

**MYKOLO ROMERIO UNIVERSITETO  
TEIS S FAKULTETO  
KRIMINALISTIKOS KATEDRA**

**RENATA KA INSKAIT**

**NEAKIVAIZDINI STUDIJ  
BAUDŽIAMOSIOS TEIS S IR KRIMINOLOGIJOS PROGRAMA**

**TEMA  
KOMPIUTERINIAI NUSIKALTIMAI IR J TYRIMO YPATUMAI**

**Magistro baigiamasis darbas**

**Darbo vadovas – doc. dr.  
Ryšardas Burda**

**Vilnius, 2006**

## TURINYS

vadas .....	3 p.
<b>I. KOMPIUTERINI NUSIKALTIM SAMPRATA IR TEISINIS REGLAMENTAVIMAS</b>	
1. Kompiuterinio nusikaltimo samprata .....	5 p.
2. Kompiuterini nusikaltim klasifikacija ir r šys .....	11 p.
3. Nusikalstam veik , susijusi su kompiuterin mis technologijomis bei informacijos sauga, teisinis reglamentavimas .....	22 p.
3.1. Kompiuterini nusikaltim teisinis reglamentavimas Europos S jungos valstyb se .....	22 p.
3.2. Kompiuterini nusikaltim teisinis reglamentavimas Lietuvoje .....	28 p.
<b>II. KOMPIUTERINI NUSIKALTIM APIB DINIMO KRIMINALISTINIAI ASPEKTAI</b>	
4. Kompiuterini nusikaltim kriminalistin charakteristika .....	33 p.
4.1. Kompiuterini nusikaltim subjekto charakteristika .....	36 p.
4.2. Kompiuterini nusikaltim vykdymo laikas ir vieta .....	40 p.
4.3. Kompiuterini nusikaltim b dai .....	41 p.
4.4. Kompiuterini nusikaltim prietaisai ir priemon s .....	48 p.
<b>III. KOMPIUTERINI NUSIKALTIM TYRIMO METODIKOS YPATUMAI</b>	
5. Kompiuterini nusikaltim tyrimo veiksmai .....	50 p.
5.1. rodin tinos aplinkyb s .....	50 p.
5.2. Tipin s tyrimo situacijos ir kriminalistin s tyrimo uždutys .....	52 p.
5.3. Atskir tyrimo veism atlikimo ypatumai .....	57 p.
5.3.1. vykio vietos apži ra .....	62 p.
5.3.2. Kompiuterin s technikos priemoni apži ra ir po mis .....	65 p.
5.3.3. Kompiuterin s informacijos laikmen apži ra bei nusikalstamo poveikio jai p dsak paieška ir po mis .....	68 p.
5.3.4. Speciali j žini panaudojimas ir ekspertiz s skyrimas .....	71 p.
6. Pagrindin s kompiuterini nusikaltim tyrimo klaidos .....	75 p.
Išvados .....	79 p.
Santrauka	
Summary	
Literat ros s rašas	
Priedai	

## VADAS

Pasaulio valstybės sukurus globalų kompiuterinį tinklą ir vieningą informacinę erdvę, kompiuterinis nusikalstamumas taip pat gavo tarptautinį pobūdį, nes modernios informacinės bei telekomunikacinės technologijos teikiamos galimybės – multimedijos procedūros ir kitos teisiniai apribojimai praktiškai nevaržomas duomenų srautų judėjimas, informacijos mainų greitis ir anonimiškumas – aktyviai naudojamos tiek teisėtai, tiek neteisėtai tikslais. Vertinusi šias aplinkybes, Lietuvos Respublika, kurianti informacinei visuomenei egzistuoti būtina infrastruktūrą, integruotą globalius tinklus, turėtų pasiręsti sparčiai kintantiems asmenims ir visuomenės bendravimo formoms, naujiems socialinio ir ekonominio gyvenimo organizavimo būdams, o kartu ir naujai nusikaltimų rūšiai, susijusiai su informacinėmis technologijų panaudojimu, automatiniais kompiuteriniais duomenų tvarkymu (apdorojimu, saugojimu, siuntimu). Siekiant išvengti neigiamų pasekmių bei išspręsti grėsmingai plintančias informacijos saugos problemas, būtina pasinaudoti jau sukaupta užsienio šalių patirtimi kovojant su kompiuteriniu nusikalstamumu ir kuriant mokslinius metodologinius pagrindus teisiniam šios srities reguliavimui. Šiuo metu Lietuvoje jau pradėta tvarkyti teisės aktų, reglamentuojančių kompiuterizuotas informacines sistemas bei nusikalstamas veikas, kuriomis ksinamasi visuomeninius santykius kompiuterinės informacijos apdorojimo procese ir kompiuterinės informacijos saugumą, bazė, tačiau didėle problema, manome, lieka šios srities terminologijos teisinis neapibrėžtumas, be to, dar nėra parengtos kompiuterinio nusikaltimų tyrimo metodikos, pagrindinės susistemintos teorinės žinios ir patikrintos praktikoje. Tikėtina, jog tai sulygoja teisės teoretikų ir praktikų nuomonių dėl kompiuterinio nusikaltimų ir jų tyrimo metodų vaizdą bei vieningos pozicijos stygius.

Atsižvelgiant minėtų problemų aktualumą bei praktinį patirtį dirbant teisiniu darbu informacijos saugos ir elektroninių ryšių srityje, autorius buvo pasirinktas baigiamojo magistro darbo **tyrimo objektas** – baudžiamojo statymo numatytos visuomenei pavojingos veikos, darančios žalą visuomeniniams santykiams kompiuterinės informacijos tvarkymo srityje.

Šio darbo **tyrimo dalykas** – baudžiamojo statymo numatytos visuomenei pavojingos veikos, darančios žalą visuomeniniams santykiams kompiuterinės informacijos tvarkymo srityje, mokslinio apibūdinimo, teisinio reglamentavimo raidos ir kriminalistinės charakteristikos bei tyrimo metodikos ypatumai.

Pradedant tyrimą, autorius iškelia **hipotezę**, jog kompiuteriniai nusikaltimai, atsižvelgiant į pagrindinius struktūrinius elementus, technologijos savitumą (pasikėsinimo dalyko skaitmeninė forma, automatizaciją, duomenų perdavimo tinklų panaudojimą), yra atskira nusikaltimų rūšis, kuri ženkliai skiriasi nuo tradicinių nusikaltimų bei nėra tapati nusikaltimams elektroninėje erdvėje savaime, o kompiuteriniai nusikaltimai išskirtinomis savybėmis sulygoja ir šių nusikaltimų tyrimo ypatumus.

Taigi baigiamojo magistro **darbo tikslas** – išanalizavus m s valstyb s ir tarptautin praktik teorine mokslo doktrinos bei praktine teis k ros ir teis saugos institucij veiklos prasme, apibr žti modernios nusikaltim r šies – kompiuterini nusikaltim –samprat bei nustatyti esminius j tyrimo ypatumus. Pagrindiniai šio **darbo uždaviniai**, siekiant nurodyto tikslo, yra tokie: atlikti Lietuvos ir Europos S jungos bei kit šali patirties kompiuterini nusikaltim teisinio reglamentavimo srityje analiz , apib dinti kompiuterini nusikaltim savybes, r šis bei pateikti baudžiam j teisin ir kriminalistin j charakteristik , taip pat išanalizuoti kompiuterini nusikaltim tyrimo metodikos specifik , nustatyti tyrimo veiksm bendruosius ir specialiuosius reikalavimus bei pateikti rekomendacijas, kaip išvengti esmini šios r šies nusikaltim tyrimo klaid , kurios gal t s lygoti kompiuterin s informacijos praradim ar sugadinim , rasti ir tinkamai užfiksuoti kal ius, turin ius rodom j vert teismo bylos nagrin jimo metu.

Rašant darb , vertinant surinkt medžiag ir darant išvadas, naudoti teoriniai bei empiriniai **tyrimo metodai**: lyginamasis, lyginamasis istorinis, analitinis, apibendrinimo, dedukcinis, statistinis, dokument analiz s, profesin s patirties apibendrinimo ir kiti. Statistiniai duomenys, kuri analiz atliko autor , pateikti iš Vidaus reikal ministerijos Nusikalstam veik žinybinio registro bei tariam , kaltinam ir teist asmen žinybinio registro. Siekiant gauti praktini duomen apie kompiuterini nusikaltim tyrimo ir informacini sistem saugos ypatumus bei problemas, vertinti surinkt teorin medžiag bei pagr sti išvadas, buvo apibendrinta ikiteisminio tyrimo staig pareig n , taip pat Informatikos ir ryši departamento prie Vidaus reikal ministerijos informacijos saugos specialist profesin patirtis.

Šio darbo pagrindin d stomoji dalis **susideda iš trij skyri** , suskirstyt poskyrius: pirmajame skyriuje „*Kompiuterini nusikaltim samprata ir teisinis reglamentavimas*“ nagrin jama nusikalstam veik , susijusi su kompiuterin mis technologijomis bei informacijos saugos pažeidimu, apibr žimo problemos, kompiuterinio nusikaltimo sampratos ypatyb s ir raida, kompiuterini nusikaltim r šys ir klasifikacija, ši nusikaltim teisinio reglamentavimo Europos S jungos valstyb se ir Lietuvoje pagrindiniai bruožai; antrajame skyriuje „*Kompiuterini nusikaltim apib dinimo kriminalistiniai aspektai*“ pateikiama kompiuterini nusikaltim kriminalistin charakteristika, analizuojami kompiuterini nusikaltim subjekto, vykdymo laiko, vietos ir b d , taip pat prietais ir priemoni b dingi bruožai; tre iajame skyriuje „*Kompiuterini nusikaltim tyrimo metodikos ypatumai*“ apib dinama ši nusikaltim tyrimo metodika, nagrin jama kompiuterini nusikaltim rodin tinos aplinkyb s, tipin s tyrimo situacijos ir kriminalistin s tyrimo užduotys, atskir tyrimo veiksm atlikimo bendrieji ir specialieji reikalavimai, akcentuojama speciali j žini panaudojimo ir ekspertiz s skyrimo svarba ir ypatumai, analizuojamos pagrindin s kompiuterini nusikaltim tyrimo klaidos. Darbo pabaigoje pateikiamos išvados ir rekomendacijos, pagr stos atlikto tyrimo rezultatais.

# I. KOMPIUTERINI NUSIKALTIM SAMPRATA IR TEISINIS REGLAMENTAVIMAS

## 1. KOMPIUTERINIO NUSIKALTIMO SAMPRATA

vertinus Lietuvos bei tarptautin praktik tiek teorine mokslo darb , tiek praktine statym leidybos prasme, galima konstatuoti, kad šiuo metu n ra suformuota vieninga kompiuterinio nusikaltimo samprata. Tiesa, siekiant vardinti visuomenei pavojingas bei teis s akt draudžiamas veikas, vykdomas panaudojant kompiuterius, j tinklus ar kompiuterizuotas informacines sistemas (toliau – informacin s sistemas), paprastai vartojamas kompiuterinio nusikaltimo terminas (*angl. computer crime, rus.* ), ta iau dažnai sutinkami ir kiti terminai: kompiuteri naudojimo arba su kompiuteri naudojimu susij s nusikaltimas (*angl. computer-related crime*), elektroninis arba kibernetinis nusikaltimas (*angl. cyber crime*), informacinis nusikaltimas ar nusikaltimas informatikai (*pranc. delit informatique*), informacin s visuomen s nusikaltimas ir kt.

Teis s darbuose minima, kad kompiuterinio nusikaltimo terminas pirm kart buvo pavartotas maždaug septintajame pra jusio amžiaus dešimtmetyje Jungtini Amerikos Valstij (toliau – JAV) mokslin je literat roje. V liau šis terminas paplito ir kit šali praktikoje.

Galima pagr stai teigti, jog teisiškai tikslingiausia b t kompiuterinio nusikaltimo s vok apibr žti baudžiamosios teis s poži riu. Baudžiamosios teis s poži riu kompiuterinius nusikaltimus reik t suprasti kaip baudžiamojo statymo numatyt visuomenei pavojing veik , kuria k sinamasi visuomeninius santykius informacijos apdorojimo procese ir kompiuterin s informacijos saugum kaip nusikaltimo objekt , o nusikaltimo dalykas arba rankis b t kompiuterin informacija, kompiuteris, kompiuterinis tinklas arba informacin sistema.

Išanalizavus Europos S jungos, JAV, Rusijos ir kit valstybi mokslo darbuose pateikt kompiuterini nusikaltim samprat vairov , galima išskirti dvi pagrindines poži rio šiuos nusikaltimus kryptis: kompiuterini nusikaltim traktavimas pla i ja prasme ir siaur ja prasme.

Pirmosios krypties atstovai teigia, kad kompiuteriniai nusikaltimai – tai visos baudžiamojo statymo nustatytos visuomenei pavojingos veikos, kurias vykdan:

- a) nusikaltimo dalykas yra kompiuterin informacija (ar pats kompiuteris) arba
- b) nusikaltimo priemon ( rankis) yra kompiuteris. Reikia atkreipti d mes tai, kad pastaruoju atveju veik objektas gali b ti skirtingas, vadinasi prie j gali b ti priskirtas ir autori teisi pažeidimas, ir suk iavimas, jei jie vykdyti panaudojant kompiuterius. O atsižvelgiant dalyko plat traktavim , kompiuteriniu nusikaltimu bus laikoma ir kompiuterio vagyst .

Kompiuterini nusikaltim s vok pla i ja prasme aiškina Vokietijos ir Austrijos

baudžiamosios teisės teoretikai, kurie apibrėžia kompiuterinius nusikaltimus kaip baudžiamąjį veiksmą, kurį vykdančiam kompiuteris yra jos priemonė (instrumentas) arba objektas<sup>1</sup>.

Vienas iš plačiausiai traktavimo pavyzdžių yra su kompiuteriais susijusi nusikaltimų (*angl. computer-related crime*) terminas, apimantis visas kriminalizuotas veikas, kurioms vykdyti panaudojamas kompiuteris, informacinė sistema ar elektroninė erdvė (pvz., tikrovės neatitinkanti, asmens garbą ir orumą žeminanti duomenų sklaidimas internete).

Atkreiptinas dėmesys tai, kad šiuo metu vis populiaresnis ir plačiau naudojamas elektroninių nusikaltimų (*angl. cybercrime*) terminas paprastai atitinka kompiuterinį nusikaltimą sampratą plačiaja prasme. Taip šiuos nusikaltimus aiškina C.J.Magninas, M.Mukhtaras, tačiau šio termino kritikai teigia, jog elektroninis nusikaltimas nėra tiksliausia sąvoka, apibūdinanti nusikaltimus, vykdomus panaudojant elektroninę erdvę, nes šie nusikaltimai būdingi ne elektronikos sričiai ar elektronikos mokslui, o informatikos inžinerijai, kompiuterijos mokslams<sup>2</sup>. Vis dėlto būtina pastebėti, jog Europos Komisijos komunikate Tarybai ir Europos Parlamentui (COM (2000) 890 final) bei Konvencijos dėl elektroninių nusikaltimų paaiškinamajame memorandume<sup>3</sup> vartojamas elektroninių nusikaltimų terminas ir nurodoma, jog Konvencijoje yra kriminalizuojamos veikos, susijusios su kompiuteriniais nusikaltimais, taigi elektroninius nusikaltimus galima būtų traktuoti kaip kompiuterinius nusikaltimus plačiaja prasme, vykdomus panaudojant elektroninę erdvę.

