

1 priedas. Interpolo Generalinio Sekretoriato patvirtintas vieningas kompiuterini nusikaltim kodifikatorius

1. QA – nesankcionuota prieiga ir per mimas:

QAH – informacijos per mimas panaudojant specialias technines priemones;

QAT – laiko vagyst (atsiskaitymo už pasinaudojim automatizuotomis informacin mis sistemomis vengimas);

QAZ – kitos nesankcionuotos prieigos ir per mimo r šys.

2. QD – kompiuterini duomen pakeitimas:

QDL – login bomba (komand , suveikian i tam tikromis s lygomis, rinkinys);

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

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

QDZ – kiti duomen pakeitimo b dai.

3. QF – kompiuterinis suk iavimas:

QFC – suk iavimas panaudojant bankomatus;

QFF – kompiuterinis padirbin jimas (kortel ar pan.);

QFG – suk iavimas panaudojant žaidimo automatus;

QFM – manipuliacija su vedimo ir išvedimo programomis (klaiding duomen vedimas ir toki program rezultat analiz);

QFP – suk iavimas panaudojant atsiskaitymo priemones (pinig pagrobimas – labiausiai paplit s kompiuterinis nusikaltimas);

QFT – telefoninis suk iavimas (pasik sinimas telekomunikacini paslaug sistemas);

QFZ – kiti kompiuterinio suk iavimo b dai.

4. QR – neteis tas kopijavimas:

QRG – kompiuterini žaidim ;

QRS –programin s rangos;

QRT – puslaidininki rangos topologijos;

QRZ – kitas neteis tas kopijavimas.

5. QS – kompiuterinis sabotažas:

QSH – aparatin s rangos (kompiuterio darbo sutrikdymas);

QSS – programin s rangos (informacijos sunaikinimas, blokavimas);

QSZ – kitos sabotažo r šys.

6. QZ – kiti kompiuteriniai nusikaltimai:

QZB – panaudojant kompiuterines skelbimo lentas;

QZE – informacijos, sudarančios komercinį 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 šešias grupes, kiekviena kompiuterinių nusikaltimų grupė detalizuojama nurodant jai priskirtus nusikaltimus, turinčius savo raidinį indeksą.

2 priedas. Veik , susijusi su kompiuterini technologij panaudojimu, kriminalizavimas Europos S jungos valstyb se ir teis s akt apžvalga

Valstyb	Neteis - tas kompiu- terin s informa- cijos rinkimas	Kenk - jiškos progra- mos	Atsisa- kymas aptar- nauti (DNS)	Bandy- mas sibrauti	Neteis ta prieiga prie informa- cijos	Neteis - tas informa- cijos per mi- mas	Neteis - tas informa- cijos pakeiti- mas	Neteis - ta prieiga prie ryši sistem
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.
Liuksem- burgas	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.
Pranc zija	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 vardintos s lyginai;

Ne¹ – veika nekriminalizuota, už j netaikoma nei administracin , nei baudžiamoji atsakomyb ;

Krim.² – veika kriminalizuota, t.y. už j taikoma baudžiamoji atsakomyb ;

Adm.ats.³ – už veik taikoma administracin atsakomyb .

Europos Sąjungos valstybi teisės aktai, susijusi su kompiuterini nusikaltimų reglamentavimu bei teisine atsakomybe už šias veikas, apžvalga

Airija. Airija priklauso bendrosios teisės sistemai, tad baudžiamieji statymai nėra kodifikuoti, o atsakomybė už nusikaltimus pažangi 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 vykdžius nusikaltimą, neatsižvelgiant tai, ar jam pavyko duomenis gauti. Už šį veiksmą numatyta bausmė – bauda arba laisvės atėmimas iki 3 mėnesių.

