**1 priedas. Interpolo Generalinio Sekretoriato patvirtintas vieningas kompiuterinių nusikaltimų kodifikatorius**

1. QA – nesankcionuota prieiga ir perėmimas:

QAH – informacijos perėmimas panaudojant specialias technines priemones;

QAT – laiko vagystė (atsiskaitymo už pasinaudojimą automatizuotomis informacinėmis sistemomis vengimas);

QAZ – kitos nesankcionuotos prieigos ir perėmimo rūšys.

2. QD – kompiuterinių duomenų pakeitimas:

QDL – loginė bomba (komandų, suveikiančių tam tikromis sąlygomis, rinkinys);

QDT – Trojos arklys (destruktyvi programa, gebanti autonomiškai platintis);

QDW – kompiuterinis kirminas (programa, gebanti autonomiškai plisti kompiuteriniu tinklu);

QDZ – kiti duomenų pakeitimo būdai.

3. QF – kompiuterinis sukčiavimas:

QFC – sukčiavimas panaudojant bankomatus;

QFF – kompiuterinis padirbinėjimas (kortelė ar pan.);

QFG – sukčiavimas panaudojant žaidimo automatus;

QFM – manipuliacija su Įvedimo ir išvedimo programomis (klaidingų duomenų Įvedimas ir tokių programų rezultatų analizė);

QFP – sukčiavimas panaudojant atsiskaitymo priemones (pinigų pagrobimas – labiausiai paplitęs kompiuterinis nusikaltimas);

QFT – telefoninis sukčiavimas (pasikėsinimas Į telekomunikacinių paslaugų sistemas);

QFZ – kiti kompiuterinio sukčiavimo būdai.

4. QR – neteisėtas kopijavimas:

QRG – kompiuterinių žaidimų;

QRS –programinės Įrangos;

QRT – puslaidininkių Įrangos topologijos;

QRZ – kitas neteisėtas kopijavimas.

5. QS – kompiuterinis sabotažas:

QSH – aparatinės Įrangos (kompiuterio darbo sutrikdymas);

QSS – programinės Įrangos (informacijos sunaikinimas, blokavimas);

QSZ – kitos sabotažo rūšys.

6. QZ – kiti kompiuteriniai nusikaltimai:

QZB – panaudojant kompiuterines skelbimo lentas;

QZE – informacijos, sudarančios komercinę paslaptį, pagrobimas;

QZS – informacijos, kuri turi būti nagrinėjama teisme, perdavimas;

QZZ – kiti kompiuteriniai nusikaltimai.

PASTABA. Kodifikatoriuje kompiuteriniams nusikaltimams priskirtas indeksas „Q“, pateiktas nusikaltimų sąrašas nėra baigtinis, apdairiai palikta galimybė jį plėsti, pasinaudojant indeksu „Z“, reiškiančiu „kiti“, visi nusikaltimai sugrupuoti Į šešias grupes, k iekviena kompiuterinių nusikaltimų grupė detalizuojama nurodant jai priskirtus nusikaltimus, turinčius savo raidinį indeksą.

**2 priedas. Veikų, susijusių su kompiuterinių technologijų panaudojimu, kriminalizavimas Europos Sąjungos valstybėse ir teisės aktų apžvalga**

| Valstybė | Neteisėtas kompiuterinės informacijos rinkimas | Kenkėjiškos programos | Atsisakymas aptarnauti (DNS) | Bandymas Įsibrauti | Neteisėta prieiga prie informacijos | Neteisėtas informacijos perėmimas | Neteisėtas informacijos pakeitimas | Neteisėta prieiga prie ryšių sistemų |
|---|---|---|---|---|---|---|---|---|
| **Airija** | Ne[1] | Ne | Ne | Krim.[2] | Krim. | Ne | Ne | Krim. |
| **Austrija** | Krim. | Krim. | Ne | Adm.ats.[3] | Krim. | Krim. | Krim. | Krim. |
| **Belgija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Danija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Ne | Krim. |
| **Didžioji Britanija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Graikija** | Ne | Ne | Ne | Krim. | Krim. | Ne | Ne | Krim. |
| **Ispanija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Italija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Liuksemburgas** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Olandija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Portugalija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Prancūzija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Suomija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Švedija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |
| **Vokietija** | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. | Krim. |

PASTABOS:

Veikos Įvardintos sąlyginai;

Ne[1] – veika nekriminalizuota, už ją netaikoma nei administracinė, nei baudžiamoji atsakomybė;

Krim.[2] – veika kriminalizuota, t.y. už ją taikoma baudžiamoji atsakomybė;

Adm.ats.[3] – už veiką taikoma administracinė atsakomybė.

**Europos Sąjungos valstybių teisės aktų, susijusių su kompiuterinių nusikaltimų reglamentavimu bei teisine atsakomybe už šias veikas, apžvalga**

***Airija.*** *Airija priklauso bendrosios teisės sistemai, tad baudžiamieji Įstatymai nėra kodifikuoti, o atsakomybė už nusikaltimus pažangių informacinių technologijų srityje numatyta 1991 m. Akte dėl kriminalinės žalos. Pagal Akto 5 straipsnĮ, asmuo, naudojantis kompiuterĮ šalies teritorijoje siekiant gauti neteisėtą prieigą prie duomenų, kurie yra saugomi valstybės teritorijoje ir už jos ribų, arba naudojantis kompiuterĮ, kuris yra ne valstybės teritorijoje, duomenims, saugomiems valstybės teritorijoje, gauti, bus pripažintas kaltu Įvykdžius nusikaltimą, neatsižvelgiant Į tai, ar jam pavyko duomenis gauti. Už šią veiką numatyta bausmė - bauda arba laisvės atėmimas iki 3 mėnesių.*

***Austrija.*** *Austrijos Įstatymai nenumatė baudžiamosios atsakomybės už nusikaltimus, susijusius su kompiuterinėmis technologijomis, iki 2002 m. Baudžiamojo kodekso pataisų. Administracinė atsakomybė už tam tikrus kompiuterinius pažeidimus numatyta Akte dėl duomenų apsaugos, priimtame 2000 m., pavyzdžiui, vadovaujantis šio Akto 52 straipsniu, administracinėn atsakomybėn traukiamas asmuo, neteisėtai gavęs prieigą prie duomenų, taip pat sudaręs galimybę ar padėjęs gauti neteisėtą prieigą kitam asmeniui, tyčia neteisėtai perdavęs konfidencialius duomenis, naudojantis duomenis pažeidžiant slaptumo reikalavimus. Administracinė atsakomybė taip pat taikoma už tyčinĮ neteisėtą duomenų sunaikinimą. Pagal Akto 52 straipsnĮ, administracinė atsakomybė numatoma taip pat ir už pasikėsinimą Įvykdyti minėtas veikas.*