Antrosios krypties atstovai, aiškinantys kompiuterinį nusikaltimą sąvoką siaurja prasme, kompiuteriniams nusikaltimams priskiria tik tokias baudžiamojo statymo nustatytas visuomenei pavojingas veikas, kurios atitinka du kriterijus:

a) šios veikos yra nurodytos specialiuose baudžiamojo statymo skirsniuose (pvz., Lietuvos Respublikos baudžiamajame kodekse XXX sk. „Nusikaltimai informatikai“) ir

b) šioms veikoms būdingas bendras pasikėsinimo objektas bei dalykas: nusikaltimo objektas yra visuomeniniai santykiai informacijos apdorojimo procese, o nusikaltimo dalykas yra kompiuterinė informacija.

vertinus užsienio valstybių bei Lietuvos statymų leidybos praktiką, galima daryti išvadą, jog šiuo metu vyrauja kompiuterinį nusikaltimą samprata siaurja prasme.

Būtina pastebėti, kad Lietuvos Respublikos baudžiamajame kodekse (LR BK, BK) sąvoka „kompiuterinis nusikaltimas“ nėra apibrėžta, taigi ji oficialiai nėra teisinta *de jure*, bet nepaisant šios aplinkybės Lietuvoje plačiau vartojama *de facto*. Atkreiptinas dėmesys tai, jog

<sup>1</sup> International review of penal law: computer crimes and other crimes against information technology.- Wurzburg, Germany, 1992. P.133.

<sup>2</sup> Civilka M., Lamanauskas T., Osinaitis G. ir kt. Informacinių technologijų teisė.- Vilnius, 2005. P.511.

<sup>3</sup> Explanatory Memorandum related to Convention on Cyber-Crime // <http://conventions.coe.int>; prisijungimo laikas: 2006-05-07.

galiojančiame Lietuvos Standarte LST ISO/IEC 2382-1: 1996 (atitinkančiame tarptautiniame standarte ISO/IEC 2382-1: 1993) ir jo pakeistame Lietuvos Standarte LST ISO/IEC 2382-1: 1993 jau 1993 m. buvo pateiktas kompiuterinio nusikaltimo apibrėžimas: „kompiuterinis nusikaltimas – tai nusikaltimas, padarytas naudojant, modifikuojant arba sugriaunant kompiuterinį techninį, programinį rangą arba duomenis“<sup>4</sup>. Nepaisant šio termino apibrėžimo, Lietuvos statym leidžia valia naujajame Baudžiamajame kodekse kompiuteriniai nusikaltimai vadinami kaip „nusikaltimai informatikai“ (BK XXX skyrius „Nusikaltimai informatikai“: kompiuterinis informacijos sunaikinimas ar pakeitimas; kompiuterinis programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas; kompiuterinis informacijos pasisavinimas ir skleidimas; neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo; neteisėtas disponavimas reikšmingais, kompiuteriniais programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti). Reikia pastebėti, jog „nusikaltimai informatikai“ terminas nevienareikšmiškai sutiktas Lietuvos teisės specialistų. Tarkime, šis terminas kritiškai vertina dr. D.Štītėlis, S.Toliušis leidinyje „Informacinė technologijų teisė“<sup>5</sup>. Galima konstatuoti, kad tiek pats terminas „nusikaltimas informatikai“, tiek šio Baudžiamojo kodekso skyriaus pavadinimas nėra tikslūs, nes šis nusikaltimų rėšinis objektas – informatika – Tarptautiniame žodžių žodyne<sup>6</sup> pirmiausia apibrėžiama kaip mokslo šaka ar tam tikra žiniavisa, o kompiuteriniais nusikaltimais ne tik nesiekiami moksliniai žiniai visumai, bet priešingai naudojamosi informatikos moksliniai žiniai kaip priemonė nusikaltimams daryti. Reikia pastebėti, kad Lietuvos statym leidžia „informatikos“ terminą traktuoti plačiau prasme kaip su informatikos mokslu susijusią praktinę veiklą, tuomet BAUDŽIAMOJO KODEKSO saugoma vertybė galėtų būti aiškinama kaip saugus ir netrukdomas kompiuterinis informacijos tvarkymas, kompiuterinio tinklo ar informacinės sistemos valdymas ir kontrolė. Taigi, nusikaltimai informatikai galėtų būti vadinami kaip nusikaltimai kompiuterinio informacijos saugumui, nes vertybės, kurioms ksinamasi šiais nusikaltimais, yra teisėtinai ginamas informacijos saugumas.

R.Petrausko ir D.Štītėlio leidinyje „Kompiuteriniai nusikaltimai ir jų prevencija“ pateikiamas kompiuterinio nusikaltimo apibrėžimas, suformuluotas baudžiamosios teisės požiūriu: „kompiuterinis nusikaltimas - tai baudžiamojo statymo numatyta visuomenei pavojinga veikla, daranti žalą visuomeniniams santykiams, saugant, vartojant ir platinant kompiuterinę informaciją“<sup>7</sup>.

Taikant Lietuvos Respublikos asmens duomenų teisės apsaugos statymą (Žin., 1996, Nr. 63-1479; 2003, Nr. 15-597) ir Lietuvos Respublikos valstybės registrų statymą (Žin., 1996, Nr.86-2043; 2004, Nr. 124-4488), kuriuose pateiktos duomenų tvarkymo bei automatinio

<sup>4</sup> Lietuvos Standartas LST ISO/IEC 2382-1: 1996. Informacijos technologija. Terminai ir apibrėžimai. D.1. P.21.

<sup>5</sup> Civilka M., Lamanauskas T., Osinaitė G. ir kt. Informacinė technologijų teisė. - Vilnius, 2005. P.528.

<sup>6</sup> Tarptautiniai žodžių žodynai. - Vilnius, 1985. P.213.

<sup>7</sup> Petrauskas R., Štītėlis D. Kompiuteriniai nusikaltimai ir jų prevencija. - Vilnius, 2000. P.7.

duomen tvarkymo s vokos, analogij , galima b t patikslinti min t apibr žim ir išd styti j taip: kompiuterinis nusikaltimas – tai baudžiamojo statymo numatyta visuomenei pavojinga veika, daranti žal visuomeniniams santykiams, tvarkant kompiuterin informacij , t.y. atliekant su ja bet kur veiksm – rinkim , užrašym , kaupim , saugojim , klasifikavim , grupavim , jungim , keitim (papildym ar taisym ), teikim , paskelbim , naudojim , logines ir (ar) aritmetines operacijas, paiešk , skleidim , naikinim ar kitok veiksm arba veiksm rinkin .

Lietuvos ryt kaimyni – Rusijos, Baltarusijos, Ukrainos – baudžiamosios teis s teoretikai tai pat susiskirst dvi grupes, ta iau vis d lto didesn j dalis kompiuterini nusikaltim s vok aiškina siaur ja prasme ir apibr žia šiuos nusikaltimus kaip veikas:

a) kurios yra nurodytos atskirame specialiame baudžiamojo statymo skyriuje (pvz., Rusijos baudžiamojo kodekso 21 sk.) ir

b) kurioms b dingas bendras pasik sinimo objektas – visuomeniniai santykiai, susij su saugiu automatizuotu informacijos apdorojimu.

Šios nuostatos laikosi V.S.Komisarovas, B.V.Zdravomislovas, V.B. echovas. Pavyzdžiui, V.S.Komisarovas teigia, jog kompiuteriniai nusikaltimai – tai „ty in s visuomenei pavojingos veikos (veikimas ar neveikimas), daran ios žal ar sukelian ios gr sm visuomeniniams santykiams, susijusiems su saugiu informacijos ar informacijos resurs k rimu, naudojimu, platinimu ar j apsauga“<sup>8</sup>. Min ti mokslininkai pabr žia, kad kompiuteriniais nusikaltimais vadintinos tos veikos, kurios numatytos baudžiamojo statymo ir pažeidžia asmen teis tus interesus, susijusius su automatizuotu duomen apdorojimu.

Ta iau yra ir toki baudžiamosios teis s specialist , kurie kompiuterini nusikaltim s vok aiškina pla i ja prasme, pavyzdžiui I.A.Voronovas, P.D.Bylen iukas, M.Dutovas. P.D.Bylen iuko teigimu, kompiuterini nusikaltim grupei priskirtinos visos neteis tos veikos, kuriomis k sintasi elektronin s informacijos tvarkym kaip objekt ir kurios vykdytos elektroninio informacijos tvarkymo d ka, vadinasi kompiuteriniais nusikaltimais laikomas ir suk iavimas, pasinaudojant magnetin mis kortel mis, suk iavimas, susij s su mok jimais už tarptautinius pokalbius bei kiti nusikaltimai telekomunikacij sferoje, neteis tas elektronini mok jim tinklo naudojimas, neteis tas programin s rangos naudojim ir kt.<sup>9</sup> I.A.Voronovas kompiuterinius nusikaltimus apibr žia kaip visus neteis tus veiksmus, vykdomus pasitelkus skai iavimo technik ir telekomunikacij priemones, kuri objektas yra informaciniai santykiai<sup>10</sup>. A.V.Sorokinas pabr žia, kad kalbant apie kompiuterinius nusikaltimus, reik t skirti dvi j grupes,

<sup>8</sup> . . . : // , 1998. .13.

<sup>9</sup> Bylenchuk P.D. Organized transnational computer crime: the global problem of the new millenium // <http://www.crime-research.org/library/bileng.htm>; prisijungimo laikas: 2006-05-02.

<sup>10</sup> . . . - // <http://www.crime-research.org/library/voron.htm>; prisijungimo laikas: 2006-05-02.



t.y. nusikaltimus, susijusius su neteis tu kompiuteri darbo trikdymu, ir nusikaltimus, kuriems vykdyti naudojami kompiuteriai kaip b tina priemon , taigi šiuo atveju kompiuteriniams nusikaltimams priskiriamos visos neteis tos veikos, vykdomos panaudojant kompiuter (pvz., dokument klastojimas, suk iavimas ir kt.)<sup>11</sup> .

J.M.Baturino teigimu, dauguma tradicini nusikaltim r ši modifikavosi d l skai iavimo technikos panaudojimo jiems vykdyti, vadinasi tikslinga kalb ti tik apie nusikaltim kompiuterinius aspektus, neišskiriant ši nusikaltim kaip r šies, nes teisiniu poži riu kompiuterini nusikaltim negali b ti<sup>12</sup>. Prieš kompiuterini nusikaltim termino vartojim pasisako ir V.V.Krilovas, kurio manymu tinkamesnis yra informacini nusikaltim terminas, nes Rusijos baudžiamajame kodekse išskirti atskir skirsn nusikaltimai kompiuterin s informacijos srityje yra tik informacini nusikaltim dalis, kuri jungia kompiuteris kaip bendra informacijos apdorojimo priemon <sup>13</sup>.

Kaip jau buvo min ta, kompiuterinio nusikaltimo s voka pirmiausia buvo pavartota JAV mokslin je literat roje. D.Parkerio teigimu, kompiuterinis nusikaltimas – tai visos ty in s veikos, susijusios su kompiuteriais, d l kuri nukent jusysis patyr ar gal jo patirti žal , o nusikaltimo subjektas tur jo ar gal jo gauti iš to naudos. Bet toks apibr žimas, viena vertus, labai išple ia kompiuterini nusikaltim rat ir apima paprast kompiuterio vagyst , o kita vertus, n ra pakankamai išsamus, nes neapima veik , padaryt d l neatsargumo arba nesiekiant naudos. Vis d lto galima konstatuoti, jog JAV baudžiamosios teis s darbuose vyrauja kompiuterini nusikaltim sampratos aiškinimas pla i ja prasme, t.y. kompiuterinis nusikaltimas apibr žiamas kaip bet koks baudžiamosios teis s pažeidimas, kuriam padaryti arba iširti naudojamos kompiuterini technologij žinios<sup>14</sup>, nors tokiu atveju dalis tradicini nusikaltim b t traukti kompiuterini nusikaltim kategorij , jei j tyrimui b t naudojamos kompiuterin s technikos žinios.

Atsižvelgdama kompiuterinio nusikaltimo s vokos traktavimo prieštaravimus bei tarptautin s bendruomen s susir pinim spar iai plintan iais moderniais nusikaltimais, susijusiais su neteis tu elektronin s erdv s panaudojimu, 1983 m. Ekonominio bendradarbiavimo ir pl tros organizacija (OECD, liet. EBPO) sudar ekspert komitet kompiuterini nusikaltim teisinio vertinimo problemoms spr sti. EBPO ataskaitoje kompiuterinis nusikaltimas buvo apibr žtas kaip bet koks neteis tas, neetiškias arba nesankcionuotas elgesys, susij s su automatiniu kompiuterini

---

<sup>11</sup> A. . : , 1999. .11.

<sup>12</sup> . // <http://www.crime-research.org/library/cyberpon.htm>; prisijungimo laikas: 2006-05-02.

<sup>13</sup> .  
<sup>14</sup> American Criminal Law Review.- Georgetown university law center, 1998. P.505.

duomen apdorojimu ir siuntimu, ta iau nebuvo nurodyta, kokios teis s šakos atžvilgiu toks elgesys yra neteis tas<sup>15</sup>.

1989 m. Europos Tarybos Nusikaltim tyrimo komitetas nagrin jo baudžiamosios teis s problemas, susijusias su kompiuteriniais nusikaltimais, ta iau buvo nutarta kompiuterini nusikaltim s vokos nereglamentuoti, tokiu b du paliekant Europos S jungos valstyb ms nar ms s lygin laisv kriminalizuoti šios srities veikas, atsižvelgiant teisin s sistemos ypatumus bei istorines tradicijas.

Atsižvelgiant kompiuterinio nusikaltimo s vokos traktavimo prieštaravimus, 1994 m. Kriminalin s policijos tarptautin je apžvalgoje kompiuterini nusikaltim srityje teigiama, jog terminai „kompiuterinis nusikaltimas“ ir „nusikaltimas, susij s su kompiuteriais“ bus vartojami, kalbant tiek apie tradicinius nusikaltimus (suk iavimas, klastojimas, vagyst ir kt.), tiek apie moderniuosius nusikaltimus (neteis ta prieiga ir kt.)<sup>16</sup>.

Apibendrinus vairi valstybi patirt bandant apibr žti kompiuterini nusikaltim s vok , galima padaryti išvad , jog šiuo metu n ra pasiekta vieningo sutarimo nei tarptautiniu, nei nacionaliniu mastu, ta iau nepaisant to, daugelis valstybi kriminalizavo didži j dal veik , kuriomis k sinamasi visuomeninius santykius informacijos apdorojimo procese ir kompiuterin s informacijos saugum kaip nusikaltimo objekt .

vertinus užsienio valstybi bei Lietuvos statym leidybos praktik , galima daryti išvad , jog šiuo metu vyrauja kompiuterini nusikaltim samprata siaur ja prasme. Taigi, kompiuterin nusikaltim galima b t apibr žti kaip baudžiamojo statymo numatyt visuomenei pavojinga veik , daran i žal visuomeniniams santykiams automatizuotai tvarkant kompiuterin informacij , t.y. atliekant su ja bet kur veiksm – rinkim , užrašym , kaupim , saugojim , klasifikavim , grupavim , jungim , keitim (papildym ar taisym ), teikim , paskelbim , naudojim , logines ir (ar) aritmetines operacijas, paiešk , skleidim , naikinim ar kitok veiksm arba veiksm rinkin .