Austrija. Austrijos statymai nenumatė baudžiamosios atsakomybės už nusikaltimus, susijusius su kompiuterinėmis technologijomis, iki 2002 m. Baudžiamojo kodekso pataisais. Administracinė atsakomybė už tam tikrus kompiuterinius pažeidimus numatyta Akte dėl duomenų apsaugos, priimtame 2000 m., pavyzdžiui, vadovaujantis šio Akto 52 straipsniu, administracinė atsakomybė netaikoma asmuo, neteisėtai gavęs prieigą prie duomenų, taip pat sudaręs galimybes 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 vykdyti minėtus veikus.

gyvendindama Konvenciją dėl elektroninių nusikaltimų, Austrija parengė Baudžiamojo kodekso pataisus, kurios sigaliojo nuo 2002 m. spalio 1 d. Pataisus 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 ranga arba prieigos teisėmis (126 str.), nesąžiningą piktnaudžiavimą duomenų apdorojimu (148 str.) ir kompiuterinių duomenų suklastojimą (225 str.). Kitos Austrijos Baudžiamojo kodekso pataisos, sigaliojusios 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 sėbrovimą asmeninėms nuosavybės saugojimo vietoms (taikoma ir duomenims, saugomiems kompiuterinėje sistemoje), taip pat už duomenų perėmimą elektroniniuose ryšiuose (telekomunikaciniuose tinkluose). Už šias veikas numatyta bausmė – bauda arba laisvės atėmimas iki 6 mėnesių. Toki pa bausmė 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 siskverbimą viešaisias

ryši sistemas, duomen apdorojimo sistemas, specialias infrastrukturas (vandens tiekimo, elektros ir dujų tiekimo, sveikatos apsaugos) ir jų normalaus veikimo sutrikdymus.

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

Graikija. Graikijos Baudžiamojo kodekso 370 straipsnio 2 punktą kaip nusikaltimą vadinija neteisėta prieiga prie kompiuterinės sistemos. Vadovaujantis šia norma, asmuo, gavęs neteisėta prieiga prie kompiuterinių duomenų ar duomenų, perduodamą elektroniniuose ryšiuose tinklais, turi būti baudžiamas bauda arba laisvės atėmimu iki 3 mėnesių. Jei neteisėta prieiga prie duomenų vykdyta asmens, turinčio prieigą prie duomenų ar monos 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 neteisėta prieiga prie kompiuterio ar elektroninių ryšių (telekomunikacinių) sistemų, t.y. prie kompiuterių ar sistemų, apsaugotą saugumo priemonėmis, taip tokią prieigą prieš savininko valią, bausmė už tokią veiklą gali būti laisvės atėmimas iki 3 metų. Griežtesnė bausmė – laisvės atėmimas nuo 1 iki 5 metų – numatyta tuomet, kai šis nusikaltimas padaro pareigūnas ar asmuo, piktnaudžiaujantis savo galiojimais, asmuo, užsiimantis privataus detektyvo veikla, taip pat sistemos operatoriaus. Tai pati bausmė yra numatyta ir tuo atveju, kai nusikaltimas vykdytas 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 vykdymas prieš gynybinę 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 naudoti 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 programą, skirtą kompiuterinėms sistemoms pakenkti ar jas sunaikinti, platinimą. Ji nustato, kad baudžiamas neteisėtas perdavimas ar pardavimas kompiuterinėms programoms, kurios tikslas ar veikimo padarinys yra kompiuterio ar telekomunikacinių sistemų gedimas, duomenų ar programų, laikomose jose, sugadinimas, taip pat dalinis ar visiškas kompiuterio ar telekomunikacinių sistemų darbo sustabdymas.

Baudžiamojo kodekso 420 straipsnio 2 dalis kaip nusikaltimą apibrėžia visuomeninei