*Įgyvendindama Konvenciją dėl elektroninių nusikaltimų, Austrija parengė Baudžiamojo kodekso pataisas, kurios Įsigaliojo nuo 2002 m. spalio 1 d. Pataisos kriminalizavo keletą naujų kompiuterinių nusikaltimų ir pakeitė kai kurias egzistuojančias sankcijas už kompiuterinius nusikaltimus. Baudžiamoji atsakomybė nustatyta už neteisėtą prieigą prie kompiuterinių sistemų (118 str.), telekomunikacijų slaptumo pažeidimą (119 str.), duomenų perėmimą (119 str.), duomenų ar kompiuterinių sistemų sugadinimą, piktnaudžiavimą programine Įranga arba prieigos teisėmis (126 str.), nesąžiningą piktnaudžiavimą duomenų apdorojimu (148 str.) ir kompiuterinių duomenų suklastojimą (225 str.). Kitos Austrijos Baudžiamojo kodekso pataisos, Įsigaliojusios 2004 m. gegužės 1 d., pertvarkė atsakomybę už seksualinius nusikaltimus (ypač dėl vaikų pornografijos, 207 str.) ir už nusikaltimus, susijusius su atsiskaitymais negrynais pinigais (241 str.).*

***Danija.*** *Danijos Baudžiamajame kodekse yra keturi straipsniai (263, 193, 291), numatantys atsakomybę už kompiuterinius nusikaltimus. 263 straipsnio 1 dalis numato baudžiamąją atsakomybę už ryšio slaptumo pažeidimą (taip pat ir elektroninio pašto), neteisėtą Įsibrovimą Į asmeninės nuosavybės saugojimo vietą (taikoma ir duomenims, saugomiems kompiuterinėje sistemoje), taip pat už duomenų perėmimą elektroninių ryšių (telekomunikaciniuose) tinkluose. Už šias veikas numatyta bausmė – bauda arba laisvės atėmimas iki 6 mėnesių. Tokią pačią bausmę numato ir antroji šio straipsnio dalis už neteisėtą prieigą prie kompiuterinių duomenų ir kompiuterinių programų. Jei minėti nusikaltimai yra padaromi pramoninio šnipinėjimo tikslu ar kitomis sunkinančiomis aplinkybėmis, tai laisvės atėmimo bausmė gali būti padidinta iki 2 metų.*

*Danijos Baudžiamojo kodekso 193 straipsnis numato atsakomybę už Įsiskverbimą Į viešąsias*

*ryšių sistemas, duomenų apdorojimo sistemas, specialiąsias infrastruktūras (vandens tiekimo, elektros ir dujų tiekimo, sveikatos apsaugos) ir jų normalaus veikimo sutrikdymą.*

*Kompiuteriniams nusikaltimas gali būti taikomos ir bendrosios normos dėl baudžiamosios atsakomybės už padarytą žalą nuosavybei (pvz., Danijos Baudžiamojo kodekso 291 straipsnis numato, kad asmuo, sunaikinęs ar pažeidęs svetimą nuosavybę gali būti baudžiamas bauda arba laisvės atėmimu iki vienerių metų).*

***Graikija.*** *Graikijos Baudžiamojo kodekso 370 straipsnio 2 punktas kaip nusikaltimą Įvardija neteisėtą prieigą prie kompiuterinės sistemos. Vadovaujantis šia norma, asmuo, Įgavęs neteisėtą prieigą prie kompiuterinių duomenų ar duomenų, perduodamų elektroninių ryšių tinklais, turi būti baudžiamas bauda arba laisvės atėmimu iki 3 mėnesių. Jei neteisėta prieiga prie duomenų Įvykdyta asmens, turinčio prieigą prie duomenų ar Įmonės darbuotojo, toks asmuo turi būti baudžiamas tik tuo atveju, jei prieiga prie duomenų buvo tiesiogiai uždrausta vidaus tvarkos taisyklėmis, raštišku dokumentu ar kompetentingo asmens nurodymu.*

***Italija.*** *Italijos Baudžiamajame kodekse yra numatyta atsakomybė už daugelĮ kompiuterinių nusikaltimų. Pavyzdžiui, Italijos Baudžiamojo kodekso 615 straipsnio 3 dalis draudžia neteisėtą prieigą prie kompiuterio ar elektroninių ryšių (telekomunikacinės) sistemos, t.y. prie kompiuterių ar sistemų, apsaugotų saugumo priemonėmis, taip tokią prieigą prieš savininko valią, bausmė už tokią veiką gali būti laisvės atėmimas iki 3 metų. Griežtesnė bausmė – laisvės atėmimas nuo 1 iki 5 metų – numatyta tuomet, kai šĮ nusikaltimą padaro pareigūnas ar asmuo, piktnaudžiaujantis savo Įgaliojimais, asmuo, užsiimantis privataus detektyvo veikla, taip pat sistemos operatoriaus. Ta pati bausmė yra numatyta ir tuo atveju, kai nusikaltimas Įvykdytas panaudojant smurtą, grasinant padaryti žalą nuosavybei, panaudojant ginklą, jei nusikaltimas padarė žalą sistemai, iš dalies ar visiškai sustabdė jos darbą, sunaikino ar sugadino duomenis, informaciją ar programas, buvusias sistemoje. Kvalifikuojantys šio nusikaltimo požymiai yra ir jo Įvykdymas prieš gynybinės paskirties kompiuterius ar telekomunikacines sistemas, taip pat prieš sistemas, skirtas viešosios tvarkos ir viešojo saugumo bei kitų visuomenės interesų užtikrinimui ir apsaugai. Šiuo atveju bausmė už nusikaltimą yra nuo 3 iki 8 metų laisvės atėmimo.*

*Italijos Baudžiamojo kodekso 615 straipsnio 4 dalis skirta neteisėtam prieigos prie kompiuterinių ir telekomunikacinių sistemų kodų disponavimui ir platinimui. Remiantis šia norma, asmuo, gaminantis, perduodantis, parduodantis kodus, slaptažodžius ar kitas prieigos prie kompiuterių ar telekomunikacinių sistemų priemones, taip pat teikiantis kitą informaciją arba instrukcijas siekiant naudos sau ar tretiesiems asmenims, ar siekiant padaryti žalą, baudžiamas bauda arba laisvės atėmimu iki 1 metų.*

*Italijos Baudžiamojo kodekso 615 straipsnio 5 dalis numato atsakomybę – baudą arba laisvės atėmimą iki dvejų metų – už programų, skirtų kompiuterinėms sistemoms pakenkti ar jas sunaikinti, platinimą. Ji nustato, kad baudžiamas neteisėtas perdavimas ar pardavimas kompiuterinės programos, kurios tikslas ar veikimo padarinys yra kompiuterio ar telekomunikacinės sistemos gedimas, duomenų ar programų, laikomų jose, sugadinimas, taip pat dalinis ar visiškas kompiuterio ar telekomunikacinės sistemos darbo sustabdymas.*