---

<sup>15</sup> Sieber U. The international handbook of computer crime. 1986.

<sup>16</sup> United Nations Manual on Computer-Related Crime. International Review of Criminal Policy Nos, 43/44, 1994 // <http://www.uncjin.org/documents/eightcongress.html>; prisijungimo laikas: 2006-05-02.

## 2. KOMPIUTERINI NUSIKALTIM KLASIFIKACIJA IR R ŠYS

Baudžiamosios teisės ir kriminalistikos mokslo darbuose galima aptikti vairi kompiuterini nusikaltim klasifikacij , kurios paremtos skirtingais klasifikavimo kriterijais. vertinus mokslin s doktrinos pateikt klasifikacij vairov , galima s lyginai išskirti keturias dideles j grupes: pirmajai grupei priklausyt t autori klasifikacijos, kuri pagrindas – nusikaltim vykdymo b das, antrajai grupei galima b t priskirti klasifikacijas, sudarytas atsižvelgiant kompiuterio panaudojimo pob d vykdant nusikaltim , tre iajai atstovaut autoriai, klasifikuojantys kompiuterinius nusikaltimus pagal poveik kompiuterinei informacijai, o ketvirtajai grupei priklausyt klasifikacijos, kuri pagrindas – baudžiam j statym saugomas interesus.

Dažniausiai kompiuteriniai nusikaltimai klasifikuojami pagal j vykdymo b d . Pavyzdžiui, J.M.Baturinas<sup>17</sup>, apibendrin s tipinius kompiuterini nusikaltim vykdymo b dus, išskyr tris pagrindines kompiuterini nusikaltim r šis:

1. Kompiuteriniai nusikaltimai, vykdomi neteis to per mimo b dais (metodais);
2. Kompiuteriniai nusikaltimai, vykdomi neteis tos prieigos b dais (metodais);
3. Kompiuteriniai nusikaltimai, vykdomi manipuliacijos b dais (metodais).

Kita dalis mokslinink klasifikuoja kompiuterinius nusikaltimus, atsižvelgdami kompiuterio panaudojimo pob d vykdant nusikaltim . Remdamasis šiuo kriterijumi, Markas Ekenvaileris<sup>18</sup> pasi l suskirstyti kompiuterinius nusikaltimus tris pagrindines grupes, kurios, savo ruožtu, toliau suskirstomos pogrupius:

1. Kompiuteriniai nusikaltimai, kai kompiuteris ar kitas elektroninis renginys yra teis spažeidimo *objektas*, o nusikalt lio tikslas – pagrobti rang , informacij arba pakenkti ar kitaip neteis tai paveikti informacin sistem :

kompiuterin s rangos pasisavinimas (šiai grupei priklauso tradiciniai prast nusikaltim r ši vykdymo b dai, kai nusikalt lis siekia pasisavinti svetim turt );

informacijos pagrobimas;

paslaug pagrobimas (neteis tos prieigos prie sistemos gavimas, siekiant neatlygintinai pasinaudoti jos teikiamomis paslaugomis);

sistemos sugadinimas (šiai grupei priklauso nusikaltimai, vykdomi siekiant sunaikinti arba pakeisti duomenis, kurie yra svarb s sistemos – neteis tos prieigos objekto – savininkui ar vartotojams);

“p dsak sl pimas” (šiai grupei priklauso nusikaltimai, vykdomi siekiant pasl pti savo

<sup>17</sup> . . . : , 1991.

<sup>18</sup> . . . « » (

», 20–21 1997 ). // <http://www.uic.ssu.samara.ru/~cclub/navigator/uglaw.htm>; prisijungimo laikas: 2006-05-01.

vard ir buvimo viet ).

2. Kompiuteriniai nusikaltimai, kai kompiuteris naudojamas kaip nusikaltimo vykdymo *priemon* :

tradicini nusikaltim vykdymo priemon (pvz., suk iavimo, klastojimo);

kompiuterini nusikaltim vykdymo priemon (neteis to poveikio kitam kompiuteriui ar sistemai priemon ).

3. Kompiuteriniai nusikaltimai, kai kompiuteris naudojamas kaip *atminties reenginys* (pvz., po silaužimo sistem yra sukuriamas special s fail katalogai, skirti nusikalt lio programini ms priemon ms, sistemos slaptažodžiams, pavogt kreditini korteli numeriams ar kt. saugoti). Reikia pasteb ti, kad šios nusikaltim grup s išskyrimas kelia abejoni , nes jei kompiuteris panaudojamas kaip atminties reenginys, t.y. nusikaltimo vykdymo priemon , tai pats nusikaltimas gal t b ti priskirtas antrajai grupei.

Atkreiptinas d mesys klasifikacijas, pagr stas poveikio kompiuterinei informacijai kriterijumi. Tokios klasifikacijos pavyzdžiu gal t b ti pakankamai išsami V.A.Meš eriakovo kompiuterini nusikaltim klasifikacija<sup>19</sup>, suskirstanti neteis tas veikas penkias pagrindines grupes ir pogrupius :

1. Neteis tas informacijos užvaldymas ( sigijimas) arba išskirtini naudojimosi ja teisi pažeidimas:

neteis tas informacijos kaip duomen , dokument visumos užvaldymas (išskirtini valdymo teisi pažeidimas);

neteis tas informacijos kaip prek s užvaldymas;

neteis tas informacijos kaip id jos (algoritmo, uždavinio sprendimo b do) užvaldymas.

2. Neteis tas informacijos pakeitimas:

neteis tas informacijos kaip duomen visumos pakeitimas;

neteis tas informacijos kaip id jos pakeitimas ir pristatymas kaip savo nuosavyb s (algoritmo pakeitimas);

neteis tas informacijos kaip prek s pakeitimas, siekiant pasinaudoti jos naudingomis savyb mis (apsaugos pašalinimas).

3. Neteis tas informacijos sunaikinimas:

informacijos kaip duomen visumos sunaikinimas;

informacijos kaip prek s sugadinimas.

4. Neteis tas informacijos suk rimas (veikos, sukuriant (generuojant) informacij su

---

<sup>19</sup>

// , . . . , 1999, N°4-5.

nustatytomis savybėmis):

informacijos, daranios žalą valstybei, visuomenei ar asmeniui, platinimas informaciniame tinklame telekomunikaciniais kanalais;

kompiuteriniai virusai ir kitos kenkėjiškos programos ir platinimas;

nusikalstamas neatsakingumas kuriant programinį rangą, algoritmus pažeidžiant nustatytas technines normas ir taisykles.

5. Neteisėtai informacijos naudojimo trukdymas (veikos, sukuriant dirbtines kliūtis teisėtiems vartotojams naudotis informacija):

neteisėtai automatizuotame sistemos resursų panaudojimas (atminties, laiko ir kt.);

informacinis telekomunikacinio tinklo mazgų blokavimas (melagingi iškvietimų srautų sukirimai).

U.Sieberio kompiuterinių nusikaltimų klasifikacija parengta atsižvelgiant baudžiamojo statymo saugomus interesus<sup>20</sup>:

- 1) ekonominius;
- 2) privatumo;
- 3) kitus.

statymai, saugantys minėtus interesus, paprastai skirstomi ekonominiams interesams apsaugoti; privatumo apsaugoti; intelektinoms nuosavybės teisėms apsaugoti; apsaugoti nuo nelegalaus ir žeidžiančio turinio informacijos.

**Ekonominio pobūdžio nusikaltimai.** Tai labiausiai paplitę kompiuteriniai nusikaltimai. Dažniausiai skiriami šie ekonominio pobūdžio kompiuteriniai nusikaltimai:

- 1) kompiuterinis silaužimas ar sibrovimas (*hacking*);
- 2) kompiuterinis šnipinėjimas (*espionage*);
- 3) programinės rangos ir kitoks piratavimas;
- 4) kompiuterinis sabotažas (*sabotage*);
- 5) kompiuterinis prievartavimas (*extortion*);
- 6) kompiuterinis sukrovimas (*fraud*).

**Privatumo pažeidimai.** Mokslo darbuose asmens privatumo pažeidimai dažniausiai skirstomi dviem šeim:

- 1) materialieji privatumo pažeidimai;
- 2) formalieji privatumo pažeidimai.

Būtinai paminėti, jog ne už visus privatumo pažeidimus numatoma baudžiamoji

---

<sup>20</sup> Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime-study // <http://www.jura.uni-wuerzburg.de/sieber/article/>; prisijungimo laikas: 2006-01-07.

atsakomybė, dažniausiai kriminalizuojami tik materialieji privatumo pažeidimai. Neteis tos veikos, susijusios su informacijos privatumo pažeidimu:

- 1) susirašinėjimo, kitoki pranešimų, siuntimų ar pokalbių telefonu slaptumo pažeidimas;
- 2) neteisėtai informacijos apie privataus asmens gyvenimą rinkimas;
- 3) neteisėtai informacijos apie asmens privataus gyvenimą atskleidimas ar panaudojimas.

**Intelektinės nuosavybės teisės pažeidimai.** Paprastai skiriami šie kompiuteriniai nusikaltimai, pažeidžiantys intelektinės nuosavybės teises:

- 1) autorių teisės pažeidimai;
- 2) gretutinių teisės pažeidimai.

Pastebima, kad intelektinės nuosavybės teisės pažeidimai yra ekonominio pobūdžio. Šie nusikaltimai yra labai paplitę elektroninėje erdvėje, nes programinėsrangos, muzikos, literatūros, fotografijos ir kitus kūrinius lengva kopijuoti ir platinti, todėl autorių ir gretutinių teisės saugomą intelektinį kūrinių atgaminimą bei platinimą be teisės akto nustatyto leidimo internete pasitaiko ypač dažnai.

**Neteisėtai turinio pažeidimai.** Dažniausiai pasitaikantys pažeidimai, susiję su informacijos turiniu, yra šie:

- 1) vaikų pornografija,
- 2) neapykantos (rasinės, religinės ir kt.) skatinimas,
- 3) šmeižtas;
- 4) persekiojimas (seksualinis ir kt.).

Tokio pobūdžio pažeidimai iš esmės yra tradiciniai, tačiau jiems vykdyti naudojama kompiuterinė ranga. Neteisėtai turinio informacijos sklaidimas internete sparčiai plinta, tai lemia elektroninėje erdvėje anonimiškumas ir praktiškai neribotos sklaidos galimybės, be to interneto paslaugų teikėjo atsakomybės teisinis neapibrėžtumas.

Nepaisant skirtingo kompiuterinių nusikaltimų klasifikavimo mokslo darbuose, tarptautinėje praktikoje bandyta sukurti universalią šių nusikaltimų klasifikaciją, kuri palengvintų teis tvarkos ir teisės saugos institucijų darbą ir bendradarbiavimą tiriant kompiuterinius nusikaltimus, pasižyminčius globalizacijos tendencija.

Šiuo metu daugelis valstybių naudoja vieningą kodifikatorių, patvirtintą Interpolo Generalinio Sekretoriato, kur rengiant siekta apjungti teisės ir informacinių technologijų žinias. Kodifikatoriuje kompiuteriniams nusikaltimams priskirtas indeksas „Q“ (beje, pateiktas nusikaltimų sąrašas nėra baigtinis, apdairiai palikta galimybė plėsti, pasinaudojant indeksu „Z“, reiškiančiu „kiti“), visi nusikaltimai sugrupuoti šešias grupes:

- nesankcionuota prieiga ir per mimas (QA);
- kompiuterini duomen pakeitimas (QD);
- kompiuterinis suk iavimas (QF);
- neteis tas kopijavimas (QR);
- kompiuterinis sabotazas (QS);
- kiti kompiuteriniai nusikaltimai (QZ).

Kiekviena kompiuterini nusikaltim grup detalizuojama nurodant jai priskirtus nusikaltimus, turin ius savo indeks (žr. 1 priedas).

1989 m. Europos Taryba pri m Rekomendacij R(89)9 d l kompiuterini nusikaltim <sup>21</sup>, skirt Europos S jungos valstyb ms, kurioje si loma tobulinant nacionalinius teis s aktus, reglamentuojan ius kompiuterinius pažeidimus ar nusikaltimus, vadovautis pateikiamais dviem tokio pob džio veik s rašais: 1) minimaliu s rašu, kuriame nurodytos aštuonios pavojingos veikos, susijusios su kompiuterin mis technologijomis, kurias rekomenduojama traukti nacionalinius teis s aktus, ir 2) papildomu s rašu, kuriame nurodytos keturios mažiau pavojingos veikos, kurios n ra privalomai trauktinos nacionalinius teis s aktus.

Minimalus s rašas:

1. Suk iavimas naudojant kompiuter (*Computer-related fraud*).
2. Klastojimas naudojant kompiuter (*Computer forgery*).
3. Kompiuterini duomen arba program sunaikinimas arba sugadinimas (*Damage to computer data or computer programs*).
4. Sabotazas naudojant kompiuter (*Computer sabotage*).
5. Neteis tas pri jimas (neteis ta kreiptis) prie kompiuterini sistem (*Unauthorised access*).
6. Neteis tas informacijos kompiuterin se sistemose per mimas (*Unauthorised interception*).
7. Neteis tas apsaugot kompiuterini program dauginimas ir platinimas (*Unauthorised reproduction of a protected computer program*).
8. Neteis tas kompiuterini lust (mikroschem ) topografij dauginimas ir platinimas (*Unauthorised reproduction of a topography*).

Papildomas s rašas:

1. Kompiuterini duomen arba program pakeitimas (*Alteration of computer data or computer programs*).
2. Šnipin jimas naudojant kompiuter (*Computer espionage*).

<sup>21</sup> Computer-related crime. Council of Europe. Recommendation No R(89)9, adopted by Committee of Ministers of the Council of Europe on 13 September 1989. Strasbourg, 1990.

3. Neteis tas kompiuterio naudojimas (laiko vagyst ) (*Unauthorised use of computer*).

4. Neteis tas apsaugot kompiuterini program naudojimas (*Unauthorised use of a protected computer program*).

Palyginus 1995 m. Interpolo Generalinio Sekretoriato rekomendacijose „Computers and crime“ ir Europos Tarybos rekomendacijose pateiktas kompiuterini nusikaltim bei pažeidim klasifikacijas, galima b t išskirti šias pagrindines neteis t veik grupes:

1. Suk iavimas naudojant kompiuter – tai kompiuterini duomen arba kompiuterini program vedimas, pakeitimas, ištrynimasis arba kitoks sikišimas duomen apdoravimo proces , kuris paveikia šio proceso galutin rezultat , padaro žalos kito asmens nuosavybei, siekiant naudoti sau arba kitam asmeniui.

2. Klavojimas naudojant kompiuter – tai kompiuterini duomen arba kompiuterini program vedimas, pakeitimas, ištrynimasis arba kitoks sikišimas duomen apdoravimo proces , kai ši veiksm tikslas yra toks pat, kaip ir teis s aktuose, numatan iuose atsakomyb už tradicin klavojim .