informacini infrastruktūrą, visuomenini duomenų bazių ar programų, veikiančių komunalinio aptarnavimo monose, 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 ne galiotas asmuo, sugadinantis ar sunaikinantis kompiuterinę sistemą ar programą, kompiuterinę informaciją ar duomenis, baudžiamas laisvės atėmimu nuo 6 mėnesių iki 3 metų. Jei nusikaltimas vykdytas 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 509¹, 509², 509³, 524 straipsniuose. 509¹ 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 slygojo duomenų, esančių sistemoje, pakeitimu ar sunaikinimu, tai laisvės atėmimo riba gali būti padidinta iki 2 metų. 509² straipsnis draudžia tyčinį automatinės duomenų apdorojimo sistemos funkcionalumo sutrikdymą ar pakeitimą. Bausmė už šiuos nusikaltimus - bauda arba laisvės atėmimas nuo 3 mėnesių iki 3 metų. 509³ straipsnis skirtas duomenų vientisumo ir kokybės apsaugai. Jis nustato, kad asmuo, tyčia ir be tam reikalingo galiojimo vedantis automatizuotą duomenų apdorojimo sistemą duomenis, trinantį ar keičiantį 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 sikišimas elektronini ryšiai (telekomunikacinės) 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, 161⁶, 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 tokios sistemos 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 šiuos veiksmus 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. Tokiu atveju bausmė numato ir trečioji 138a straipsnio dalis tais atvejais, kai asmuo vykdo neteisėtą prisijungimą, pasinaudodamas telekomunikacinėmis sistemomis, siekdamas naudoti 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 automatizuotą sistemą pasiklausymo ar pokalbių rašymo 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 baudžiamąjį atsakomybę už automatizuotą sistemą ar telekomunikacinę sistemą panaudojimą rašant pokalbius už gyvenamą patalpą ribą (sankcija - bauda arba laisvės atėmimas iki 3 mėnesių). 139c straipsnis numato baudžiamąjį atsakomybę asmeniui už tyčinę techninių priemonių panaudojimą duomenų, perduodamą telekomunikacinėmis sistemomis, tinklais ar prijungta ranga, per mimui ir rašymui, siekiant naudoti sau arba trečiajam asmeniui (sankcija – bauda arba laisvės atėmimas iki 1 metų). 139d straipsnis nustato, kad asmuo, teikiantis priemones, skirtas neteisėtai duomenų, perduodamą telekomunikacinėmis ar automatizuotomis sistemomis, per mimui ir rašymui, 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, rašymą arba per mimą 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, rašymą ar automatizuotą bei telekomunikacinę sistemą duomenų per mimą, arba padarant žalos šiuos duomenis prieinamais tretiesiems asmenims.

161^o straipsnis numato atsakomybę už tyčinę automatizuotą duomenų apdorojimo sistemą, duomenų saugojimo sistemą, telekomunikacinę sistemą sugadinimą ar sunaikinimą, pažeidžiant tokių sistemų funkcionalumą, pažeidžiant bet kokią šios sistemos apsaugai naudojamą priemonę efektyvumą. Už šio veiksmo numatyta bausmė - bauda arba laisvės atėmimas iki 6 mėnesių. Tuo atveju, kai vykdant veiksmą tiesioginiame rimtame pavojuje atsiduria prekės ar teikiamos paslaugos, laisvės atėmimo laikas gali būti padidintas iki 6 metų, o jeigu nusikaltimas su lygojo žmogaus mirtimi – 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 tyčinę neteisėtą duomenų, saugomą automatizuotose sistemose, perduodamą arba apdorojamą jomis, pakeitimą, ištrynimą, sugadinimą (sankcija - pinigine bauda arba laisvės atėmimas iki 2 metų). Laisvės atėmimo bausmė gali būti sugriežtinta iki 4 metų, jei asmuo vykdo nusikaltimą prieigai gauti, pasinaudodamas telekomunikacinėmis sistemomis, taip pat, jei duomenims padaryta žala yra labai didelė. Tokia pati bausmė numatyta už tyčinę neteisėtą duomenų, kurie kenkia sistemai, platinimą. 350b straipsnis nustato atsakomybę už nurodytas veikas, nesukeliantias didelės žalos (sankcija – bauda arba laisvės atėmimas iki 1 mėnesio).

351 straipsnis numato atsakomybę asmeniui, kuris tyčia naikina, gadina ar kitaip padarant netinkamomis naudotis automatizuotas sistemas, skirtas visuomenei būtiniam infrastruktūriniai sistemų funkcionavimui (dujų, vandens, elektros tiekimo sistemos, telekomunikacinės sistemos). Už tokio pobūdžio veiksmą numatoma sankcija - pinigine bauda arba laisvės atėmimas iki 3 metų.