*Baudžiamojo kodekso 420 straipsnio 2 dalis kaip nusikaltimą apibrėžia visuomeninių*

*informacinių infrastruktūrų, visuomeninių duomenų bazių ar programų, veikiančių komunalinio aptarnavimo Įmonėse, sugadinimą ar sunaikinimą. Už tokias veikas numatyta bausmė - laisvės atėmimas nuo 3 iki 8 metų.*

*Baudžiamojo kodekso 635 straipsnio 2 dalis numato baudžiamąją atsakomybę už žalą, padarytą kompiuterinėms sistemoms. Pagal šią normą neĮgaliotas asmuo, sugadinantis ar sunaikinantis kompiuterinę sistemą ar programą, kompiuterinę informaciją ar duomenis, baudžiamas laisvės atėmimu nuo 6 mėnesių iki 3 metų. Jei nusikaltimas Įvykdytas asmens, piktnaudžiaujančio sistemos administratoriaus teisėmis, tai bausmė gali būti nuo 1 iki 4 metų laisvės atėmimo.*

***Liuksemburgas.*** *Kompiuterinių nusikaltimų normos yra išdėstytos Liuksemburgo Baudžiamojo kodekso 509[1], 509[2], 509[3], 524 straipsniuose. 509[1] straipsnis numato atsakomybę už neteisėtą prieigą prie duomenų apdorojimo sistemos ar jos dalies bei už buvimą tokioje sistemoje. Sankcija - bauda arba laisvės atėmimas nuo 2 mėnesių iki 1 metų. Jeigu nurodyti veiksmai sąlygojo duomenų, esančių sistemoje, pakeitimą ar sunaikinimą, tai laisvės atėmimo riba gali būti padidinta iki 2 metų. 509[2] straipsnis draudžia tyčinĮ automatinės duomenų apdorojimo sistemos funkcionalumo sutrikdymą ar pakeitimą. Bausmė už šĮ nusikaltimą – bauda arba laisvės atėmimas nuo 3 mėnesių iki 3 metų. 509[3] straipsnis skirtas duomenų vientisumo ir kokybės apsaugai. Jis nustato, kad asmuo, tyčia ir be tam reikalingų Įgaliojimų Įvedantis Į automatizuotą duomenų apdorojimo sistemą duomenis, trinantis ar keičiantis duomenis, esančius tokioje sistemoje, keičiantis sistemos veikimo principus ar duomenų perdavimo būdą, baudžiamas bauda arba laisvės atėmimas nuo 3 mėnesių iki 3 metų.*

*Pagal Liuksemburgo Baudžiamojo kodekso 524 straipsnĮ, bet koks neteisėtas Įsikišimas Į elektroninių ryšių (telekomunikacines) sistemas yra kvalifikuojamas kaip nusikaltimas, už kurĮ asmeniui gali būti skirta bauda arba laisvės atėmimas nuo 1 mėnesio iki 3 metų.*

***Olandija.*** *Olandijos Baudžiamajame kodekse yra daug straipsnių, numatančių baudžiamąją atsakomybę už kompiuterinius nusikaltimus (138a, 139a, 139b, 139c, 139d, 139e, 161[6], 350a, 350b, 351).*

*138a straipsnis numato atsakomybę už neteisėtą prieigą ir nustato, kad asmuo, tyčia ir neteisėtai gavęs prieigą prie automatinės duomenų saugojimo sistemos, duomenų apdorojimo sistemos ar tokių sistemų dalies, pripažĮstamas kaltu, jei jis veikos vykdymo metu apeina techninę apsaugos sistemą ar naudoja tokias technines priemones, kaip melagingi signalai, melagingi slaptažodžiai, melagingas identifikavimas. Už šią veiką numatyta bausmė - bauda arba laisvės atėmimas iki 6 mėnesių. Antroji 138a straipsnio dalis numato kvalifikuojančias minėtų veikų aplinkybes: jeigu asmuo kopijuoja ar perrašo sau ar kitam asmeniui duomenis, prie kurių jis neteisėtai gavo prieigą nurodytais būdais, tai sankcija gali būti sugriežtinta padidinant laisvės atėmimo laiką iki 4 metų. Tokią pačią bausmę numato ir trečioji 138a straipsnio dalis tais atvejais, kai asmuo Įvykdo neteisėtą prisijungimą, pasinaudodamas telekomunikacinėmis sistemomis, siekdamas naudos sau ar trečiajam asmeniui, arba kai sistemos, prie kurios asmuo gavo neteisėtą prieigą, pagalba jis gauna prieigą prie dar vienos sistemos.*

*139 straipsnis nustato atsakomybę už neteisėtą informacijos perėmimą. 139a straipsnis numato, kad asmuo, tyčia naudojantis automatizuotas sistemas pasiklausymo ar pokalbių Įrašymo gyvenamose patalpose tikslais (išskyrus atvejus, kai su pokalbio dalyviu yra susitariama iš anksto ar kai*

*asmuo pats betarpiškai dalyvauja pokalbyje), gali būti baudžiamas bauda ar laisvės atėmimu iki 6 mėnesių. 139b straipsnis numato baudžiamąją atsakomybę už automatizuotų sistemų ar telekomunikacinių sistemų panaudojimą Įrašant pokalbius už gyvenamų patalpų ribų (sankcija -bauda arba laisvės atėmimas iki 3 mėnesių). 139c straipsnis numato baudžiamąją atsakomybę asmeniui už tyčinĮ techninių priemonių panaudojimą duomenų, perduodamų telekomunikacinėmis sistemomis, tinklais ar prijungta Įranga, perėmimui ir Įrašymui, siekiant naudos sau arba trečiajam asmeniui (sankcija – bauda arba laisvės atėmimas iki 1 metų). 139d straipsnis nustato, kad asmuo, teikiantis priemones, skirtas neteisėtam duomenų, perduodamų telekomunikacinėmis ar automatizuotomis sistemomis, perėmimui ir Įrašymui, gali būti baudžiamas pinigine bauda arba laisvės atėmimu iki 6 mėnesių. 139e straipsnis nustato, kad asmuo, disponuojantis duomenimis, ir žinantis ar privalantis žinoti apie tai, kad šie duomenys buvo gauti vykdant neteisėtą pasiklausymą, Įrašymą arba perėmimą automatizuotose duomenų ar telekomunikacinėse sistemose, baudžiamas pinigine bauda arba laisvės atėmimu iki 6 mėnesių. Tokia pati bausmė gali būti skirta asmeniui, tyčia atskleidžiančiam kitiems asmenims duomenis, kurie yra gauti vykdant neteisėtą pasiklausymą, Įrašymą ar automatizuotų bei telekomunikacinių sistemų duomenų perėmimą, arba padarančiam šiuos duomenis prieinamais tretiesiems asmenims.*