3. Sabotažas naudojant kompiuter – tai kompiuterini duomen arba kompiuterini program vedimas, pakeitimas, ištrynimasis arba sikišimas bei trukdymas kompiuterin ms sistemoms, siekiant sutrikdyti kompiuterin s sistemas arba telekomunikacij tinklo darb .

4. Kompiuterini duomen arba program sunaikinimas arba sugadinimas – tai neteis tas kompiuterini duomen arba kompiuterini program ištrynimasis, sunaikinimas, sugadinimas.

5. Neteis ta prieiga prie kompiuterini sistem – tai neteis tas pri jimas prie kompiuterin s sistemas arba kompiuterinio tinklo, pažeidžiant saugumo priemones.

6. Neteis tas informacijos kompiuterin se sistemose per mimas – tai informacijos per mimas nelegaliais b dais kompiuterinio tinklo viduje arba išor je.

Siekiant suvienodinti Europos S jungos valstybi baudžiam j materialin teis ir išvengti dvigubo baudžiamumo taisykl s neatitikimo problem , 2001 m. Budapešte buvo priimta Konvencija d l elektronini nusikaltim (priimta 2001 m. lapkri io 23 d., pasirašyta 2003 m. birželio 23 d., ratifikuota Lietuvos Respublikos 2004 m. sausio 22 d. statymu Nr. IX-1974 (Žin., 2004, Nr.36), sigaliojo 2004 m. liepos 1 d.), kurioje pateikiama kompiuterini nusikaltim klasifikacija, parengta atsižvelgiant min t Rekomendacij R(89)9 d l kompiuterini nusikaltim . Konvencijoje nusikaltimai buvo suskirstyti keturias grupes pagal statym saugom interesus :

1. Nusikaltimai kompiuterini duomen ir sistem konfidencialumui, vientisumui ir prieinamumui:

neteis ta prieiga;



neteis ta perimtis;  
neteis tas poveikis duomenims;  
neteis tas poveikis sistemai;  
neteis tas tais naudojimas.

2. Kompiuteriniai nusikaltimai (nusikaltimai panaudojant kompiuterines technologijas):

kompiuterinis klastojimas;  
kompiuterinis suk iavimas.

3. Turinio nusikaltimai (nusikaltimai, susij su vaik pornografija).

4. Nusikaltimai, susij su autori teisi ir gretutini teisi pažeidimais (autori teisi pažeidimai, gretutini teisi pažeidimai).

Jungtini Taut parengtoje tarptautin je kriminalin s policijos kompiuterini nusikaltim apžvalgoje pateikiama tokia kompiuterini nusikaltim klasifikacija<sup>22</sup>:

1. Manipuliavimas naudojant kompiuter (kompiuterinis suk iavimas);
2. Klastojimas naudojant kompiuter ;
3. Kompiuterini duomen ir program sunaikinimas ir modifikavimas (kompiuterinis sabotazas);
4. Neteis tas pri jimas prie kompiuterini duomen ;
5. Neteis tas kompiuterini program platinimas.

Išnagrin jus min tas Europos Tarybos ir Jungtini Taut parengtas kompiuterini nusikaltim klasifikacijas bei j apib dinim , galima atrasti daug bendr dalyk , nepaisant skirtingo konkre ios nusikaltim r šies vardijimo.

### **Nusikaltimai kompiuterini duomen ir sistem konfidencialumui, vientisumui ir prieinamumui**

**Neteis ta prieiga (*illegal access*)** – tai ty inis ir neteis tas pri jimas prie visos kompiuterin s sistemos arba jos dalies, t.y. isibrovimas, slaptažodži iškodavimas ar neteis tas naudojimas, vykdytas pažeidžiant apsaugos priemones, kuris gali b ti padarytas siekiant gauti kompiuterinius duomenis ar turint kit nes žining ketinim , taip pat gali b ti susij s su kompiuterine sistema, sujungta su kita kompiuterine sistema.

**Neteis ta perimtis (*illegal interception*)** – tai ty inis ir neteis tas neviešo kompiuterini duomen perdavimo (srauto) kompiuterin sistem , iš jos ir jos viduje per mimas

---

<sup>22</sup> United Nations Manual on computer-related crime. International review of criminal policy. No 43/44.

techninis priemonis, taip pat elektromagnetinės emisijos iš kompiuterinės sistemos, perduodanios tokius kompiuterinius duomenis, perimamas, kuris gali būti vykdytas turint nes žinimą ketinimą arba gali būti susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema.

**Poveikis duomenims (*data interference*)** – tai tyinis ir neteisėtas kompiuterinių duomenų sugadinimas, sunaikinimas, apgadinimas, pakeitimas arba galimybių naudotis tokiais duomenimis panaikinimas. Ši veikta teisės aktuose apibūdinama tokiomis sąvokomis kaip „pažeidimas“ (*damaging*), „gadinimas“ (*deterioration*), „ištrynimasis“ (*deletion*), „pakeitimas“ (*alteration*), „slopinimas“ (*suppression*) ir kt.

**Poveikis sistemai (*system interference*)** – tai tyinis ir neteisėtas kompiuterinės sistemos darbo sutrukdyimas vedant, perduodant, sugadinant, sunaikinant, apgadinant, pakeičiant kompiuterinius duomenis arba panaikinant galimybių naudotis tokiais duomenimis.

**Netinkamas taisyklės naudojimas, arba piktnaudžiavimas prietaisais, (*misuse of devices*)** – tai tyinis ir neteisėtas:

1) gaminimas, pardavimas, sigijimas naudoti, vežimas, platinimas arba kitoks galimybių naudotis suteikimas:

a) taisyklės, skaitant kompiuterinę programą, sukurtą ar pritaikytą pirmiausia anksčiau minėtiems nusikaltimams (neteisėta prieiga; neteisėta perimtis; poveikis duomenims; poveikis sistemai) daryti,

b) kompiuterio slaptažodžio, prieigos kodo arba panašiu duomenų, kuriais galima prieiti prie visos kompiuterinės sistemos arba jos dalies, kai ketinama juos panaudoti anksčiau minėtiems nusikaltimams daryti;

2) turėjimas 1 punkto a ir b papunkčiuose minimų dalykų, siekiant juos panaudoti anksčiau minėtiems nusikaltimams daryti.

Svarbu pabrėžti, kad minimos veikos ( taisyklės, slaptažodžiai, kodų gaminimas, pardavimas, sigijimas naudoti, vežimas, platinimas ir kitoks galimybių naudotis suteikimas arba turėjimas) neužtraukia baudžiamosios atsakomybės, jei jos yra teisėtos, t.y. skirtos tik sankcionuotam kompiuterinės sistemos tikrinimui arba jos apsaugai.

**Nusikaltimų kompiuterini duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui** grupę Jungtini Tautų tarptautinėje kriminalinės policijos kompiuterini nusikaltimų apžvalgoje sudaro **neteisėtas priėjimas prie kompiuterinių duomenų ir kompiuterinių duomenų ir programų sunaikinimas arba modifikavimas (kompiuterinis sabotžas)**. Teigiama, jog neteisėtu priėjimu prie kompiuterinių duomenų gali būti siekiama vairių tikslų. Šiai grupei priskiriami hakerių veiksmai, demonstruojantys gebėjimą apeiti apsaugos sistemas, pasinaudojant įvairiais (pvz., pasinaudojus sistemoje vartojamais bendrais

slaptažodžiais, per mus slaptažod "Trojos arklio" pagalba ir apsimetus teis tu vartotoju, naudojant specialias slaptažodži veikimo programas ir pan.). Svarbu pamin ti neteis t prieig prie ypatingos kategorijos duomen , laikom valstyb s, tarnybos, banko ar komercine paslaptimi, kuri daugelyje valstybi yra kriminalizuota. Neteis ta prieiga gali padaryti žal duomenims, sutrikdyti kompiuterin s sistemos darb . **Kompiuterini duomen ir program sunaikinimas arba modifikavimas (kompiuterinis sabotžas)** – tai kompiuterini program , duomen , kompiuterin s rangos sugadinimas, sunaikinimas arba teis t vartotoj ir sistemos administratori veiklos apribojimas, trukdant jiems dirbti su sistemos ištekliais, taip pat program , skirt sugadinti arba sunaikinti kitas kompiuterines programas bei duomenis (kompiuterini virus , „logini bomb “, „kirm li “ ir kt.), k rimas, platinimas bei naudojimas. Duomenys gali b ti sunaikinami ar sistemos darbas sutrikdomas panaudojant prieiga internetu, taip pat panaudojant elektromagnetines bangas, radioaktyv spinduliavim ir kt. Kompiuterinio sabotžo motyvai gali b ti skirtingi: komerciniai (konkurencin kova), kariniai, politiniai, chuliganiški, keršto ir kt. Šios kategorijos nusikalstamos veikos apima ir tiesiogin ir slapt neteis t pri jim prie kompiuterin s sistemos.

**Kompiuteriniai nusikaltimai** (nusikaltimai panaudojant kompiuterines technologijas)

**Kompiuterin s klastot s (forgery)** – tai ty inis ir neteis tas kompiuteri duomen suklastojimas, t.y. duomen vedimas, pakeitimas, sunaikinimas arba galimyb s naudotis jais panaikinimas, siekiant, kad pakeisti, neautentiški duomenys b t laikomi autentiškais, ar jais b t naudojamosi teis tiems tikslams, (nepriklausomai nuo to, ar šie duomenys yra tiesiogiai skaitomi ir suprantami), esant ketinimui apgauti ar panašiam nes žiningam ketinimui.

Jungtini Taut tarptautin je kriminalin s policijos kompiuterini nusikaltim apžvalgoje ši nusikaltim grup vardinta kaip **klastojimas naudojant kompiuter** , t.y. kompiuteri duomen pakeitimas, sugadinimas arba sunaikinimas d l vairi tiksl , ta iau nesiekiant tiesiogin s turtin s naudos, o tai ir skiria šiuos nusikaltimus nuo suk iavimo panaudojant kompiuter . Šiai grupei nusikaltim priskiriami tradiciniai dokument klastojimo nusikaltimai, vykdomi naudojant kompiuterin rang (ypa naujos kartos lazerinius spausdintuus ir kopijuoklius), taip pat gali b ti priskiriama nes žininga konkurencija, mokes i sl pimas, kai apskaita yra kompiuterizuota, ir kt.

**Kompiuterinis suk iavimas (fraud)** – tai ty iniai ir neteis ti veiksmai, s lygojantys kito asmens nuosavyb s pradim , vedant, pakei iant, sunaikinant kompiuterinius duomenis arba panaikinant galimyb naudotis tokiais duomenimis, paveikiant kompiuterin s sistemos darb , siekiant gauti neteis tos ekonomin s naudos sau arba kitam asmeniui.

Jungtini Taut tarptautin je kriminalin s policijos kompiuterini nusikaltim apžvalgoje kompiuterinis suk iavimas vardijamas kaip **manipuliavimas naudojant kompiuter** , t.y.

kompiuterini duomen vedimo ir išvedimo manipuliacijos, kuriomis sunaikinami arba sugadinami duomenys, padaromi nuostoliai, siekiant turintis naudoti sau.

Duomen vedimo manipuliacij metu kompiuterin sistem gali bti vesti neteisingi duomenys, tokius veiksmus s lyginai paprasta atlikti vykdant kompiuterini sistem duomen apdorojimo funkcijas, nes tam nereikia ypating kompiuterini žini, taiau gana sunku aptikti. Program manipuliacij metu kompiuterin sistem gali bti vestos naujos programos arba pakeistos kompiuterin je sistemoje esan ios programos (pvz., taikomas „Trojos arklio“ metodas), tokios manipuliacijos yra sud tingos ir sunkiai aptinkamos, reikalauja speciali kompiuterini žini.

Duomen išvedimo manipuliacij metu iš kompiuterin s sistemos gali bti vairiais b dais išvesti duomenys, falsifikuojant komandas (pvz., gryn j pinig automato apgavimas, naudojant vogtas bank kortel s ar specialius renginius, „Salami“ metodas, kai kartojamos kompiuterin s proced ros, siekiant pervesti pinigus iš vienos s skaitos kit ).

**Nusikaltimai, susij su vaik pornografija** – tai turinio nusikaltimai, tiksliau ty inis ir neteis tas pornografinio turinio produkcijos, kurioje atvaizduotas vaikas:

- 1) gaminimas, turint tiksl platinti per kompiuterin sistem ;
- 2) si lymas arba pateikimas per kompiuterin sistem ;
- 3) platinimas arba perdavimas per kompiuterin sistem ;
- 4) sigijimas per kompiuterin sistem sau arba kitam asmeniui;
- 5) laikymas kompiuterin je sistemoje arba kokioje nors kompiuterini duomen laikmenoje.

Konvencijoje s voka „pornografinio turinio produkcija, kurioje atvaizduotas vaikas“ reiškia pornografin medžiag , vizualiai vaizduojan i :

- a) aiškiai seksual nepilname io elges ;
- b) aiškiai seksual asmens, atrodan io kaip nepilnametis, elges ;
- c) tikroviškus nepilname io aiškiai seksualaus elgesio vaizdus.

Konvencijoje s voka „vaikas“ reiškia nepilnametis asmuo iki 18 met , taiau šalys gali nustatyti žemesn amžiaus rib – iki 16 met .

**Nusikaltimai, susij su autori teisi ir gretutini teisi pažeidimais,** – tai šios veikos:

- 1) autori teisi pažeidimai, nustatyti šalies teis s aktuose, laikantis sipareigojim , kuriuos ji prisi m pagal Berno konvencijos d l literat ros ir meno k rini apsaugos Paryžiaus akt , priimt 1971 m. liepos 24 d., Sutart d l intelektin s nuosavyb s teisi prekyboje aspekt ir WIPO autori teisi sutart , išskyrus moralines teises, suteikiamas toki konvencij , kai tokie veiksmai

atliekami s moningai, komerciniais tikslais ir naudojantis kompiuteri sistema.

2) gretutini teisi pažeidimai, nustatyti šalies teis s aktuose, laikantis sipareigojim , kuriuos ji prisi m pagal Romoje sudaryt Tarptautin konvencij d l atlik j , fonogram gamintoj ir transliuojan i j organizacij apsaugos (Romos konvencija), Sutart d l intelektin s nuosavyb s teisi prekyboje aspekt ir WIPO atlikim ir fonogram sutart , išskyrus moralines teises, suteikiamas toki konvencij , kai tokie veiksmai atliekami s moningai, komerciniais tikslais ir naudojantis kompiuteri sistema.

Jungtini Taut tarptautin je kriminalin s policijos kompiuterini nusikaltim apžvalgoje nurodytas **neteis tas kompiuterini program platinimas**, t.y. programin s rangos, kuria turi teis naudotis tik j suk r s arba sigij s juridinis ar fizinis asmuo, pasisavinimas ir platinimas, darantis turtin žal teis tiems savininkams (pvz., programin s rangos piratinis platinimas).