Portugalija. Portugalijoje 1991 m. buvo priimtas specialus statymas Nr.109/91 dėl kompiuterinių nusikaltimų. Šio statymo 5 straipsnis numato atsakomybę už žalą, padarytą kompiuteriniams duomenims. Jis nustato, kad tyčinis dalinis ar visiškas duomenų arba programų pažeidimas ar sunaikinimas, siekiant naudoti sau ar tretiesiems asmenims, yra baudžiamas bauda arba laisvės atėmimu nuo 3 iki 10 metų, priklausomai nuo vykdyto nusikaltimo sunkumo. Pasiksinimas vykdyti nusikaltimą taip pat yra

baudžiamas. 6 straipsnis numato atsakomybę už kompiuterinį sabotаж – neteisėtai duomenis ar programą pakeitim, sunaikinimą, sutrikdymą arba siterpimą duomenų apdorojimo sistemoje kitomis priemonėmis, siekiant sutrikdyti sistemos darbą ar jos funkcionalumą. Asmeniui, vykdžiusiam tokią veiklą, 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 neteisėtai naudoti sau ar tretiesiems asmenims. Pasiksinimas vykdyti tokio pobūdžio veiklą taip pat yra baudžiamas. Sankcija – bauda arba laisvės atėmimas iki 3 metų, jei prieiga buvo pasiekta veikiant apsaugos sistemas ir priemones, ir iki 5 metų, jei prieiga buvo gauta siekiant išgauti komercines ar pramonines paslaptis, saugomas statymo, arba siekiant gauti didelę ekonominę naudą. 8 straipsnis skirtas neteisėtam duomenų perimimui telekomunikaciniuose tinkluose, panaudojant technines priemones ryšio sistemoje ar tinkle. Pasiksinimas vykdyti šiuos nusikaltimus 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 elektroninio ryšio (telekomunikaciniais) tinklais perduodamos informacijos turinį, turi būti baudžiamas bauda arba laisvės atėmimu iki vienerių metų. Tokia pati sankcija yra numatyta už minėtų neviešųjų pranešimų pažeidimą, sunaikinimą, nuslėpimą.

Suomijos Baudžiamojo kodekso 28 straipsnio bendroji norma, numatanti atsakomybę už neteisėtą svetimos kilnojamos nuosavybės, rangos, mašinų, mechanizmų panaudojimą, (sankcija - laisvės atėmimas iki vienerių metų), gali būti pritaikoma ir kompiuteriniams nusikaltimams. Suomijos Baudžiamojo kodekso 35 straipsnis, nustatantis atsakomybę už didelį žalą 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 klaidingumo, kurios taip pat taikomos ir kompiuteriniams nusikaltimams atžvilgiu, pavyzdžiui neteisėtai informacijos pakeitimo atvejams.

Suomijos 1984 m. Aktas dėl ryšio sutrikdymo taip pat gali būti taikomas tokiems nusikaltimams, kaip atsisakymas aptarnauti (DNS) ir kenkėjišką programą platinimas, tyčiniam telekomunikacinei sistemoje darbo sutrikdymui (sankcija už šiuos nusikaltimus – iki 2 metų laisvės atėmimo).

Švedija. Švedijos Baudžiamajame kodekse už kompiuterinius nusikaltimus atsakomybę yra numatoma skirtingi skyrių straipsniuose (4, 12, 13 skyriai). Baudžiamojo kodekso 4 skyriaus 8 straipsnis numato atsakomybę už veiksmus, kuriais ksinamasi ryšio slaptumą – neteisėtai ryšio perimimą 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 pašalinio asmens. 9a straipsnis numato, kad nusikalstamas yra neteisėtas pasiklausymas, atliktas su papildomu techniniu priemonių pagalba. 9c straipsnis skirtas duomenų paslapties pažeidimui – neteisėtai tos prieigos gavimui darbui su duomenimis.

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

nuosavybei, taip pat ir kompiuteriniams nusikaltimams, kuri metu buvo padaryta žala nuosavybei. Bauda arba laisvės atėmimas 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, sunaikinantis arba sugadinantis nuosavybę, turinti ypatingą reikšmę valstybės gynybai, teis saugai, 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 vykdymą numatyta bausmė - laisvės atėmimas iki 4 metų. 13 skyriaus 5 straipsnis nustato atsakomybę už sabotažą, kuris sukėlė ar galėjo sukelti didelį pavojų valstybei arba suklaidino daugelio žmonių žinias. Sankcija - laisvės atėmimas nuo 2 iki 10 metų arba iki gyvos galvos.