*$161^6$ straipsnis numato atsakomybę už tyčinĮ automatizuotų duomenų apdorojimo sistemų, duomenų saugojimo sistemų, telekomunikacinių sistemų sugadinimą ar sunaikinimą, pažeidžiant tokių sistemų funkcionalumą, pažeidžiant bet kokių šių sistemų apsaugai naudojamų priemonių efektyvumą. Už šią veiką numatyta bausmė - bauda arba laisvės atėmimas iki 6 mėnesių. Tuo atveju, kai vykdant veiką tiesioginiame rimtame pavojuje atsiduria prekės ar teikiamos paslaugos, laisvės atėmimo laikas gali būti padidintas iki 6 metų, o jeigu nusikaltimas sąlygojo žmogaus mirtĮ – iki 15 metų.*

*350a ir 350b straipsniai numato atsakomybę už kompiuterinius nusikaltimus ir žalą, kuri padaroma kompiuteriams ar kompiuterinėms programoms. 350a straipsnis nustato atsakomybę už tyčinĮ neteisėtą duomenų, saugomų automatizuotose sistemose, perduodamų arba apdorojamų jomis, pakeitimą, ištrynimą, sugadinimą (sankcija - piniginė bauda arba laisvės atėmimas iki 2 metų). Laisvės atėmimo bausmė gali būti sugriežtinta iki 4 metų, jei asmuo Įvykdo nusikaltimą prieigai gauti, pasinaudodamas telekomunikacinėmis sistemomis, taip pat, jei duomenims padaryta žala yra labai didelė. Tokia pati bausmė numatyta už tyčinĮ neteisėtą duomenų, kurie kenkia sistemai, platinimą. 350b straipsnis nustato atsakomybę už nurodytas veikas, nesukeliančias didelės žalos (sankcija – bauda arba laisvės atėmimas iki 1 mėnesio).*

*351 straipsnis numato atsakomybę asmeniui, kuris tyčia naikino, gadino ar kitaip padarė netinkamomis naudotis automatizuotas sistemas, skirtas visuomenei būtinų infrastruktūrinių sistemų funkcionavimui (dujų, vandens, elektros tiekimo sistemos, telekomunikacinės sistemos). Už tokio pobūdžio veikas numatoma sankcija - piniginė baudą arba laisvės atėmimas iki 3 metų.*

***Portugalija.*** *Portugalijoje 1991 m. buvo priimtas specialus Įstatymas Nr.109/91 dėl kompiuterinių nusikaltimų. Šio Įstatymo 5 straipsnis numato atsakomybę už žalą, padarytą kompiuteriniams duomenims. Jis nustato, kad tyčinis dalinis ar visiškas duomenų arba programų paėmimas ar sunaikinimas, siekiant naudos sau ar tretiesiems asmenims, yra baudžiamas bauda arba laisvės atėmimu nuo 3 iki 10 metų, priklausomai nuo Įvykdyto nusikaltimo sunkumo. Pasikėsinimas Įvykdyti nusikaltimą taip pat yra*

*baudžiamas. 6 straipsnis numato atsakomybę už kompiuterinĮ sabotažą – neteisėtą duomenų ar programų pakeitimą, sunaikinimą, sutrikdymą arba Įsiterpimą Į duomenų apdorojimo sistemą kitomis priemonėmis, siekiant sutrikdyti sistemos darbą ar jos funkcionalumą. Asmeniui, Įvykdžiusiam tokią veiką, skiriama bauda arba laisvės atėmimas iki 5 metų, jeigu nusikaltimo pasekmės sunkios ir yra padaroma didelė žala, gali būti paskirta laisvės atėmimo bausmė nuo 1 iki 5 metų. 7 straipsnis nustato bausmes už neteisėtą prieigą prie sistemos, siekiant gauti neteisėtos naudos sau ar tretiesiems asmenims. Pasikėsinimas Įvykdyti tokio pobūdžio veiką taip pat yra baudžiamas. Sankcija – bauda arba laisvės atėmimas iki 3 metų, jei prieiga buvo pasiekta Įveikiant apsaugos sistemas ir priemones, ir iki 5 metų, jei prieiga buvo gauta siekiant išgauti komercines ar pramonines paslaptis, saugomas Įstatymo, arba siekiant gauti didelę ekonominę naudą. 8 Įstatymo straipsnis skirtas neteisėtam duomenų perėmimui telekomunikaciniuose tinkluose, panaudojant technines priemones ryšių sistemoje ar tinkle. Pasikėsinimas Įvykdyti šĮ nusikaltimą taip pat yra baudžiamas. Numatyta bausmė – bauda arba laisvės atėmimas iki 3 metų.*

***Suomija.*** *Suomijos Baudžiamojo kodekso 38 straipsnis nustato, kad asmuo, pažeidžiantis susirašinėjimo ar pranešimų, skirtų kitam asmeniui, perdavimo slaptumą, gaunantis ar siekiantis gauti informaciją apie telefoninio pokalbio, telegramos, pranešimo turinĮ, kurĮ gali sudaryti tekstas, vaizdas ar kiti duomenys, arba kitos elektroninių ryšių (telekomunikaciniais) tinklais perduodamos informacijos turinĮ, turi būti baudžiamas bauda arba laisvės atėmimu iki vienerių metų. Tokia pati sankcija yra numatyta už minėtų neviešų pranešimų pažeidimą, sunaikinimą, nuslėpimą.*

*Suomijos Baudžiamojo kodekso 28 straipsnio bendroji norma, numatanti atsakomybę už neteisėtą svetimos kilnojamos nuosavybės, Įrangos, mašinų, mechanizmų panaudojimą, (sankcija - laisvės atėmimas iki vienerių metų), gali būti pritaikoma ir kompiuteriniams nusikaltimams. Suomijos Baudžiamojo kodekso 35 straipsnis, nustatantis atsakomybę už didelės žalos padarymą svetimai nuosavybei, taip pat taikytinas ir kompiuteriniams nusikaltimams, jei yra pažeidžiami duomenys, saugomi kompiuteryje ar kompiuterinėje sistemoje. 28 ir 35 straipsnių sankcijos numato baudą už padarytą nedidelę žalą bei laisvės atėmimą iki 4 metų už padarytą didelę žalą. Tokios pačios sankcijos numatytos ir Suomijos Baudžiamojo kodekso 33 straipsnyje – bendrosios normos dėl klastojimo, kurios taip pat taikomos ir kompiuterinių nusikaltimų atžvilgiu, pavyzdžiui neteisėto informacijos pakeitimo atvejams.*

*Suomijos 1984 m. Aktas dėl ryšio sutrikdymo taip pat gali būti taikomas tokiems nusikaltimams, kaip atsisakymas aptarnauti (DNS) ir kenkėjiškų programų platinimas, tyčiniam telekomunikacinių sistemų darbo sutrikdymui (samkcija už šĮ nusikaltimą – iki 2 metų laisvės atėmimo).*