### 3. NUSIKALSTAM VEIK , SUSIJUSI SU KOMPIUTERINIS MIS TECHNOLOGIJOMIS BEI INFORMACIJOS SAUGA, TEISINIS REGLAMENTAVIMAS

#### 3.1. KOMPIUTERINI NUSIKALTIM TEISINIS REGLAMENTAVIMAS EUROPOS S JUNGOS VALSTYB SE

Kompiuterini nusikaltim teisin reglamentavim tarptautiniu mastu vykdo šios organizacijos:

1. Europos Taryba;
2. Europos ekonominio bendradarbiavimo ir pl tros organizacija (OECD);
3. Jungtini Taut Organizacija;
4. Pasaulio prekybos organizacija;
5. kitos organizacijos.

Europos Tarybos Kompiuterini nusikaltim ekspert komitetas pareng ir Europos Taryba išleido šias rekomendacijas, skirtas teisin ms kompiuterini nusikaltim problemoms spr sti: rekomendacij R(85)S, rekomendacij R(89)9 ir rekomendacij R(95)13.

1994 m. Jungtin s Tautos išleido Vadov , skirt su kompiuteriais susijusi nusikaltim kontrolei ir prevencijai, kuriame nagrin jami kompiuterini nusikaltim apibr žimo, j teisinio reglamentavimo, prevencijos, tarptautinis bendradarbiavimo klausimai.

Ta iau bene svarbiausias tarptautinis teis s aktas buvo 2001 m. lapkri io 23 d. Budapešte priimta Europos Tarybos Konvencija d l elektronini nusikaltim <sup>23</sup>. Svarbu pamin ti, kad Budapešto Konvencija yra vienintel sutartis, tarptautiniu mastu reglamentuojanti su kompiuteriniais nusikaltimais susijusius teisinius klausimus. Vis d lto nors Konvencija yra privaloma j pasirašiusiems ir ratifikavusiems valstyb ms, o jos pateikt nusikaltim klasifikacij galima laikyti universaliausia, ji suk l nemažai diskusij bei prieštarig atsiliepim : vien mokslinink nuomone šio dokumento pri mimas – žymus post mis kovojant su moderniais nusikaltimais, kuri vykdymo objektas ar priemon s yra kompiuterin s technologijos, kit , daugiausia informacini technologij specialist , vertinimu, Konvencija t ra formalus susitarimas, kurio pagrindinis tr kumas – teisinis ir technologini aspekt kolizija. Pagrindin Konvencijos paskirtis – harmonizuoti Europos valstybi teisin baz , reglamentuojan i kompiuterinius nusikaltimus.

Beje, 2003 m. birželio 23 d. Konvencij pasiraš 33 šalys, ta iau j ratifikavo tik trys šalys – Albanija, Estija ir Kroatija, o tam, kad Konvencija sigalio , j ratifikuoti prival jo ne mažiau kaip penkios šalys ir mažiausiai trys iš j – Europos Tarybos nar s. Tik 2004 m. kovo 18 d. Konvencij ratifikavo penktoji šalis – Lietuva (Lietuvos Respublikos 2004 m. sausio 22 d. statymu

<sup>23</sup> Konvencija d l elektronini nusikaltim // Valstyb s žinios. 2004, Nr.36.

Nr. IX-1974 (Žin., 2004, Nr.36), vadinasi nuo 2004 m. liepos 1 d. Albanijai, Kroatijai, Estijai, Vengrijai ir Lietuvai ši Konvencija tapo privalomu teisės aktu.

Išanalizavus Europos valstybių teisės aktus, galima konstatuoti, kad nepaisant to, ar Konvencija buvo pasirašyta, į teisinės normos, susijusios su kompiuteriniais nusikaltimais, išlieka pakankamai skirtingos<sup>24</sup>. Vienos valstybės atliko kai kuriuos baudžiamųjų statymų pakeitimus, kitos išleido specialius statymus, skirtus kovai su kompiuteriniu nusikalstamumu. Kai kuriose šalyse, pavyzdžiui, Ispanijoje, nėra speciali norma, skirta kompiuteriniams nusikaltimams, tačiau tokio pobūdžio veikos šioje šalyje vis dėlto yra kriminalizuotos, nes Ispanijos Baudžiamajame kodekse yra bendrieji straipsniai, pagal kuriuos galima patraukti atsakomybėn už vykdytus kompiuterinius nusikaltimus. Austrijoje iki 2002 m. Baudžiamojo kodekso pataisėn viena iš veikų, susijusių su kompiuteriniais technologijomis, nebuvo kriminalizuota, t.y. buvo kvalifikuojama kaip administraciniai nusižengimai.

Palyginus Europos valstybių teisės aktus, galima teigti, jog daugelyje Europos Sąjungos narių veikos, susijusios su kompiuterinių technologijų panaudojimu, yra kriminalizuotos, tik vienoje valstybėje kompiuterinius nusikaltimus reglamentuoja specialios teisės normos, o kitose – tik bendrosios, dalis valstybių taiko tik administracinę atsakomybę arba apskritai nelaiko tokiomis veikomis nei nusikaltimu, nei administraciniu pažeidimu (apibendrinti duomenys pateikiami 2 priede).

Toliau trumpai apžvelgsiu kai kuriuos Europos Sąjungos valstybių teisės aktus, susijusius su kompiuteriniais nusikaltimų reglamentavimu bei teisine atsakomybe už šias veikas (kitas Europos valstybių teisės aktų apžvalga pateikiama 2 priede).

**Belgija.** 2000 m. lapkritį Belgijos Parlamentas Baudžiamųjų kodeksą traukė pakeitimus, skirtus kovai su kompiuteriniais nusikaltimais, kurie sigaliojo nuo 2001 m. vasario 13 d. Belgijos Baudžiamojo kodekso 550<sup>1</sup> straipsnis numato atsakomybę už hakerių (kompiuterinių silaužėlių) veiksmus. Pirma šio straipsnio dalis numato atsakomybę už tyčiną neteisėtą prieigą prie kompiuterinių sistemų arba tyčiną tarpininkavimą suteikiant neteisėtą prieigą (sankcija – bauda arba areštas nuo 3 mėnesių iki 1 metų). Antroje dalyje numatoma atsakomybė už neteisėtą prieigą prie kompiuterinių sistemų, vykdytą asmens, turinčio galiojimus ir teises šiai prieigai, tačiau pasinaudojusio šia teise viršijant suteiktus galiojimus ir turint piktaširdišką slėpimą su tikslu vykdyti kenksmingus veiksmus (sankcija - bauda arba laisvės atėmimas nuo 6 mėnesių iki 2 metų). Pirmosios minėtos straipsnio dalys akcentuoja kompiuterinių sistemų apsaugą, o trečiojoje dalyje kalbama apie pažeidimą duomenų, saugomų kompiuterinėse sistemose, vientisumą, neliečiamumą ir saugumą. Ji numato baudžiamąją atsakomybę už neteisėtą prieigą prie duomenų, kurie yra saugomi kompiuterijoje ar kompiuterinėse sistemose, apdorojami ar perduodami kompiuterinėse sistemose,

<sup>24</sup> Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs) // <http://www.csirt-handbook.org.uk/>; prisijungimo laikas: 2006-06-04

taip pat už neteis t ši duomen panaudojim . Atsakomyb numatoma tiek už ty inius, tiek už neatsargius veiksmus, jei jie suk l žal . Už ši veik vykdyt baudžiama laisv s at mimu nuo 1 iki 3 met , pasik sinimas vykdyti min tus nusikaltimus taip pat yra baudžiamas. Už nusikaltim , numatyt min tame straipsnyje, organizavim , taip pat už skatinim juos vykdyti, numatoma bausm – bauda arba laisv s at mimas nuo 6 m nesi iki 5 met .

Belgijos Baudžiamojo kodekso 314 straipsnis numato baudžiam j atsakomyb už neteis t duomen per mim ryši tinkluose (sankcija – nuo 1 iki 3 met laisv s at mimo); 523, 528, 559 straipsniai numato atsakomyb už kenk jišk program suk rim ir kompiuterin sabotaz , rangos sugadinim , nuostoli nuosavybei padarym . Neteis tas kompiuterin s informacijos pakeitimas nusikalstamais tikslais gali b ti baudžiamas priklausomai nuo jo pob džio pagal Belgijos Baudžiamojo kodekso 134 straipsn (klastojimas), 461 straipsn (vagyst ), 496 straipsn (suk iavimas).

**Didžioji Britanija.** Ši valstyb priklauso bendrosios teis s sistemai, tad baudžiamieji statymai n ra kodifikuoti. Kompiuteriniams nusikaltimams reglamentuoti skirtas 1990 m. Aktas d l kompiuteri panaudojimo neteis tiems tikslams. Šio Akto pirmasis straipsnis numato atsakomyb už neteis t prieig prie kompiuterini duomen ir nustatyto, kad asmuo vykdo nusikaltim , jei jis naudoja kompiuter bet kurios funkcijos vykdymui, siekdamas užtikrinti prieig prie bet kurios programos ar duomen , saugom bet kuriame kompiuteryje, jei tokia prieiga žinomai yra neteis ta. Anglijos baudžiamoji teis nenumato skirting bausmi už prieig prie kompiuteri , apsaugot specialiomis priemon mis, ir neapsaugot . Be to, nusikaltimu yra pripaž stama prieiga prie kompiuterio, kurio pagalba duomenys arba programos pakei iami arba sunaikinami, kopijuojami ar perkeliami kit viet , nei jie buvo saugomi, arba naudojami bet kuriuo b du. Už šio nusikaltimo vykdyt numatyta bausm - bauda arba laisv s at mimas iki 6 m nesi .

Antrasis Akto straipsnis numato atsakomyb už nelegali prieig siekiant vykdyti kit nusikaltim (kompiuterio panaudojimas vagystei, suk iavimui). Tai gali b ti nusikaltimas, numatytas šiame Akte, ar kitas nusikaltimas, kur asmuo ketina vykdyti arba palengvinti jo vykdyt sau ar kitam asmeniui. Bausm , priklausomai nuo vykdytos veikos sunkumo, yra skirtinga – bauda arba laisv s at mimas iki 6 m nesi , sunki nusikaltim atvejais – iki 5 met .

Tre iasis Akto straipsnis numato atsakomyb už neteis t duomen pakeitim . Ty iniai neteis ti veiksmai, s lygojantys bet kurio kompiuterio duomen turinio poky ius, laikomi nusikaltimu, asmuo žinojo ar tur jo žinoti, kad neturi teis s vykdyti duomen keitimo (sankcijos už toki veik yra analogiškos, nurodytoms 2 straipsnyje).

Baudžiamosios atsakomyb s normos d l neteis to informacijos rinkimo, neteis tos prieigos prie informacijos, neteis to per mimo taip pat yra nustatytos Akte d l tyrim reguliavimo. Šis aktas numato, kad ty inis be nustatyto leidimo vykdomas bet kokio pob džio ryšio viešaisiais



telekomunikaciniais tinklais per mimas yra laikomas nusikaltimu. Už šio nusikaltimo vykdym numatyta bausm - bauda arba laisv s at mimas iki 2 met .

**Ispanija.** Ispanijos Baudžiamojo kodekso 197 straipsnis numato baudžiam j atsakomyb už slapt duomen atskleidim ir platinim be savininko sutikimo, taip pat ir duomen iš elektroninio pašto arba saugom duomen baz se. Nusikaltimu taip pat yra laikoma informacijos, perduodamos telekomunikaciniais tinklais ar sistemomis, per mimas arba rašymo ar pasiklausymo rangos naudojimas. Už toki veik vykdym numatyta sankcija - bauda arba laisv s at mimas nuo 1 iki 4 met . Jeigu šie duomenys buvo viešai išplatinti, pademonstruoti arba pateko tretiesiems asmenims, numatytas laisv s at mimas nuo 2 iki 5 met . 197 straipsnyje yra kelios dalys, patikslinan ios bausm , atsižvelgiant vykdyto nusikaltimo sunkum , maksimali bausm numatoma tuo atveju, jeigu duomenys yra susij su nukent jusiojo ideologija, religija, sveikata, rase, seksualine orientacija (lietuviškas atitikmuo - ypatingieji asmens duomenys pagal Asmens duomen teisin s apsaugos statym ). 198 ir 199 straipsniai yra susij su 197 straipsniu ir skirti atvejams, kai nusikaltimo subjektas yra asmuo, galiotas dirbti su duomenimis, o taip pat kai nusikaltimas yra vykdomas pareig no, viršijant tarnybinius galiojimus. Už šias veikas baudžiama laisv s at mimu iki 10 met . 263 straipsnis numato atsakomyb už telekomunikacij panaudojim be savininko sutikimo, jei taip buvo padaryta žala (sankcija - laisv s at mimas nuo 3 m nes i iki 1 met ). 264 straipsnio 2 dalis numato atsakomyb asmenims, kurie kokiu nors b du sugadino, padar netinkamais naudotis ar kitaip padar žal svetimiems elektroniniams duomenims, programoms ar dokumentams, esantiems tinkle, informaciniuose renginiuose ar sistemose. Už tokio pob džio nusikaltim numatyta bausm - bauda arba laisv s at mimas nuo 1 iki 3 met . 278 straipsnis numato baudžiam j atsakomyb už duomen , rašytini ar elektronini dokument , informacini rengini ar kit objekt , kurie priskiriami komercin ms paslaptims, gavim bet kokiu b du.

**Pranc zija.** Pranc zijos Baudžiamajame kodekse yra du – 186<sup>1</sup> ir 323 straipsniai, susij su kompiuteriniais nusikaltimais. 186<sup>1</sup> straipsnis nustato baudžiam j atsakomyb už neteis t duomen per mim elektronini ryši (telekomunikacin se) sistemose. Už šio nusikaltimo padarym numatoma bausm - bauda arba laisv s at mimas iki 1 met , o jei nusikaltimo subjektas yra pareig nas, tai laisv s at mimo bausm gali b ti padidinta iki 5 met . 323 straipsnio pirma dalis numato baudžiam j atsakomyb už neteis t prieig prie automatizuotos duomen apdorojimo sistemos ar tokios sistemos dalies, jei tokios prieigos metu sunaikinti ar pakeisti duomenys, saugomi sistemoje, arba pažeistas ar pakeistas sistemos funkcionalumas. Atsakomyb pagal min t straipsn gali b ti pritaikyta ir už kenk jišk program suk rim , pasik sinim silaužti sistem , neteis t prieig prie duomen , neteis t prieig prie ryšio sistem . Už ši nusikalstam veik padarym yra numatoma bausm - bauda ar laisv s at mimas iki 2 met . 323 straipsnio antroji dalis

nustato atsakomyb už duomen pakeitim ar bet kok kit siskverbim veikian i automatizuot duomen apdoravimo sistem . Tre ioji šio straipsnio dalis nustato atsakomyb už duomen pakeitim sistemose su klastojimo arba suk iavimo tikslu. Už nurodytus nusikaltimus numatytos bausm s - bauda arba laisv s at mimas iki 3 met .