3 priedas. Lietuvos Respublikos teisės aktai, susijusi su visuomenini santyki saugaus kompiuterinės informacijos tvarkymo srityje reglamentavimu, s rašas bei aktuali teisės norm komentaras

1. Lietuvos Respublikos Konstitucija (pvz., 22 str. teigiama, jog žmogaus privatus gyvenimas nelieiamas; asmens susirašinėjimas, pokalbiai telefonu ar kitoks susižinojimas yra nelieiami; 23 str. teigiama, kad nuosavybės teisė yra nelieinama; nuosavybės teisės saugo statymas 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 statymas (Žin., 1996, Nr.86-2043; 2004, Nr. 124-4488);
5. Lietuvos Respublikos elektroninių ryšių statymas (Žin., 2004, Nr. 69-2382);
6. Lietuvos Respublikos asmens duomenų teisinės apsaugos statymas (Žin., 1996, Nr. 63-1479; 2003, Nr. 15-597);
7. Lietuvos Respublikos valstybės ir tarnybos paslapties statymas (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29);
8. Lietuvos Respublikos autorių teisių ir gretutinių teisių statymas (Žin., 1999, Nr. 50-1598);
9. Lietuvos Respublikos patentų statymas (Žin., 1994, Nr. 8-120);
10. Lietuvos Respublikos mokymų statymas (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 teisinimo taisykli patvirtinimo“ (Žin., 2004, Nr. 58-2061).

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

- 1) viešojoji informacija (prieinama visiems vartotojams);
- 2) neviešojoji (konfidencialioji) informacija (prieinama tik tiems vartotojams, kuriems tokia galimybė suteikta teisės akto nustatyta tvarka).

Neviešajai informacijai priskiriama tokia informacija, kurios tvarkymui, saugojimui, kaupimui, naudojimui ir platinimui riboja Lietuvos Respublikos teisės aktai (Valstybės ir tarnybos paslapties statymas, Asmens duomenų teisinės apsaugos statymas, Autorių ir gretutinių teisių statymas, Elektroninių ryšių statymas 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 privatioji informacija (asmens privataus gyvenimo duomenys, leidžiantys ją identifikuoti). Minėta kategorijų informacija gali būti saugoma ir perduodama elektroniniais būdais 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 statymu nustatyta tvarka. Be to, būtina pastebėti, jog statymo saugoma yra bet kuri informacija, kurios neteisėtus panaudojimas gali padaryti žalą jos savininkui, valdytojui, tvarkytojui, naudotojui ar kitam asmeniui.

Lietuvos Respublikos valstybės registrų statymas reglamentuoja valstybės ir žinybini registrų duomenų tvarkymą ir apsaugą, apibrėžia duomenų tvarkymo sąvokas – 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 ši veiksmų vykdymo tvarka.

Lietuvos Respublikos elektroninių ryšių statymas 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 visuomeninius santykius, susijusius 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 visose šalyse teritorijose būtų gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia, jo teisė privat gyvenimui.

Lietuvos Respublikos asmens duomenų teisinės apsaugos statymas reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiškai būdu, taip pat neautomatiškai būdu tvarkant asmens duomenis susistemintas rinkmenas: sąrašus, kartotekas, bylas, sąvadas ir kita. Statymas nustato fizinių asmenų kaip duomenų subjektų teises, ši teisė apsaugos tvarka, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis.

Lietuvos Respublikos valstybės ir tarnybos paslapties statymas reglamentuoja slaptintos informacijos apsaugą, automatizuoto duomenų apdorojimo sistemų ir tinklų (ADA sistemos ir tinklai) apsaugą, apibrėžia aktualius terminus: „slaptinta informacija – paslapties subjekto pripažinta valstybės ar tarnybos paslaptimi informacija apie dokumentą, darbą, gaminius ar kitus objektus buvimą, esmę ar turinį, taip pat tokia paslaptimi pripažinti patys dokumentai, darbai, gaminiai ar kiti objektai“; „slaptintas dokumentas – valstybės ar tarnybos paslaptimi pripažinta fiksuota informacija, nesvarbu, koks jos fiksavimo būdas ir informacijos laikmenos (grafiniai darbai, atlikti veiksmai: parašyti ranka, išleisti spaustuve, išspausdinti rašoma mašinu, surinkti kompiuteriu, nupiešti ar nubraižyti; vaizdo ar garso rašai, kompiuterinė informacijos rinkmenos, kino ir fotografijos neigiamai, pozityvai ar kiti informacijos masyvai), taip pat bet koks būdas ar priemonės padarytos tokios informacijos laikmenų kopijos“; „slaptinti gaminiai – valstybės ar tarnybos paslaptimi pripažinti vaizdiniai, sistemos, ginkluotieji, kariniai, kompiuteriniai bei kitos technikos rangai, kompleksai, agregatai, prietaisai, programinių rangų ir chemijos produkcija“; „slaptinti darbai – valstybės ar tarnybos paslaptimi pripažinti moksliniai, tyrimo, bandymų, projektavimo, techninio aptarnavimo darbai bei technologiniai procesai“; „ADA sistemos ir tinklų apsauga –