***Švedija.*** *Švedijos Baudžiamajame kodekse už kompiuterinius nusikaltimus atsakomybė yra numatoma skirtingų skyrių straipsniuose (4, 12, 13 skyriai). Baudžiamojo kodekso 4 skyriaus 8 straipsnis numato atsakomybę už veiksmus, kuriais kėsinamasi Į ryšio slaptumą – neteisėtą ryšio perėmimą ar neteisėtą prieigą prie jo. 9 straipsnis numato atsakomybę už neteisėtą prieigą prie laiškų, telegramų ir panašių dokumentų, kurie yra užantspauduoti ar kitaip apsaugoti nuo pašalinių asmenų. 9a straipsnis numato, kad nusikalstamas yra neteisėtas pasiklausymas, atliktas su papildomų techninių priemonių pagalba. 9c straipsnis skirtas duomenų paslapties pažeidimui – neteisėtos prieigos gavimui darbui su duomenimis.*

*Baudžiamojo kodekso 12 skyrius skirtas nusikaltimams, kurių pasekmė – materialinė žala*

*nuosavybei, taip pat ir kompiuteriniams nusikaltimams, kurių metu buvo padaryta žala nuosavybei. Bauda arba laisvės atėmimu iki 6 mėnesių baudžiama už svetimos nuosavybės sunaikinimą arba sugadinimą, jeigu nusikaltimu yra padaroma didelė žala arba iškyla pavojus žmogaus gyvybei arba sveikatai, tai bausmė gali būti sugriežtinama laisvės atėmimu iki 4 metų.*

*Baudžiamojo kodekso 13 skyrius skirtas nusikaltimams visuomenės saugumui. 13 skyriaus 4 straipsnis nustato, kad asmuo, sunaikinęs arba sugadinęs nuosavybę, turinčią ypatingą reikšmę valstybės gynybai, teisėsaugai, visuomenės apsaugai, yra laikomas kaltu dėl sabotažo vykdymo. Sabotažui yra priskiriama telegrafo, telefono, ir radijo komunikacijų, dujų, vandens, elektros tiekimo, šildymo sistemų sunaikinimas arba jų veikimo sutrikdymas. Už sabotažo Įvykdymą numatyta bausmė - laisvės atėmimas iki 4 metų. 13 skyriaus 5 straipsnis nustato atsakomybę už sabotažą, kuris sukėlė ar galėjo sukelti didelĮ pavojų valstybei arba sąlygojo daugelio žmonių žūtĮ. Sankcija - laisvės atėmimas nuo 2 iki 10 metų arba iki gyvos galvos.*

**3 priedas. Lietuvos Respublikos teisės aktų, susijusių su visuomeninių santykių saugaus kompiuterinės informacijos tvarkymo srityje reglamentavimu, sąrašas bei aktualių teisės normų komentaras**

*1. Lietuvos Respublikos Konstitucija (pvz., 22 str. teigiama, jog žmogaus privatus gyvenimas neliečiamas; asmens susirašinėjimas, pokalbiai telefonu ar kitoks susižinojimas yra neliečiami; 23 str. teigiama, kad nuosavybės teisė yra neliečiama; nuosavybės teises saugo Įstatymas ir kt.);*

*2. Konvencija dėl elektroninių nusikaltimų (Žin., 2004, Nr.36);*

*3. Konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“ (Žin., 2001, Nr. 32-1059);*

*4. Lietuvos Respublikos valstybės registrų Įstatymas (Žin., 1996, Nr.86-2043; 2004, Nr. 124-4488);*

*5. Lietuvos Respublikos elektroninių ryšių Įstatymas (Žin., 2004, Nr. 69-2382);*

*6. Lietuvos Respublikos asmens duomenų teisinės apsaugos Įstatymas (Žin., 1996, Nr. 63-1479; 2003, Nr. 15-597);*

*7. Lietuvos Respublikos valstybės ir tarnybos paslapčių Įstatymas (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29);*

*8. Lietuvos Respublikos autorių teisių ir gretutinių teisių Įstatymas (Žin., 1999, Nr. 50-1598);*

*9. Lietuvos Respublikos patentų Įstatymas (Žin., 1994, Nr. 8-120);*

*10. Lietuvos Respublikos mokėjimų Įstatymas (Žin.,1999, Nr. 97-2775; 2003, Nr. 61-2753);*

*11. Europos Sąjungos Tarybos 2005 m. vasario 24 d. pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas (Official Journal L 069 , 16/03/2005 P. 0067 – 0071);*

*12. Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimas Nr. 451 „Dėl Valstybės informacinių sistemų steigimo ir Įteisinimo taisyklių patvirtinimo“ (Žin., 2004, Nr. 58-2061).*

*Vadovaujantis Lietuvos Respublikos teisės aktais, galima išskirti dvi kompiuterinės informacijos rūšis:*

*1) viešoji informacija (prieinama visiems vartotojams);*

*2) neviešoji (konfidencialioji) informacija (prieinama tik tiems vartotojams, kuriems tokia galimybė suteikta teisės aktų nustatyta tvarka).*

*Neviešajai informacijai priskiriama tokia informacija, kurios tvarkymą, saugojimą, kaupimą, naudojimą ir platinimą riboja Lietuvos Respublikos teisės aktai (Valstybės ir tarnybos paslapčių Įstatymas, Asmens duomenų teisinės apsaugos Įstatymas, Autorių ir gretutinių teisių Įstatymas, Elektroninių ryšių Įstatymas ir kt.). Tokiai informacijai paprastai suteikiama paslapties kategorija, – tai valstybės, tarnybos, komercinės, asmens duomenų ir kt. paslaptys, taip pat autorių ir gretutinių teisių objektu esanti informacija (intelektinė nuosavybė) bei privačioji informacija (asmens privataus gyvenimo duomenys, leidžiantys jį identifikuoti). Minėtų kategorijų informacija gali būti saugoma ir perduodama elektroniniu būdu telekomunikaciniais tinklais ir informacinėmis sistemomis (telefono judriojo ir fiksuoto ryšio, radijo ryšio,*

*elektroninio pašto ir kt. priemonėmis), taip pat paštu ir kitais būdais. Disponuoti konfidencialia informacija gali tik tie asmenys, kuriems ši teisė suteikta Įstatymų nustatyta tvarka. Be to, būtina pastebėti, jog Įstatymo saugoma yra bet kuri informacija, kurios neteisėtas panaudojimas gali padaryti žalos jos savininkui, valdytojui, tvarkytojui, naudotojui ar kitam asmeniui.*

*Lietuvos Respublikos valstybės registrų Įstatymas reglamentuoja valstybės ir žinybinių registrų duomenų tvarkymą ir apsaugą, apibrėžia duomenų tvarkymo sąvoką – tai „bet kurie su registro duomenimis atliekami veiksmai: duomenų rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas (papildymas ar taisymas), teikimas, paskelbimas, naudojimas, loginės ir (ar) aritmetinės operacijos, duomenų paieška, naikinimas ir kiti veiksmai“ ir šių veiksmų vykdymo tvarką.*