**Vokietija.** Vokietijos Baudžiamajame kodekse yra pakankamai daug straipsni , kurie gali b ti taikomi ir kompiuteriniams nusikaltimams, ta iau pagrindiniai yra du – 202 ir 303 straipsniai. 202 straipsnio a punktas numato baudžiam j atsakomyb asmeniui už neteis t duomen , apsaugot specialiomis priemon mis nuo neteis tos prieigos, pa mim , siekiant asmenin s naudos ar naudos tre iajam asmeniui. 202 straipsnis nustato atsakomyb už neteis t prieig prie duomen , laikom elektronin se ar magnetin se laikmenose, ar kitose panašiose laikmenose, t.y. tokie duomenys apibr žiami kaip kompiuteriniai. Už ši veik taikoma bausm - bauda arba laisv s at mimas iki 3 met . 303 straipsnio a punktas nustato atsakomyb už duomen pakeitim , duomen ištrynim , sunaikinim , padarym netinkamais naudoti ar pasik sinim atlikti išvardintus veiksmus. Šis straipsnis taikomas tik tiems duomenims, kurie nurodyti 202 straipsnyje. Bausm - bauda arba laisv s at mimas iki 2 met . 303 straipsnio b punktas apima tokius nusikaltimus kaip DNS atakos (kompiuterinis sabotažas) ir kenk jišk program suk rimas. Straipsnyje apibr žta, kad kompiuterinis sabotažas – tai sikišimas duomen apdoravimo proces , kuris yra svarbus monei, valstyb s institucijoms, ar verslui. sikišimas gali b ti vykdytas b dais, nurodytais 303 straipsnio a punkte arba sunaikinant, pažeidžiant, padarant netinkamais naudoti, pakei iant kompiuterin sistem ar sikišant duomen perdavimo sistem . Nurodytos veikos baudžiamos bauda arba laisv s at mimu iki 5 met . Baudžiama ir už pasik sinim vykdyti min tus nusikaltimus.

**Estija.** Estijos elektronini ryši sektorius yra vienas labiausiai išvystyt Centrin je ir Ryt Europoje, ta iau greita informacin s visuomen s pl tra buvo glaudžiai susijusi ir su kompiuterini nusikaltim plitimu. Šiuo metu pagrindin s kompiuterini nusikaltim r šys, kriminalizuotos Estijoje, yra kompiuterinis suk iavimas (fišingas, kardingas), neteis tas kompiuteri , kompiuterini sistem ar kompiuteri tinkl panaudojimas), kenk jišk program (kompiuterini virus , kirmin , Trojos arkli ir kit ) panaudojimas vairiems nusikalstamiems tikslams, pedofilijos turinio platinimas internete. Estai m si pertvarkyti savo teis s akt baz jau 2000 m. Nuo 2000 m. sigaliojo trys svarb s statymai elektronini ryši srityje: Asmens duomen apsaugos aktas, Informacin s visuomen s paslaug aktas ir Telekomunikacij aktas, nustatantys atsakomyb už „spam“ ir reguliuojantys komercin komunikacij internete. Informacin s visuomen s paslaug aktas nustat tam tikras ribas informacin s visuomen s paslaug tiek jams ir atsakomyb už šio akto nuostat pažeidimus. Juo vadovaujamas, kai b tina kovoti su neteis tu viešu turinio paskelbimu Internete, nustatant reikalavimus automatizuotoms paslaugoms ir duomen

perdavimui. Be to, Estija 2004 m. ratifikavo papildomą Vaikų teisių konvencijos protokolą dėl prekybos vaikais, vaikų prostitucijos ir vaikų pornografijos, kuris padeda kovoti su vaikų pornografijos platinimu internete. 2003 m. Estijos Parlamentas ratifikavo Europos Tarybos Konvenciją dėl elektroninių nusikaltimų.

**Latvija.** Latvijos Baudžiamasis kodeksas buvo atnaujintas 2002 m., kriminalizuojant šias veikas, susijusias su kompiuteriais ar jų tinklais, ryšiu per mimas, savavališkas prisijungimas prie kompiuterinių sistemų, neteisėtas kompiuterinių programų sigijimas; programinėsrangos sugadinimas, kompiuterinių virusų platinimas, informacinių sistemų apsaugos priemonių pažeidimas. Be to, daug diskusijų sukėlė klausimas, ar terorizmo apibūdinimas Latvijos baudžiamojoje teisėje apima ir kompiuterinį terorizmą, tačiau tokio pobūdžio bylų praktikoje dar nebuvo, todėl sunku pasakyti, kaip teismai interpretuos šį straipsnį. Už minėtus kompiuterinius nusikaltimus Baudžiamojo kodekso numatytos sankcijos – bauda arba areštas (trumpalaikis laisvės atėmimas nuo 3 dienų iki 6 mėnesių). Atkreiptinas dėmesys tai, kad naujasis Latvijos Baudžiamojo proceso kodeksas, kuris buvo patvirtintas 2005 m. balandžio 21 d. ir sigaliojo nuo 2005 m. spalio 1 d., nustatė specialius procesinius veiksmus, susijusius su kompiuterinių nusikaltimų tyrimu.

**Lenkija.** Galiojantiame Lenkijos Baudžiamajame kodekse kompiuteriniams nusikaltimams paskirtas atskiras skirsnis. Be to, atskiruose straipsniuose numatyta baudžiamoji atsakomybė už nusikaltimus, susijusius su intelektinės nuosavybės teisių pažeidimu. Visos procesinės procedūros, tarp jų ir tyrimo bei sulaikymo, yra nustatytos Baudžiamojo proceso kodekse. Pastaraisiais metais sigaliojo keletas šio kodekso pataisų, susijusių su kompiuteriniais nusikaltimais. 2004 m. gegužės 18 d. baudžiamųjų statymų pataisos buvo priimtose siekiant suderinti Lenkijos Baudžiamojo kodekso ir Baudžiamojo proceso kodekso nuostatas su Europos Konvencija dėl elektroninių nusikaltimų.

Lenkijos statyme dėl elektroninių būdu teikiamų paslaugų (2002 m. liepos 18 d.) tvirtintos nuostatos, draudžiančios perteklinę informacijos siuntimą, nepageidaujamos komercinio pobūdžio informacijos platinimą („spam“).

Apibendrinant Europos valstybių, pasirašiusių Konvenciją dėl elektroninių nusikaltimų, baudžiamosios teisės harmonizavimo patirtį, galima teigti, kad nacionaliniai statymai turi daug skirtumų tiek teisiniuose technikos, tiek turinio prasme. Vis dėlto daugelyje valstybių veiktos, susijusios su kompiuterinėmis technologijomis bei informacijos saugos pažeidimais, yra kriminalizuotos, nors sankcijos už analogiškas veikas gali gerokai skirtis. Būtina pastebėti, jog po Konvencijos dėl elektroninių nusikaltimų pasirašymo ryškėja gera tendencija, siekiant sutvarkyti, pakeisti ar papildyti ir suvienodinti nacionalinius teisės aktus, o tai, savo ruožtu, turi didžiulę reikšmę kovojant su kompiuteriniais nusikaltimais.

### 3.2. KOMPIUTERINI NUSIKALTIMŲ TEISINIS REGLAMENTAVIMAS LIETUVOJE

Kaip jau buvo minėta, Lietuvos Respublikos baudžiamajame kodekse terminas „kompiuterinis nusikaltimas“ nėra apibrėžtas, taigi jis oficialiai nėra teisintas *de jure*, tačiau kalbant apie veikas, susijusias su kompiuteriniais technologijomis bei elektronine erdve, vartojamas *de facto*. Lietuvoje nėra specialaus statymo, reglamentuojančio kompiuterinius nusikaltimus, tačiau kai kurių statymų normos gali būti taikomos kompiuteriniams nusikaltimams ar pažeidimams. Svarbu tai, kad naujajame Lietuvos Respublikos baudžiamajame kodekse veikoms, susijusioms su kompiuteriniais technologijomis, paskiras atskiras XXX skyrius „**Nusikaltimai informatikai**“. Kriminalizuotos yra penkios veikos:

- 1) kompiuterinės informacijos sunaikinimas ar pakeitimas (196 straipsnis);
- 2) kompiuterinės programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas (197 straipsnis);
- 3) kompiuterinės informacijos pasisavinimas ir skleidimas (198 straipsnis);
- 4) neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo (198<sup>1</sup> straipsnis);
- 5) neteisėtas disponavimas reikmenimis, kompiuteriniais programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti (198<sup>2</sup> straipsnis).

Reikia pastebėti, kad Lietuvos Respublikos vidaus reikalų ministerijos Nusikalstamų veikų žinybinio registro, kurį tvarko Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos Statistikos skyrius, duomenimis, sigaliojus naujajam Baudžiamajam kodeksui, santykinai labai mažai veikų kvalifikuota pagal šio kodekso XXX sk. „Nusikaltimai informatikai“ straipsnius: nuo 2003 m. gegužės 1 d. iki 2006 m. rugsėjo 1 d. iš viso užregistruotos 55 veikos, iš jų 20 veikų (žr. 4 priedas 1 lentelė). Galima daryti prielaidą, jog tai lemia kelios objektyvios aplinkybės: kompiuterinės technologijos dažniausiai panaudojamos siekiant vykdyti kitas nusikalstamas veikas (plg. 4 priedas 2 lentelė), be to, šios rūšies nusikaltimams būdingas ypač didelis latentinis (iki 90 proc.).

Pažymėtina, kad už **kompiuterinius nusikaltimus intelektinei nuosavybei** atsakomybė gali būti taikoma pagal Baudžiamojo kodekso XXIX skyrių „Nusikaltimai intelektinei ir pramoninei nuosavybei“. Baudžiamojo statymo kriminalizuotos šios veikos:

- 1) autorystės pasisavinimas (191 str.);
- 2) literatūros, mokslo, meno ar kitokio kūrinių neteisėtas atgaminimas, neteisėtas kopijavimas, platinimas, gabenimas ar laikymas (192 str.);
- 3) informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas (193 str.);
- 4) neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių

pašalinimas (194 str.).

Beje, šios nusikaltimų sudėty buvo reglamentuotos ir senajame Baudžiamajame kodekse. Atkreiptinas dėmesys tai, kad skirtingai nei senajame Baudžiamajame kodekse, aprašant minėtus nusikaltimų objektyviuosius požymius nepateikiama tiesioginė nuoroda kompiuterinėms programoms, tačiau pagal Lietuvos Respublikos autorių teisių ir gretutinių teisių statymą kompiuterinė programa yra laikoma kūrinium, todėl naujojo Baudžiamojo kodekso 191-194 straipsniai taikytini ir kompiuterinėms programoms atžvilgiu.

**Kompiuteriniai nusikaltimai, susiję su vaikų pornografija**, gali būti baudžiami pagal Baudžiamojo kodekso 162 straipsnį (vaiko išnaudojimas pornografijai) ir 309 straipsnį (disponavimas pornografinio turinio dalykais). 162 straipsnis nustato atsakomybę už vaiko išnaudojimą pornografinėi produkcijai gaminti (atsakomybę pagal šį straipsnį taikoma gamintojams: operatoriui, fotografui ir kitiems). Baudžiamojo kodekso 309 straipsnio 2 dalis nustato atsakomybę už tokios produkcijos, kurioje vaizduojamas vaikas arba asmuo, pateikimą kaip vaikas, pagaminimą su tikslu platinti, ar jos sigijimą arba platinimą, o Baudžiamojo kodekso 309 straipsnio 3 dalyje numatoma, kad baudžiamas tas, kas viešai demonstravo ar reklamavo pornografinio turinio dalykus arba gijimą ar laikymą pornografinio turinio dalykus.

Už **kompiuterinius nusikaltimus privataus gyvenimo neliečiamumui** atsakomybę gali būti taikoma pagal naujojo Baudžiamojo kodekso XXIV skyrių „Nusikaltimai asmens privataus gyvenimo neliečiamumui“. Baudžiamojo statymo kriminalizuotos šios veikos:

- 1) neteisėtai susirašinėjimo, kitokių pranešimų, siuntimų ar pokalbių telefonu slaptumo pažeidimas (166 straipsnis);
- 2) neteisėtai informacijos apie privatų asmens gyvenimą rinkimas (167 straipsnis);
- 3) neteisėtai informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas (168 straipsnis).

Lietuvos kriminalinės policijos biuro Nusikaltimų tyrimo vyriausiosios valdybos Nusikaltimų elektroninėje erdvėje tyrimo skyriaus duomenimis, galiojančiame Baudžiamajame kodekse nurodyta keletas tradicinių nusikaltimų, susijusių su informacijos saugumo pažeidimu, kuriuos darant gali būti naudojama kompiuterinė technika<sup>25</sup>: šnipinėjimas (119 straipsnis); neteisėtai disponavimas informacija, kuri yra valstybės paslaptis (124 straipsnis); valstybės paslapties atskleidimas (125 straipsnis); valstybės paslapties praradimas (126 straipsnis); šmeižimas (154 straipsnis); žeidimas (155 straipsnis); diskriminavimas dėl tautybės, rasės, lyties, kilmės, religijos ar kitos grupinės priklausomybės (169 straipsnis); kurstymas prieš bet kokios tautos, rasės, etninę, religinę ar kitokių žmonių grupę (170 straipsnis); komercinis šnipinėjimas (210 straipsnis);

<sup>25</sup> Nusikaltimų elektroninėje erdvėje tyrimo skyriaus veikla // [http://www.cyberpolice.lt/index\\_.asp?DL=L&TopicID=4](http://www.cyberpolice.lt/index_.asp?DL=L&TopicID=4); prisijungimo laikas: 2006-10-14.

komercinės paslapties atskleidimas (211 straipsnis); melagingas pranešimas apie visuomenei gresiant pavoj ar ištikusį nelaim (285 straipsnis); grasinimas valstybės tarnautojui ar viešojo administravimo funkcijas atliekaniam asmeniui (287 straipsnis); valstybės tarnautojo ar viešojo administravimo funkcijas atliekanio asmens žeidimas (290 straipsnis); neteisėtai specialios technikos rengimas ar panaudojimas informacijai rinkti (295 straipsnis); tarnybos paslapties pagrobimas ar kitoks neteisėtus gijimas (296 straipsnis); tarnybos paslapties atskleidimas (297 straipsnis).

Išanalizavus Nusikalstam veik žinybinio registro 2003–2006 m. statistinius duomenis (žr. 4 priedas 7 ir 8 lentelės), darytina išvada, jog informatikos priemonės (kompiuterinė technika (74) ir internetas (75)), kaip nusikalstamos veikos padarymo priemonės, dažniausiai panaudojamos vykdant šiuos tradicinius nusikaltimus: šmeižimas (154 straipsnis); sukčiavimas (182 straipsnis); literatūros, mokslo, meno ar kitokio kūrinių neteisėtą atgaminimą, neteisėtą kopijavimą, platinimą, gabenimą ar laikymą (192 straipsnis); netikrą pinigų ar vertybinių popierių pagaminimą, laikymą arba realizavimą (213 straipsnis); neteisėto mokėjimo instrumento ar jo duomenų panaudojimą (215 straipsnis); dokumento suklastojimą ar disponavimą suklastotu dokumentu (300 straipsnis, senojo BK 207 straipsnis); antspaudo, spaudo ar blanko suklastojimą (301 straipsnis, senojo BK 208 straipsnis); disponavimą pornografinio turinio dalykais (309 straipsnis).

Siekiant išsiaiškinti kompiuterinių nusikaltimų kriminalistinės charakteristikos ypatumus, būtina trumpai apibūdinti šiuos nusikaltimus baudžiamąja teisine prasme. Išanalizavus galiojančio Baudžiamosios kodekso XXX skyriaus normas, reikia pastebėti, jog visi kompiuteriniai nusikaltimai, išskyrus kompiuterinės informacijos pasisavinimą ir skleidimą (198 str.), **sud tisyra materialios**, t.y. tokio pobūdžio nusikalstama veika turėtų sukelti didelę žalą (kuri gali būti tiek turtinė, tiek neturtinė).