mechanini , programini , proced rini ir elektronini apsaugos priemoni visuma, užtikrinanti ADA sistemoje ir tinkluose saugomos, apdorojamos bei šiais tinklais perduodamos slaptintos informacijos slaptum (konfidencialum), prieinamum teis tiems informacijos vartotojams bei tokios informacijos vientisum ir autentiškum “.

Lietuvos Respublikos autori teisi ir gretutini teisi statymas nustato: 1) autori teises literat ros, mokslo ir meno k rinius (autori teises); 2) atlik j , fonogram gamintoj , transliuojan i j organizacij ir audiovizualinio k rinio (filmo) pirmojo rašo gamintoj teises (gretutines teises); 3) duomen bazi gamintoj teises (sui generis teises) (1 straipsnis). Šis statymas apibr žia duomen baz s ir kompiuteri programas terminus: „**duomen baz** – susistemintas ar metodiškai sutvarkytas k rini , duomen arba kitokios medžiagos rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu b du, išskyrus kompiuteri programas, naudojamas toki duomen baz ms kurti ar valdyti“; „**kompiuteri programa** – žodžiais, kodais, schemomis ar kitu pavidalu pateikiam instrukcij , kurios sudaro galimyb kompiuteriui atlikti tam tikr užduot ar pasiekti tam tikr rezultat , visuma, kai tos instrukcijos pateikiamos tokiomis priemon mis, kurias kompiuteris gali perskaityti; ši s voka apima ir parengiam j projektin toki instrukcij medžiag , jeigu pagal j galima b t sukurti min t instrukcij visum “, reglamentuoja kompiuterini program , duomen bazi k r j ir gretutini teisi apsaug . Lietuvos Respublikos patent statymas taip pat reguliuoja intelektin s nuosavyb s teisi gynim , išradim kaip pramonin s nuosavyb s objekt teisinim , nors išradimais nelaikomos kompiuteri programas bei informacijos teikimo b dai (2 straipsnio 1 dalies 3, 4 punktai).

Lietuvos Respublikos mok jim statymas reglamentuoja kredito staigos ir kliento santykius, susijusius su elektronini mok jimo priemoni (nuotolin s prieigos mok jimo priemoni ir elektronini pinig) naudojimu, autentiškumo ir tapatyb s patvirtinimo proced ras.

Valstyb s informacini sistem steigimo ir teisinimo taisykl s reglamentuoja valstyb s informacini sistem (išskyrus valstyb s registrus) steigimo ir teisinimo proced r , nustato, kad informacin s sistemos steig jas, teikdamas derinti informacin s sistemos nuostat projekt Vidaus reikal ministerijai, kartu turi prid ti informacin s sistemos duomen saugos nuostatus, parengtus vadovaujantis Tipiniais duomen saugos nuostatais, patvirtintais vidaus reikal ministro 2003 m. liepos 16 d. sakymu Nr. IV-272 (Žin., 2003, Nr. 76-3511).

4 priedas. Statistiniai duomenys

PASTABOS:

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

2. Lentelėse ir diagramose nurodomi statistiniai duomenys, gauti iš Lietuvos Respublikos vidaus reikalų ministerijos Nusikalstamų veikų žinybinio registro bei tariamų, kaltinamų ir teisėtų asmenų žinybinio registro. Statistinius duomenis pateikė šis registrų tvarkytojas – Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos Statistikos skyrius, statistinį analizę atliko bei lenteles ir diagramas sudarė autorius.

3. Statistiniai duomenų paieška min tuose 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 rankiai ir priemonės: kompiuterinė technika (74), internetas (75)“); surinkti duomenys apie: 1) nusikalstamą veiką (20 kortelė - BK straipsnis, stadija, sprendimas ir kt.); 2) tariamą, kaltinamą asmenį (30 kortelė - fizinis ar juridinis asmuo, amžius, lytis, tautybė, išsilavinimas, užimtumas, bendrininkavimas ir kt.).