*Lietuvos Respublikos elektroninių ryšių Įstatymas reglamentuoja visuomeninius santykius, susijusius su elektroninių ryšių paslaugomis, tinklais ir su jais susijusiomis priemonėmis bei paslaugomis, elektroninių ryšių išteklių naudojimu, viešųjų elektroninių ryšių paslaugų ir tinklų saugumą, ryšio slaptumą, srauto duomenų tvarkymą (tačiau nereglamentuoja visuomeninių santykių, susijusių su paslaugomis, teikiamomis naudojant nurodytus tinklus ir paslaugas, taip pat elektroninių ryšių tinklais perduodamo turinio ir su juo susijusių paslaugų).*

*Konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“ siekiama užtikrinti, kad, tvarkant asmens duomenis automatizuotai visų šalių teritorijose būtų gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia, jo teisė Į privatų gyvenimą.*

*Lietuvos Respublikos asmens duomenų teisinės apsaugos Įstatymas reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas, bylas, sąvadus ir kita. Įstatymas nustato fizinių asmenų kaip duomenų subjektų teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis.*

*Lietuvos Respublikos valstybės ir tarnybos paslapčių Įstatymas reglamentuoja Įslaptintos informacijos apsaugą, automatizuoto duomenų apdorojimo sistemų ir tinklų (ADA sistemos ir tinklai) apsaugą, apibrėžia aktualius terminus: „Įslaptinta informacija – paslapčių subjekto pripažinta valstybės ar tarnybos paslaptimi informacija apie dokumentų, darbų, gaminių ar kitų objektų buvimą, esmę ar turinĮ, taip pat tokia paslaptimi pripažinti patys dokumentai, darbai, gaminiai ar kiti objektai“; „Įslaptintas dokumentas – valstybės ar tarnybos paslaptimi pripažinta fiksuota informacija, nesvarbu, koks jos fiksavimo būdas ir informacijos laikmenos (grafiniai darbai, atlikti Įvairiais būdais: parašyti ranka, išleisti spaustuvėje, išspausdinti rašomąja mašinėle, surinkti kompiuteriu, nupiešti ar nubraižyti; vaizdo ar garso Įrašai, kompiuterių informacijos rinkmenos, kino ir fotografijos negatyvai, pozityvai ar kiti informacijos masyvai), taip pat bet kokiu būdu ar priemonėmis padarytos tokios informacijos laikmenų kopijos“; „Įslaptinti gaminiai – valstybės ar tarnybos paslaptimi pripažinti Įvairūs Įrenginiai, sistemos, ginkluotė, karinės, kompiuterinės bei kitos technikos Įranga, kompleksai, agregatai, prietaisai, programinė Įranga ir chemijos produkcija“; „Įslaptinti darbai – valstybės ar tarnybos paslaptimi pripažinti mokslo, tyrimo, bandymų, projektavimo, techninio aptarnavimo darbai bei technologiniai procesai“; „ADA sistemų ir tinklų apsauga –*

*mechaninių, programinių, procedūrinių ir elektroninių apsaugos priemonių visuma, užtikrinanti ADA sistemose ir tinkluose saugomos, apdorojamos bei šiais tinklais perduodamos Įslaptintos informacijos slaptumą (konfidencialumą), prieinamumą teisėtiems informacijos vartotojams bei tokios informacijos vientisumą ir autentiškumą“.*

*Lietuvos Respublikos autorių teisių ir gretutinių teisių Įstatymas nustato: 1) autorių teises Į literatūros, mokslo ir meno kūrinius (autorių teises); 2) atlikėjų, fonogramų gamintojų, transliuojančiųjų organizacijų ir audiovizualinio kūrinio (filmo) pirmojo Įrašo gamintojų teises (gretutines teises); 3) duomenų bazių gamintojų teises (sui generis teises) (1 straipsnis). Šis Įstatymas apibrėžia duomenų bazės ir kompiuterių programos terminus: „**duomenų bazė** – susistemintas ar metodiškai sutvarkytas kūrinių, duomenų arba kitokios medžiagos rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu, išskyrus kompiuterių programas, naudojamas tokių duomenų bazėms kurti ar valdyti“; „**kompiuterių programa** – žodžiais, kodais, schemomis ar kitu pavidalu pateikiamų instrukcijų, kurios sudaro galimybę kompiuteriui atlikti tam tikrą užduotĮ ar pasiekti tam tikrą rezultatą, visuma, kai tos instrukcijos pateikiamos tokiomis priemonėmis, kurias kompiuteris gali perskaityti; ši sąvoka apima ir parengiamąją projektinę tokių instrukcijų medžiagą, jeigu pagal ją galima būtų sukurti minėtą instrukcijų visumą“, reglamentuoja kompiuterinių programų, duomenų bazių kūrėjų ir gretutinių teisių apsaugą. Lietuvos Respublikos patentų Įstatymas taip pat reguliuoja intelektinės nuosavybės teisių gynimą, išradimų kaip pramoninės nuosavybės objektų Įteisinimą, nors išradimais nelaikomos kompiuterių programos bei informacijos teikimo būdai (2 straipsnio 1 dalies 3, 4 punktai).*

*Lietuvos Respublikos mokėjimų Įstatymas reglamentuoja kredito Įstaigos ir kliento santykius, susijusius su elektroninių mokėjimo priemonių (nuotolinės prieigos mokėjimo priemonių ir elektroninių pinigų) naudojimu, autentiškumo ir tapatybės patvirtinimo procedūras.*

*Valstybės informacinių sistemų steigimo ir Įteisinimo taisyklės reglamentuoja valstybės informacinių sistemų (išskyrus valstybės registrus) steigimo ir Įteisinimo procedūrą, nustato, kad informacinės sistemos steigėjas, teikdamas derinti informacinės sistemos nuostatų projektą Vidaus reikalų ministerijai, kartu turi pridėti informacinės sistemos duomenų saugos nuostatus, parengtus vadovaujantis Tipiniais duomenų saugos nuostatais, patvirtintais vidaus reikalų ministro 2003 m. liepos 16 d. Įsakymu Nr. IV-272 (Žin., 2003, Nr. 76-3511).*

**4 priedas. Statistiniai duomenys**

PASTABOS:

1. Šiame priede pateikiamos sudarytos statistinių duomenų lentelės su diagramomis (1-15 lentelės) bei panaudotos statistinių kortelių formos: nusikalstamos veikos statistinė kortelė (10 kortelė); tyrimo rezultatų statistinė kortelė (20 kortelė); asmens, įtariamo (kaltinamo) nusikalstamos veikos padarymu, statistinė kortelė (30 kortelė).