Atkreiptinas dėmesys tai, kad, kitaip nei senajame Baudžiamajame kodekse, galiojantis Baudžiamasis kodeksas **detaliai neaprašo veikos padarymo būdą**, nes teisiškai netikslinga ar net nerealu apibrėžti visus būdus, kuriais galima paveikti kompiuterinę informaciją, ypač vertinusiųjų dinamiką.

Galiojantis Baudžiamasis kodeksas nustato, kad kompiuteriniai nusikaltimai **subjektas** gali būti ne tik **fizinis, bet ir juridinis asmuo**. 20 straipsnyje nurodyta, kad juridiniai asmenys už nusikalstamas veikas atsako, jeigu nusikalstamą veiką juridinio asmens naudai arba interesais padarė fizinis asmuo, veikęs individualiai ar juridinio asmens vardu, jeigu jis, eidamas vadovaujančias pareigas juridiniame asmenyje, turėjo teisę: atstovauti juridiniam asmeniui arba priimti sprendimus juridinio asmens vardu, arba kontroliuoti juridinio asmens veiklą. 20 straipsnio trečioji dalis nustato, kad juridinis asmuo gali atsakyti už nusikalstamas veikas ir tuo atveju, jeigu

jas juridinio asmens naudai padar juridinio asmens darbuotojas ar galiotas atstovas d l jam vadovaujantio asmens nepakankamos priežiūros arba kontrolės. Be to, juridinio asmens baudžiamoji atsakomyb nepašalina fizinio asmens, kuris padar , organizavo, kurst arba padar jo padaryti nusikalstam veik , baudžiamosios atsakomyb s.

Baudžiamojo kodekso apibr žt kompiuterini nusikaltim sud ties analiz rodo, jog **kalt s forma gali b ti tiek ty ia, tiek neatsargumas**, bet galima teigti, jog didžioji dalis ši veik bus padaromos tiesiogine ty ia, re iau – netiesiogine, o galimyb tokias veikas padaryti d l nusikalstamo pasitik jimo ar nusikalstamo ner pestingumo yra mažai tik tina, vertinus kompiuterini sistem funkcionavimo ypatumus bei saugos priemones.

vertinus galiojan io Baudžiamojo kodekso XXX skyriaus norm sankcijas, pažym tina, kad visi kompiuteriniai nusikaltimai **yra nesunk s**, nes pagal Baudžiamojo kodekso 11 straipsnio tre i j dal nusikaltimai, už kuriuos statymas numato bausm , neviršijan i 3 met laisv s at mimo, laikomi nesunkiais.

B tina pasteb ti, kad veikos, nurodytos Baudžiamojo kodekso XXX skyriuje, dažnai vykdomos ne kaip atskiri nusikaltimai, bet kartu su kitais nusikaltimais ir inkriminuojamos papildomai. Tai s lygota aplinkyb s, jog kompiuterin technika ir informacija dažniausiai panaudojama siekiant vykdyti kitas nusikalstamas veikas.

2004 m. kovo 18 d. Lietuva ratifikavo Konvencij d l elektronini nusikaltim (Lietuvos Respublikos 2004 m. sausio 22 d. statymu Nr. IX-1974 (Žin., 2004, Nr.36), kuri sigaliojo nuo 2004 m. liepos 1 d. Išanalizavus Konvencijos rekomenduojamas kriminalizuoti neteis tas veikas bei m s Baudžiamojo kodekso XXX skyriaus „Nusikaltimai informatikai“ kriminalizuotas veikas, galima daryti išvad , jog šiuo metu kodekso normos iš esm s atitinka Konvencijos reikalavimus. 2004 m. sausio 29 d. Lietuvos Respublikos Seimas pri m Baudžiamojo kodekso pataisas, kuriomis suderino Baudžiamojo kodekso 196 ir 197 straipsnius su Konvencijos nuostatomis, taip pat papild Baudžiamojo kodekso XXX skyri 198<sup>1</sup> straipsniu „Neteis tas prisijungimas prie kompiuterio ar kompiuterinio tinklo“ ir 198<sup>2</sup> straipsniu „Neteis tas disponavimas renginiais, kompiuterin mis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti“. Ta iau galima b t pamin ti ir kelet Lietuvos Baudžiamojo kodekso ir Konvencijos neatitikim : rengiant Baudžiamojo kodekso pataisas nebuvo atsižvelgta Konvencijos vartojamus terminus kompiuterini nusikaltim apib dinimui, pvz., Lietuvos Baudžiamojo kodekso vartojamas kompiuterin s informacijos terminas neatitinka Konvencijos nustatyto termino *computer data*, reiškian io kompiuterinius duomenis, be to, Konvencijoje neskiriamos kompiuterini duomen ir kompiuterin s programos s vokos, kaip tai yra padaryta m s Baudžiamajame kodekse, nes kompiuterin s programos laikomos sudarytomis iš

kompiuterini duomen ir todėl iš esmės nesiskiria; Konvencijoje vartojama kompiuterinės sistemos sąvoka, reiškianti kietosios ir programinės rangos visumą, skirtą tvarkyti duomenis (taip apibrėžiamas kompiuteris arba kompiuterinis tinklas).

Šiuo metu teisės normos, taikytinos veikoms, susijusioms su kompiuterio panaudojimu, galima rasti atskiruose Lietuvos Respublikos statymuose, Lietuvos Respublikos Vyriausybės nutarimuose ir kituose teisės aktuose (sąrašas ir komentarai pateikiami 3 priede). Už šiuos teisės aktus, daugiau ar mažiau susijusių su visuomeninio santykių saugaus kompiuterinės informacijos tvarkymo srityje reglamentavimu, nustatyti reikalavimai pažeidimus atsakomybę numatyta Lietuvos Respublikos baudžiamajame kodekse ir Lietuvos Respublikos administraciniame teisės pažeidimų kodekse.

Kompiuterini nusikaltimų tyrimui taikomos bendrosios procesinės normos, nustatytos Lietuvos Respublikos baudžiamojo proceso kodekse, taip pat procesinės normos, nustatytos Konvencijoje dėl elektroninių nusikaltimų. Reikėtų pastebėti, jog atlikus Lietuvos kriminalinės policijos biuro Nusikaltimų tyrimo vyriausiosios valdybos Nusikaltimų elektroninėje erdvėje tyrimo skyriaus pareigūnų apklausą, pateikiant elektroninį klausimyną (žr. 5 priedas), paaiškėjo, jog Baudžiamojo proceso kodekso normos, taikytinos tiriant kompiuterinius nusikaltimus, netikslumas ar trūkumas nurodomas kaip viena iš priežasčių, slygojančių kompiuterini nusikaltimų tyrimo problemomis. Ikitiesminio tyrimo pareigūnų teigimu, keblumų kyla praktiškai taikant Baudžiamojo proceso kodekso normas, kurios nepakankamai išsamiai reglamentuoja veiksmus, susijusius su kompiuterini nusikaltimų tyrimo ypatumais. Taigi, galima teigti, jog būtina tikslinti Baudžiamojo proceso kodekso normas patikslinti, atsižvelgiant į Konvencijos dėl elektroninių nusikaltimų 2 skirsnio „Proceso teisės“ reikalavimus (laikomąjį kompiuterini duomenų paiešką ir poimį, kompiuterini duomenų surinkimą realiuoju laiku – srauto duomenų bei turinio duomenų perimtis).

Apibendrinant kompiuterini nusikaltimų teisinį reglamentavimą Lietuvoje, galima teigti, kad šiuo metu Lietuvos teisinė bazė pakankamai papildyta ir atnaujinta normomis, susijusiomis su kompiuterinių technologijų panaudojimu bei informacijos sauga, o Baudžiamojo proceso normos iš esmės atitinka Konvencijos dėl elektroninių nusikaltimų reikalavimus, tačiau, pagrindinė problema, autorės manymu, lieka šios srities terminologijos teisinis neapibrėžtumas.



## II. KOMPIUTERINI NUSIKALTIM APIB DINIMO KRIMINALISTINIAI ASPEKTAI

### 4. KOMPIUTERINI NUSIKALTIM KRIMINALISTIN CHARAKTERISTIKA

Kriminalistin charakteristika yra dinamiška kategorija, kintanti priklausomai nuo kriminalin s praktikos. Kriminalistinei nusikaltim charakteristikai svarb s nusikalstam veik elementai kei iasi pakankamai spar iai, nes tobul ja nusikaltim padarymo b dai, kinta nusikalstam veik tikslai ir motyvai, k sinimosi dalykas, priežastys ir s lygos, palankios tam tikroms nusikaltim r šims, tod l ir pati kriminalistin charakteristika n ra pastovi ir apibr žta vairi nusikaltim r ši duomen visuma, bet dinamiškas reiškiny, atspindintis b dingiausias nusikaltim ypatybes tam tikru laikotarpiu.

Taigi, siekiant, kad kriminalistin charakteristika atlikt savo praktin taikom j užduot ir pad t atskleisti nusikaltimus, ji privalo b ti tiksli, išsami ir aktuali, t.y. šiuolaikiška, atspindinti naujausius kriminalin s praktikos poky ius, apimti aktualius kriminalistin s nusikaltim , vykdyt pastaruoju laikotarpiu, analiz s rezultatus.

Daugelyje kriminalistikos mokslo darb pabr žiama, kad kompiuterini nusikaltim kriminalistin charakteristika, palyginus su kit nusikaltim r ši charakteristika, pasižymi savitomis ypatyb mis, kurias s lygoja kompiuterini nusikaltim pagrindini strukt rini element specifika ir išskirtiniai, tik šiai nusikaltim r šiai b dingi bruožai. Atkreiptinas d mesys šiuos kriminalistiniu poži riu svarbius elementus:

- pažeid jo asmenyb ;
- nusikalstamo elgesio motyvai ir tikslai;
- tipiniai nusikaltimo rengimo, vykdymo ir nusl pimo b dai;
- laikas, vieta ir pasik sinimo aplinkyb s.

Be to, kriminalistikos mokslo darbuose akcentuojamos ir kompiuterin s informacijos, kaip pasik sinimo dalyko, išskirtin s kriminalistin s ypatyb s:

1) kompiuterin informacija palyginti paprastai ir greitai kei iama (kinta), kopijuojama, dauginama vairia technine ranga, siun iama vairiausiu atstumu, ribojamu tik elektronini ryši rangos veikimo plotu;

2) paimant kompiuterin informacij (atliekant po m ), skirtingai nei material objekt (daikt ), ji išlieka pirminiame šaltinyje, nes prieig prie jos gali tur ti tuo pa iu metu keli asmenys, pvz., jei dirbama su informacija, esan ia faile, kuriuo gali naudotis keli informacin s sistemos vartotojai.

Kompiuterinio nusikaltimo vykdymo aplinkyb s apima vairius aplinkos, kurioje vykdyta nusikalstama veika, faktorius: fizinius, techninius, socialinius ir psichologinius. Tai gali

takoti visus kitus kompiuterini nusikaltim kriminalistin s charakteristikos elementus bei lemti nusikalt lio ir nukent jusiojo elgesio ypatumus.

V.B.Vechovas metodiniame leidinyje „Nusikaltim , vykdom panaudojant elektronin s skai iavimo technikos priemones, tyrimo ypatyb s“ nurodo, kad kompiuterini nusikaltim rengimo, vykdymo ir nusl pimo aplinkybi visumos kriminalistin savitum lemia dvejopi faktoriai – objektyv s ir subjektyv s<sup>26</sup>. Prie objektyvi faktori galima b t priskirti šias nukent jusi fizini ir juridini asmen veiklos s lygas:

- veiklos sritis arba darbo pob dis ( kin , gamybin , komercin , valdymo, informacin , tarpininkavimo, finansin , energetin , paslaug ir kita veikla);
- juridinio ar fizinio asmens nuosavyb s forma, informacini sistem ir informacini ištekli , kaip nuosavyb s dalies, teisinis statusas;
- gamybini ar valdymo proces paskirtis ir organizacin strukt ra, naudojam ištekli ir gaminamos produkcijos, taip pat ir intelektualios, pob dis;
- apskaitos ir atsiskaitomyb s sistemos pob dis;
- žmonišk j ištekli (personalo) valdymas ir materialinis-techninis apr pinimas;
- naudojam kompiuterini sistem , telekomunikacij rangos r šys, j techniniai duomenys ir konstrukciniai tr kumai;
- patalp ir rangos pob dis;
- produkcijos, kit vertybi apskaitos ir realizavimo tvarka;
- vis grandži apsaugos sistem pob dis (apsaugos priemoni egzistavimas, technin b kl ir kt.).

Prie subjektyvi faktori galima b t priskirti šias nukent jusi fizini ir juridini asmen veiklos organizacinio, socialinio, psichologinio pob džio s lygas:

- informacijos apdorojimo technologini proces , gamybos, diegimo, derinimo, remonto, techninio aptarnavimo, kompiuterini sistem eksploatavimo, taip pat vertybi apskaitos, saugojimo, skirstymo, panaudojimo tvark reglamentuojan i taisykli pažeidimas ir nesilaikymas;
- ši taisykli netobulumas;
- informacijos apsaugos priemoni nebuvimas ar netobulumas;
- darbo su statym saugoma kompiuterine informacija (pvz., valstyb s, tarnybos ar komercin mis paslaptimis) taisykli pažeidimas;
- nepagr stas kompiuterini sistem naudojimas konkre iuose technologiniuose procesuose ir operacijose;

- nepatenkinamas gamybini ar valdymo proces organizavimas, dokument administravimo sistemos tr kumai, pvz., dokument neautomatizuotos („rankin s“) ir automatizuotos apskaitos egzistavimas tuo pa iu metu;
- netinkama psichologin darbo aplinka (problemiški asmeniniai santykiai tarp vadov ir pavaldini , kit darbuotoj , atsakomyb s masto ir darbo užmokes io neatitikimas).

Tiek objektyv s, tiek subjektyv s faktoriai gali stipriai takoti konkretaus kompiuterinio nusikaltimo vykdymo aplinkybes.

#### 4.1. KOMPIUTERINI NUSIKALTIM SUBJEKTO CHARAKTERISTIKA

Svarbi nusikaltim , susijusi su kompiuterin s technikos panaudojimu, kriminalistin s charakteristikos dalis yra duomenys, apib dinantys nusikaltimo subjekt .