5 priedas. Lietuvos kriminalinis policijos biuro Nusikaltimų tyrimo vyriausiosios valdybos Nusikaltimų elektroninėje erdvėje tyrimo skyriaus pareigūnų atsakymų pateiktą klausimų apibendrinimas

1. Kokios, Jūsų nuomone, pagrindinės kompiuteriniai (elektroniniai) nusikaltimų tyrimo klaidos? (nurodyti tipines, dažniausiai pasitaikančias arba svarbiausias pirminio ikiteisminio tyrimo veiksmų – apžiūros, kratos, paieškos 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 programinėsrangos autentiškumą, t.y. jos atitikimą rangai (jos bus senai), kuri buvo kompiuteryje paieškos metu;
5. nesugebama tinkamai užfiksuoti ir išsaugoti elektroninių kalbų, duomenų;
6. tiriamasis kompiuteris nepatikrinamas dėl virusų ar programinių užsklandų;
7. patikrinamos ne visos kompiuterinės laikmenos;
8. neužfiksuojamos kompiuterinės rangos sąsajos tinkle, informacinėje sistemoje;
9. kita (nurodyti).

Atsakymas:

1; 2; 5; 7

2. Kas lemia kompiuteriniai (elektroniniai) nusikaltimų tyrimo problemas? (nurodyti svarbiausias priežastis)

1. tyrėjų specialieji žiniai arba praktiniai gūdžiai kompiuterinių technologijų srityje trūkumas;
2. nėra parengtos kompiuterinių nusikaltimų tyrimo metodikos, metodinių rekomendacijų;
3. Lietuvos teisinė bazė 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 galimybių pasitelkti kompiuterinių technologijų specialistus, ekspertus;
5. tyrėjams trūksta specialiųjų techninių ar programinių priemonių, rangos;
6. kita (nurodyti).

Atsakymas:

1; 3.2; 5;

3. Kokie kompiuteriniai (elektroniniai) nusikaltimų vykdymo būdai dažniausiai naudojami Lietuvoje? (nurodyti vieną ar kelis punktus iš pateikto sąrašo)

1. Naudojant per mimos metodus:

1.1. Tiesioginis per mimos – kai prisijungimas vykdomas tiesiogiai prie ryšio kanalų ar prie duomenų perdavimo rangos mazgų (per mimos objektu gali būti kabelinės ar laidinės sistemos, radijo ar palydovinio ryšio sistemos);

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

2. Naudojant neteisėtus prieigos metodus:

2.1. “Sekimas paskui kvailį” (pigbacking) – tai neteisėtas pateikimas uždaras zonas, sekant paskui teisėtai

vartotoj arba kartu su juo.

2.2. „Paskui uodeg“ (*between the lines entry*) – tai prisijungimas prie teisto vartotojo linijos ir, po šio vartotojo ryšio seanso pabaigos, prieigos prie sistemos taisyklės vartotojo vardu.

2.3. „silaužimas“ (*hacking*) – šis metodas paprastai naudojamas siskverbimui svetimas informacinės sistemos, naudojantis specialia programine ranga, parenkant identifikuojančius teisto vartotojų požymius (paprastai slaptažodžius ir vardus).

2.4. „Ltas parinkimas (lta atranka)“ (*browsing*) – tai prisijungimas prie kompiuterio vieną kartą aptikus silpnas apsaugos sistemos vietas ar trūkumus bei viliu 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 viliu pasinaudojama.

2.7. „Maskaradas (apsišauklis)“ (*masquerading*) – tai siskverbimas kompiuterinėje sistemoje, apsimetant teisto vartotoju, sužinojus jo kodą ar slaptažodį, jei nėra galimybių papildomai identifikuoti asmenį.

2.8. „Mistifikacija“ (*spoofing*) – šis metodas techniškai pakankamai sudėtingas, kai pažeidžias, formuodamas teisingas užklausas ir atsakymus, imituoja serverio darbą, sukurdamas vartotojui prisijungimo prie sistemos spūdį, taip jį suklaidindamas ir gaudamas dominanę informaciją, pvz., vartotojo kodus.