2. Lentelėse ir diagramose nurodomi statistiniai duomenys, gauti iš Lietuvos Respublikos vidaus reikalų ministerijos Nusikalstamų veikų žinybinio registro bei Įtariamų, kaltinamų ir teistų asmenų žinybinio registro. Statistinius duomenis pateikė šių registrų tvarkytojas – Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos Statistikos skyrius, statistinę analizę atliko bei lenteles ir diagramas sudarė autorė.

3. Statistinių duomenų paieška minėtuose registruose atlikta pagal 10 kortelės 19 eilutės 85 požymį („19. Pasikėsinimo dalykas: kompiuterinė informacija ir sistemos (85)“) bei 21 eilutės 74 ir 75 požymius („21. Nusikalstamos veikos padarymo Įrankiai ir priemonės: kompiuterinė technika (74), internetas (75)“); surinkti duomenys apie: 1) nusikalstamą veiką (20 kortelė - BK straipsnis, stadija, sprendimas ir kt.); 2) Įtariamą, kaltinamą asmenį (30 kortelė - fizinis ar juridinis asmuo, amžius, lytis, tautybė, išsilavinimas, užimtumas, bendrininkavimas ir kt.).

**5 priedas. Lietuvos kriminalinės policijos biuro Nusikaltimų tyrimo vyriausiosios valdybos Nusikaltimų elektroninėje erdvėje tyrimo skyriaus pareigūnų atsakymų Į pateiktą klausimyną apibendrinimas**

1. Kokios, Jūsų nuomone, pagrindinės kompiuterinių (elektroninių) nusikaltimų tyrimo klaidos? (nurodyti tipines, dažniausiai pasitaikančias arba svarbiausias pirminių ikiteisminio tyrimo veiksmų – apžiūros, kratos, poėmio klaidas)

1. leidžiama dirbti su tiriamuoju kompiuteriu jo savininkui, tiesioginiam vartotojui ar kitam suinteresuotam asmeniui;
2. neprofesionaliai atliekami veiksmai su tiriamuoju kompiuteriu ar informacijos laikmenomis;
3. nepasitelkiamas informacinių technologijų specialistas;
4. sudaroma galimybė kaltinamojo gynėjui teisminio bylos nagrinėjimo metu paneigti teismui pateiktos programinės Įrangos autentiškumą, t.y. jos atitikimą tai Įrangai (jos būsenai), kuri buvo kompiuteryje poėmio metu;
5. nesugebama tinkamai užfiksuoti ir išsaugoti elektroninių Įkalčių, duomenų;
6. tiriamasis kompiuteris nepatikrinamas dėl virusų ar programinių užsklandų;
7. patikrinamos ne visos kompiuterinės laikmenos;
8. neužfiksuojamos kompiuterinės Įrangos sąsajos tinkle, informacinėje sistemoje;
9. kita (nurodyti).

**Atsakymas:**

| |
|---|
| 1; 2; 5; 7 |

2. Kas lemia kompiuterinių (elektroninių) nusikaltimų tyrimo problemas? (nurodyti svarbiausias priežastis)

1. tyrėjų specialiųjų žinių arba praktinių Įgūdžių kompiuterinių technologijų srityje trūkumas;
2. nėra parengtos kompiuterinių nusikaltimų tyrimo metodikos, metodinių rekomendacijų;
3. Lietuvos teisinės bazės trūkumai:
3.1. BK normų netikslumas ar trūkumas,
3.2. BPK normų netikslumas ar trūkumas,
3.3. teisės aktų, reglamentuojančių informacinių sistemų veiklą, elektroninės informacijos saugumą, netobulumas;
3.4. terminologijos problemos;
4. tyrėjai neturi galimybės pasitelkti kompiuterinių technologijų specialistų, ekspertų;
5. tyrėjams trūksta specialių techninių ar programinių priemonių, Įrangos;
6. kita (nurodyti).

**Atsakymas:**

| |
|---|
| 1; 3.2; 5; |

3. Kokie kompiuterinių (elektroninių) nusikaltimų Įvykdymo būdai dažniausiai naudojami Lietuvoje? (nurodyti vieną ar kelis punktus iš pateikto sąrašo)

**1. Naudojant perėmimo metodus:**

1.1. Tiesioginis perėmimas – kai prisijungimas Įvykdomas tiesiogiai prie ryšio kanalų ar prie duomenų perdavimo Įrangos mazgų (perėmimo objektu gali būti kabelinės ar laidinės sistemos, radijo ar palydovinio ryšio sistemos);

1.2. Netiesioginio (nuotolinis) elektromagnetinis perėmimas – Įvykdomas per Įrangos šalutinį spinduliavimą (vaizduoklio, spausdintuvo, ryšio sistemų), be to, pakankamai dideliu atstumu nuo spinduliuojančio objekto.

**2. Naudojant neteisėtos prieigos metodus:**

2.1. "Sekimas paskui kvailį" *(pigbacking)* – tai neteisėtas patekimas Į uždaras zonas, sekant paskui teisėtą

vartotoją arba kartu su juo.

2.2. "Paskui uodegą" *(between the lines entry)* – tai prisijungimas prie teisėto vartotojo linijos ir, po šio vartotojo ryšio seanso pabaigos, prieigos prie sistemos tęsimas vartotojo vardu.

2.3. "Įsilaužimas" *(hacking)* – šis metodas paprastai naudojamas Įsiskverbimui Į svetimas informacines sistemas, naudojantis specialia programine Įranga, parenkant identifikuojančius teisėtų vartotojų požymius (paprastai slaptažodžius ir vardus).

2.4. "Lėtas parinkimas (lėta atranka)" *(browsing)* – tai prisijungimas prie kompiuterio vieną kartą aptikus silpnąsias apsaugos sistemos vietas ar trūkumus bei vėliau jais naudojantis pagal poreikĮ.

2.5. "Spragos paieška (klaidos paieška)" *(trapdoor entry)* – šis metodas remiasi programos klaidos ar spragos, kuri aptinkama analizuojant programos darbą, panaudojimu.

2.6. "Liukas" *(trapdoor)* – tai ankstesnio metodo patobulintas variantas, kai aptikus programos klaidą ar spragą, ji dar pakoreguojama, papildoma naujomis komandomis, kuriomis vėliau pasinaudojama.

2.7. "Maskaradas (apsišaukėlis)" *(masquerading)* – tai Įsiskverbimas Į kompiuterinę sistemą, apsimetant teisėtu vartotoju, sužinojus jo kodą ar slaptažodĮ, jei nėra galimybių papildomai identifikuoti asmenĮ.

2.8. "Mistifikacija" *(spoofing)* – šis metodas techniškai pakankamai sudėtingas, kai pažeidėjas, formuodamas teisingas užklausas ir atsakymus, imituoja serverio darbą, sukurdamas vartotojui prisijungimo prie sistemos Įspūdį, taip jĮ suklaidindamas ir gaudamas dominančią informaciją, pvz., vartotojo kodus.

