Priedas Nr. 3

Nukentėjusių asmenų nuo LR BK XXX skyriaus nusikalstamų veikų, pasiskirstymas pagal amžių 2020 - 2025 m. laikotarpiu



Priedas Nr. 4

Nukentėjusių asmenų nuo LR BK XXX skyriaus nusikalstamų veikų, pasiskirstymas pagal išsilavinimą 2020 - 2025 m. laikotarpiu



Priedas Nr. 5

Kokybinio interviu, skirto ikiteisminio tyrimo tyrėjams, atliekantiems kompiuterinių nusikalstamų veikų tyrimus, klausimai

1. Kiek metų tiriate nusikalstamas veikas, numatytas BK XXX skyriuje (nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui)?
2. Kaip per pastaruosius kelerius metus pasikeitė kompiuterinių nusikaltimų pobūdis ir mastas Jūsų praktikoje?
3. Kokie, Jūsų nuomone, yra pagrindiniai veiksniai, lemiantys kompiuterinius nusikaltimus?
4. Ar Jūsų nuomone, Lietuvos policijai pakanka techninių ir žmogiškųjų išteklių ir kvalifikacijos, tiriant kompiuterinius nusikaltimus?
5. Ar praktikoje susiduriate su sunkumais bendradarbiaujant su kitomis įstaigomis (nacionaliniu ir tarptautiniu lygmeniu)? Jei taip, kokiais?
6. Kaip vertinate Lietuvoje vykdomas prevencines priemones, siekiant sumažinti kompiuterinių nusikaltimų skaičių? Ar, Jūsų nuomone, jos yra veiksmingos ir ar jų yra pakankamai?
7. Kokias priemones, Jūsų nuomone, reikėtų taikyti Lietuvoje siekiant stiprinti kompiuterinių nusikaltimų prevenciją?