2.9. „Avarin programa“ – šis metodas remiasi ta aplinkybe, kad paprastai apsaugos sistemos diegiamos specialios programos, kurios naudojamos ypatingais atvejais, jei sutrinka sistemos darbas, ir skirtos greitai apeiti apsaugą. Turėdamos tokią programinę priemonę, pažeidžias gali prieiti prie visų kompiuterinio 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 kiti vartotojų failai.

3. Naudojant manipuliacij metodus:

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

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

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

3.3. Modeliavimas – tai programinės rangos naudojimas modeliuojant, kaip elgsis renginys arba sistema. Šis metodas naudojamas analizuojant procesus, kuriuos nusikaltėliai planuoja siterpti, ir planuojant nusikaltimo vykdymo metodus.

3.4. „Trojos arklys“ – tai būdas, kurio metu programai slaptai rašomos tokios komandos, kurios padeda vykdyti kitas, programos savininko nenumatytas, funkcijas, tačiau tuo pat metu išsaugomas ir pirminis programos funkcionalumas.

3.5. Kompiuteriniai virusai – specialia programa, kuri sugeba savarankiškai prisijungti prie kitų programų (užkrėsti jas) ir jas paleidžiant vykdyti vairius 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 takoti naudojama Trojos arklio taktika, pagrįsta aritmetiniu sumų apvalinimu (kitais variantais, skaitant apvalinimo metu gautą liekaną pasisavinimas).

3.7. Login bomba (logic bomb) – slaptas komandų rinkinio terpinimas programoje, kuris turi pradėti veikti tam tikromis sąlygomis.

3.8. Laiko bomba (time bomb) – loginis 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 situacijų sąlygoja tyrimo turima pradinė kriminalistiniu požiūriu svarbi informacija. Pirminis tyrimo, operatyvinių veiksmų visuma, jų atlikimo nuoseklumas priklauso nuo konkrečios tyrimo situacijos. Nurodyti dažniausiai pasitaikančios tyrimo situacijų)

A. Atsižvelgiant duomen apie vykdyt nusikaltim gavimo šaltin , skiriamos šios situacijos:

- a1. nukent j s asmuo savarankiškai aptinka kompiuterin nusikaltim , numano, kas yra kaltininkas, ir praneša tai teis saugos staigai;
- a2. nukent j s asmuo savarankiškai aptinka kompiuterin nusikaltim , ta iau nežino kaltininko ir praneša tai teis saugos staigai;
- a3. vykdyto kompiuterinio nusikaltimo duomenys paaišk ja iš kit šaltini (dažniausiai teis saugos pareig nams tiriant kit nusikaltim)

B. Atsižvelgiant turim duomen apie nusikaltim ir tariam j išsamum , skiriami šios situacijos:

- b1. n ra duomen apie nusikaltimo vykdymo b d ir tariamojo asmenyb , žinomos tik pasekm s, nukent jusysis;
- b2. yra duomen apie nusikaltimo vykdymo b d , bet n ra duomen apie tariamojo asmenyb ;
- b3. yra duomen apie nusikaltimo vykdymo b d , tariamojo asmenyb ir kitas aplinkybes;
- b4. tariamasis sulaikytas nusikaltimo vietoje su kal iais.

Atsakymas:

a1; a2; b1

5. Kompiuterini nusikaltim subjekto (tariamojo, kaltinamojo) charakteristika (nurodyti tipines, dažniausiai pasitaikan ias savybes)

Klausimas	Atsakymas
Amžius (nuo iki) -	16-30 m.
Išsilavinimas (aukštasis universitetinis, profesinis specialusis, vidurinis, nebaigtas vidurinis) -	aukštasis universitetinis
Intelektu lygis (labai aukštas, aukštas, vidutinis, žemas) -	aukštas
g džiai (profesionalas programuotojas, vartotojo lygiu dirbantis kompiuteriu asmuo, saugos darbuotojas, m g jas, kt.) -	vartotojo lygiu dirbantis kompiuteriu asmuo
Užimtumas (ne valstybin s mon s ar staigos darbuotojas, valstyb s tarnautojas, bedarbis, studentas ar moksleivis, buhalteris ar finansininkas, kt.) -	studentas ar moksleivis; ne valstybin s mon s ar staigos darbuotojas
Bendrininkavimas (veikia vienas ar su bendrininkais) -	veikia vienas (50 proc.); veikia su bendrininkais (50 proc.)