2.9. "Avarinė programa" – šis metodas remiasi ta aplinkybe, kad paprastai Į apsaugos sistemas Įdiegiamos specialios programos, kurios naudojamos ypatingais atvejais, jei sutrinka sistemos darbas, ir skirtos greitai apeiti apsaugą. Turėdamas tokią programinę priemonę, pažeidėjas gali prieiti prie visų kompiuterių tinklo išteklių.

2.10. "Sandėlis be sienų" – tai pasinaudojimas atsitiktinai susiklosčiusia palankia situacija, pvz., sistemos gedimu ar trūkumu, dėl kurio tampa prieinami ne tik savi, bet ir kitų vartotojų failai.

**3. Naudojant manipuliacijų metodus:**

Šiai grupei priskiriami nusikaltėlių veiksmai, kuriais manipuliuojama duomenimis arba kompiuterio komandomis; dažniausiai siekiama pakeisti vertybių apskaitos, buhalterinius duomenis ar Įtakoti šių duomenų srautus.

3.1. Duomenų pakeitimas – šio metodo esmę sudaro neteisingos informacijos Įvedimas, t.y. duomenų pakeitimas arba naujų Įvedimas, po kurio automatizuoto apdorojimo sistemos pateikia neteisingus rezultatus.

3.2. Kodo pakeitimas – tai informacijos Įvedimo, saugojimo, apdorojimo, išvedimo ar kitos funkcijos arba kodo iškreipimas, kuris nepakeičia pačios programos funkcionavimo, bet, pvz., neteisingai koduoja pasirinktų sumų pervedimą. Kodo pakeitimas gali būti aptiktas tik atlikus detalią programos duomenų analizę.

3.3. Modeliavimas – tai programinės Įrangos naudojimas modeliuojant, kaip elgsis Įrenginys arba sistema. Šis metodas naudojamas analizuojant procesus, Į kuriuos nusikaltėliai planuoja Įsiterpti, ir planuojant nusikaltimo Įvykdymo metodus.

3.4. „Trojos arklys" – tai būdas, kurio metu Į programą slaptai Įrašomos tokios komandos, kurios padeda Įvykdyti kitas, programos savininko nenumatytas, funkcijas, tačiau tuo pat metu išsaugomas ir pirminis programos funkcionalumas.

3.5. Kompiuteriniai virusai - speciali programa, kuri sugeba savarankiškai prisijungti prie kitų programų (užkrėsti jas) ir jas paleidžiant vykdyti Įvairius neplanuotus, nepageidaujamus veiksmus: trinti duomenis ir informaciją, gadinti failus ir katalogus, perpildyti kompiuterio atmintĮ, sutrikdyti jo darbą.

3.6. Saliami ataka *(salami attack)* – buhalterinėms operacijoms Įtakoti naudojama Trojos arklio taktika, pagrĮsta aritmetinių sumų apvalinimu (kitaip tariant, sąskaitų apvalinimo metu gautų liekanų pasisavinimas).

3.7. Loginė bomba *(logic bomb)* – slaptas komandų rinkinio Įterpimas Į programą, kuris turi pradėti veikti tam tikromis sąlygomis.

3.8. Laiko bomba *(time bomb)* – loginės bombos atmaina, kurios veikimo sąlyga yra tam tikras laiko momentas ar laiko intervalas.

3.9. Asinchroninė ataka – tai labai sudėtingas programinis metodas, kurĮ gali sudaryti dviejų ar kelių vartotojų, kurių komandas sistema apdoroja vienu metu, komandų sukeitimas ar kitoks operacinės sistemos veiklos sutrikdymas, pažeidžiantis ar apsunkinantis informacijos apdorojimo procesus.

**4. Naudojant kompleksinius metodus (kelių metodų derinius).**

## Atsakymas:

| |
|---|
| 1.1; 2.3; 3.4; 3.5 |

4. Tipinės (dažniausios) tyrimo situacijos:

(Tyrimo situaciją sąlygoja tyrėjo turima pradinė kriminalistiniu požiūriu svarbi informacija. Pirminių tyrimo, operatyvinių veiksmų visuma, jų atlikimo nuoseklumas priklauso nuo konkrečios tyrimo situacijos. Nurodyti dažniausiai pasitaikančią tyrimo situaciją)

A. Atsižvelgiant Į duomenų apie Įvykdytą nusikaltimą gavimo šaltinĮ, skiriamos šios situacijos:

a1. nukentėjęs asmuo savarankiškai aptinka kompiuterinĮ nusikaltimą, numano, kas yra kaltininkas, ir praneša tai teisėsaugos Įstaigai;

a2. nukentėjęs asmuo savarankiškai aptinka kompiuterinĮ nusikaltimą, tačiau nežino kaltininko ir praneša tai teisėsaugos Įstaigai;

a3. Įvykdyto kompiuterinio nusikaltimo duomenys paaiškėja iš kitų šaltinių (dažniausiai teisėsaugos pareigūnams tiriant kitą nusikaltimą)

B. Atsižvelgiant Į turimų duomenų apie nusikaltimą ir ĮtariamąjĮ išsamumą, skiriami šios situacijos:

b1. nėra duomenų apie nusikaltimo Įvykdymo būdą ir Įtariamojo asmenybę, žinomos tik pasekmės, nukentėjusysis;

b2. yra duomenų apie nusikaltimo Įvykdymo būdą, bet nėra duomenų apie Įtariamojo asmenybę;

b3. yra duomenų apie nusikaltimo Įvykdymo būdą, Įtariamojo asmenybę ir kitas aplinkybes;

b4. Įtariamasis sulaikytas nusikaltimo vietoje su Įkalčiais.

**Atsakymas:**

| |
|---|
| a1; a2; b1 |

5. Kompiuterinių nusikaltimų subjekto (Įtariamojo, kaltinamojo) charakteristika (nurodyti tipines, dažniausiai pasitaikančias savybes)

| **Klausimas** | **Atsakymas** |
|---|---|
| Amžius (nuo iki) - | 16-30 m. |
| Išsilavinimas (aukštasis universitetinis, profesinis specialusis, vidurinis, nebaigtas vidurinis) - | aukštasis universitetinis |
| Intelekto lygis (labai aukštas, aukštas, vidutinis, žemas) - | aukštas |
| Įgūdžiai (profesionalas programuotojas, vartotojo lygiu dirbantis kompiuteriu asmuo, saugos darbuotojas, mėgėjas, kt.) - | vartotojo lygiu dirbantis kompiuteriu asmuo |
| Užimtumas (ne valstybinės Įmonės ar Įstaigos darbuotojas, valstybės tarnautojas, bedarbis, studentas ar moksleivis, buhalteris ar finansininkas, kt.) - | studentas ar moksleivis;<br>ne valstybinės Įmonės ar Įstaigos darbuotojas |
| Bendrininkavimas (veikia vienas ar su bendrininkais) - | veikia vienas (50 proc.);<br>veikia su bendrininkais (50 proc.) |