Asmenys, darantys kompiuterinius nusikaltimus, pagal specializacij skirstomi kelias grupes<sup>27</sup>, nusikalt li žargonu vadinamas “hakeriais”, “krekeriais”, “frekeriais”, „karderiais“ (angl.k. „*hacker*“, „*cracker*“, „*phracker*“, „*carder*“). Hakeris – tai kompiuterio, informacin s sistemos ar tinklo vartotojas, kuris dažniausia savanaudiškais tikslais užsiima nesankcionuotos prieigos prie kompiuterini sistem ar statym saugomos kompiuterin s informacijos b d paieška. Krekeris – kompiuterio, informacin s sistemos arba tinklo vartotojas, kuris specializuojasi statym saugomos kompiuterin s informacijos programini ir technini apsaugos priemoni „nulažimo“ srityje (modifikavimo, blokavimo, sunaikinimo). Karderiai – t a i profesional s nusikalt liai, užsiimantys neteis ta veikla elektronini korteli apyvartos bei elektronini rekvizit padirbimo ir klastojimo srityje. Frekeri specializacija – nusikaltimai elektronini ryši , telekomunikacij srityje, panaudojant konfidenciali informacij ir specialias technines priemones, skirtas srauto duomen ir turinio per mimui.

vairi šali kriminalist duomenimis, hakeriai ir kiti kompiuteriniai nusikalt liai veikia tiek pavieniui, tiek jungdamiesi regionines grupes, be to, naudojami internetu savo „profesinei“ informacijai skleisti bei keistis patirtimi tarptautiniu mastu, j elektroniniuose leidiniuose pateikiama vairi kompiuterini nusikaltim vykdymo metodika ir nusl pimo b dai, kiti duomenys, padedantys jauniems pažeid jams tobul ti. V.B.Vechovo pasteb ta, jog Rusijoje šie asmenys leidžia savo elektronines masin s informacijos priemones (laikraš ius, žurnalus, skelbim lentas su skubiais pranešimais), rengia elektronines konferencijas, kiekviena grup (“hakeriai”, “krekeriai”, “frekeriai”, „karderiai“) turi savo žargonin žodyn , kuris yra nuolat papildomas ir platinamas elektroniniais leidiniais. Be to, nusikalt liai glaudžiai bendradarbiauja su užsienio „kolegomis“, naudodamiesi globaliais telekomunikaciniais tinklais.

Kompiuteriniai nusikalt liai priklauso vairiems visuomen s sluoksniams – nuo moksleivi ir student m g j iki profesionali nusikalt li , terorist grupuo i , pagal išsilavinim šiuos asmenis galima suskirstyti diletantus ir profesionalus. Nusikalt li amžius svyruoja nuo 15 iki 45 met , Europos ir JAV tyr j duomenis, nusikaltimo vykdymo metu 33 proc. nusikalt li amžius neviršijo 20 met , 13 proc. – vyresni nei 40 met ir 54 proc. – nuo 20-40 met .Lietuvos Respublikos vidaus reikal ministerijos tariam , kaltinam ir teist asmen žinybinio registro duomenimis, asmen , kaltinam nusikalstamos veikos, kurios pasik sinimo dalykas - kompiuterin informacija ir sistemos, o priemon - kompiuterin technika ar internetas, padarymu, amžius toks:

<sup>27</sup>

iki 20 metų – beveik 22 proc., vyresni nei 40 metų – 14 proc., nuo 20 iki 40 metų – 64 proc. (žr. 4 priedo 9 lentelę); šių asmenų išsilavinimas: aukštasis – 22 proc., aukštesnysis arba profesinis – 23 proc., vidurinis, pagrindinis ar pradinis – 55 proc. (žr. 4 priedo 10 lentelę); užimtumas: valstybės tarnautojai – 9 proc., nevalstybiniai staigūs ir moniški darbuotojai – 34 proc., moksleiviai ir studentai – 21 proc., nedirbantys ir nesimokantys – 36 proc. (žr. 4 priedo 11 lentelę). Palyginus pasaulio ir Lietuvos kompiuterinio nusikaltimų tendencijas bei vertinus šio nusikaltimo latentinį pavojumą, galima daryti prielaidą, jog šiuo metu Lietuvoje išaiškinama daugiausia santykinai nesudėtingų kompiuterinio nusikaltimų, nes daugiau nei pusę jų padariusi asmenys turi vidurinį ar žemesnį išsilavinimą, kai tuo tarpu kitose Europos valstybėse ir JAV didžioji dalis šių asmenų priskiriami „baltųjų apykaklių“, t.y. turinčių aukštą išsilavinimą tarnautojų ir darbuotojų kategorijai.

Mokslo leidiniuose asmenys, darantys kompiuterinius nusikaltimus, skirstomi į įvairius pagrindais, pvz., pagal jų minties specializaciją, taip pat pagal motyvaciją (skiriamos trys grupės: hakeriai, tipiniai nusikaltėliai ir vandalai), pagal organizacinę priklausomybę (skiriami asmenys, susiję su staiga, mone ar organizacija darbo santykiais (darbuotojai) ir nesusiję darbo santykiais (pašaliniai asmenys) ir kt. Rusijoje dažnas autorius skirsto kompiuterinius nusikaltėlius į tris grupes: 1) informacinių technologijų profesionalai, programuotojai; 2) asmenys, sergantys psichikos ligomis, susijusiomis su informacijos badu, perkrova arba fobijomis; 3) profesionalūs nusikaltėliai. Pastaroji grupė kelia didžiausią grėsmę ir padaro nuostolingiausių ekonominių nusikaltimų. Nuo pirmųjų dviejų grupių ji skiriasi tuo, kad turi aiškias nusikalstamų motyvacijų, o jų veikla pasižymi pakartotinumumu ir organizuotumu.

Asmenys, darantys kompiuterinius nusikaltimus, veikia skirtingose srityse ir išorės pasiekimus. Svarbu pastebėti, jog didžioji dalis kompiuterinio nusikaltimų juridinio asmens atžvilgiu vykdomi nusikaltėlių arba jų bendrininkų, kurie yra tos staigos, organizacijos ar moniški darbuotojai (vidaus pasiekimai sudaro apie 80 proc. visų nusikaltimų, 90 proc. ekonominių kompiuterinio nusikaltimų padaro staigūs ir moniški darbuotojai). Šie asmenys paprastai yra puikiai išsilavinę, turi specialias žinias ir turi praktinį patirties kompiuterinių technologijų srityje. Dažniausiai šie asmenys dirba kompiuterinių tinklų ar ryšių sistemų operatoriais, programuotojais, informacinių sistemų inžinieriais, duomenų bazių administratoriais, taip pat tai gali būti valstybės tarnautojai ar darbuotojai, dirbantys pagal darbo sutartis, turintys prieigą prie informacinių sistemų, duomenų bazių ar telekomunikacinio tinklo.

Apibrėžiant tokius nusikaltėlius, svarbu pabrėžti, kad jiems būdingas aukštas intelektas, nestandartinis mąstymas, išradingumas, profesionalumas, fanatiškas domėjimasis naujomis kompiuterinėmis technologijomis, turtinga fantazija ir tam tikras paslaptinumas. Paprastai tokie asmenys yra pavyzdingi darbuotojai, turintys atitinkamą išsilavinimą, neretai – tai skirtingo lygio vadovai, tiesiogiai neatsakingi už konkrečias darbo su kompiuterine informacija

sritis. Dažniausiai šie asmenys nebena patekę teis saugos akiratin, anksčiau nevykdę joki nusikaltimų.

Būtinai pastebėti, kad vis dažniau kompiuteriniai nusikaltimai yra vykdomi organizuotai grupiai, kurioms būdinga aiški motyvacija siekiant naudos, geras techninės aprėpties, mobilumas, tikslus vaidmenų pasidalinimas, gerai apgalvota nusikalstamos veiklos pildymo sistema. Didžiausi pavojų kelia bei sunkiausiai išaiškinamos tos nusikalstamos grupės, kuriose dirba aukštos kvalifikacijos informatikos specialistai, ekonomistai, teisininkai, turintys specialinių ir patirties kompiuterinėje informacijos apsaugos srityje. Didelė dalis nusikaltimų, vykdytų šioje grupėje, išlieka latentiniai. Tariamais kaltinamais ir teisiamais asmenimis žinybinio registro duomenimis, beveik 30 proc. asmenų, kaltinamų nusikalstama veikla, kuri pasikėlė sinimo dalykas - kompiuterinė informacija ir sistemos, o priemonės - kompiuterinė technika ar internetas, padarymu, vykdytą veikla bendrininkų ar organizuotoje grupėje (pastarosios nariais buvo apie 3 proc. asmenų) (žr. 4 priedo 12 lentelę).

Galima konstatuoti, jog kompiuteriniai nusikaltimų vykdymo **motyvai ir tikslai** yra labai skirtingi:

- pasipelnymas (neteisėtai pinigai, vertybiniai popieriai, kredito, materialiniai vertybės, prekės, paslaugos, privilegijos, lengvatų, kvotų, nekilnojamojo turto, energetiniai ir kiti išteklių gavimas);
- mokesčių, rinkliavų mokėjimo vengimas;
- nusikalstamais būdais gauti pajamų legalizavimas;
- dokumentų, antspaudų, blankų, piniginių ženklų klastojimas ar gamyba savanaudiškais tikslais;
- konfidencialios ar slaptintos informacijos gavimas pasipelnymo ar politiniais tikslais;
- kerštas dėl asmeninio priešiško darbovietės administracijai ar kolegoms;
- šalies valiutos sistemos dezorganizavimas piktavališkais ar politiniais tikslais; padėties šalyje, atskiroje gyvenamojoje vietovėje ar staigoje destabilizavimas politiniais tikslais;
- pastangos nuslėpti kitus nusikaltimus;
- chuliganiškos paskatos;
- tyrinėjimo tikslai;
- asmeniniai intelektualiniai galimybių ir pranašumo demonstravimas.

Pagal statistinį populiarumą asmenų, darančių kompiuterinius nusikaltimus, motyvus

ir tikslus Interpolo ekspert komisija skirsto taip<sup>28</sup>:

- 1) savanaudiški – didžioji dalis, 66 proc.;
- 2) politiniai (terorizmas, politinės akcijos) – 17 proc.;
- 3) tiriamieji – 7 proc.;
- 4) chuliganiški – 5 proc.;
- 5) keršto – 4 proc.

Apibendrinant kompiuterini nusikaltimų subjekt charakteristik , galima pateikti šiuos bendruosius užsienio valstybi duomenis <sup>29</sup>: 1) amžius: 54 proc. – 20-40 met ; 33 proc. – jaunesni kaip 20 met ; 13 proc. – vyresni kaip 40 met ; 2) intelektas: 21 proc. – aukštesnis nei vidutinis; 2 proc. – žemesnis nei vidutinis; 3) išsilavinimas: 40 proc. – aukštasis; 40 proc. – specialusis; 20 proc. – vidurinis; 4) profesija: 52 proc. nusikaltėlių profesija susijusi su informacinėmis technologijomis; 5) organizuotumas: 62 proc. – nusikalstam grupių nariai; 38 proc. – veikia be bendrinink .

Lyginamieji užsienio valstybi ir Lietuvos kompiuterini nusikaltimų subjekt duomenys:

Rodiklis		Užsienio valstybi duomenys, proc.	Lietuvos duomenys, proc.
<b>1. Amžius:</b>	20-40 met –	54	64
	jaunesni kaip 20 met –	33	22
	vyresni kaip 40 met –	13	14
<b>2. Išsilavinimas:</b>	aukštasis –	40	22
	specialusis (aukštesnysis arba profesinis) –	40	23
	vidurinis (ir žemesnis) –	20	55
<b>3. Organizuotumas:</b>	nusikalstam grupių nariai –	62	29
	veikia be bendrinink –	38	71

Palyginus pasaulio ir Lietuvos kompiuterini nusikaltimų tendencijas bei vertinus ši nusikaltimų latentškumą , galima daryti prielaid , jog šiuo metu Lietuvoje išaiškinama daugiausia santykinai nesudėtingi kompiuterini nusikaltimai , nes daugiau nei pus jų padariusi asmen teturi vidurin ar žemesn išsilavinim , be to, mažiau nei tre dalis jų yra nusikalstam grupių nariai, kai tuo tarpu kitose Europos valstybėse ir JAV didžioji dalis ši asmen priskiriami „baltųjų apykaklių“, t.y. turinčių aukštą išsilavinimą tarnautojų ir darbuotojų , kategorijai, o nusikalstam grupių nariai sudaro net šešiasdešimt procent vis padariusi kompiuterinius nusikaltimus asmen .

<sup>28</sup>

// <http://www.crime-research.org>; prisijungimo laikas: 2006-05-06.

<sup>29</sup> Petrauskas R., Štītėlis D. Kompiuteriniai nusikaltimai ir jų prevencija.- Vinius, 2000. P.23.

## 4.2. KOMPIUTERINI NUSIKALTIM VYKDYMO LAIKAS IR VIETA

Apibdinant kompiuterini nusikaltim laik ir viet , b tina pasteb ti ši aplinkybi išskirtinum , kur s lygoja tai, jog kompiuteriniai nusikaltimai paprastai yra vykdomi nuotoliniu b du, naudojant nutolusius terminalus, kuriuos sieja su atakos objektu elektroninio ryšio kanalai, ta iau pasitaiko ir tiesiogin s prieigos atvej . Taigi, pirma, faktin neteis tos veikos vykdymo vieta ir visuomenei pavojing pasekmi atsiradimo vieta dažniausiai nesutampa; antra, veikos vykdymo ir pasekmi atsiradimo laikas taip pat gali skirtis, pati ataka gali trukti labai trumpai, nes vykdoma naudojant specialias technines ir programines priemone s, nors pasirengimo veikai stadija gali b ti pakankamai ilga. Tiek planuojant tokio pob džio nusikaltim , tiek j vykdant b tinos vairi sri i specialiosios žinios (informacijos apdorojimo ir apsaugos, finansini ir bankini operacij , technin s ir programin s rangos), taip pat paprastai reikalingas detalus nusikaltimo vykdymo planas bei kiti duomenys, padedantys nepalikti joki p dsak .

B tina pasteb ti, kad kompiuteriniai nusikaltimai gali b ti vietiniai, lokals arba tarptautiniai, transnacionaliniai, taigi tiriant šios kategorijos nusikaltim bylas, nusikalstamo pasik sinimo vieta gali b ti:

- 1) staiga, organizacija ar mon , kuri naudoja kompiuterin rang kuriame nors iš technologini ar administracini proces ;
- 2) konkreti, apibr žta teritorija ar sritis, iš kurios galima realizuoti prieig ;
- 3) neapibr žta teritorija, jei kompiuterin s atakos objektas jungtas tarptautin elektronini ryši tinkl (tai gali b ti kita valstyb , kitas žemynas).

Tiriant kompiuterini nusikaltim bylas, veikos vykdymo laikas gana retai nustatomas labai tiksliai, ta iau b na atvej , kai laik b tina fiksuoti valand ar minu i tikslumu, siekiant išsiaiškinti atskirus nusikalstamos veikos epizodus. Paprastai kompiuterini nusikaltim vykdymo laikas apskai iuojamas tam tikrais tarpsniais, susijusiais su konkre i fizini ar juridini asmen veikla. Baudžiam ja teisine prasme, nusikalstamos veikos vykdymo laiku yra pripaž stamas šios veikos vykdymo pabaigos laikas, nepriklausomai nuo pasekmi atsiradimo laiko.



### 4.3. KOMPIUTERINI NUSIKALTIM B DAI

Kriminalistikos metodikos darbuose paprastai pabr žiama, kad svarbiausiu bet kurios r šies nusikaltimo kriminalistin s charakteristikos elementu yra duomen , charakterizuojan i jo vykdymo b d , visuma. Baudžiamojoje teis je nusikaltimo b das yra objektyviosios nusikaltimo sud ties pus s požymis, kuris gali b ti tik fakultatyvinis, jei jis nenurodytas konkre ioje nusikaltimo sud tyje, arba b tinasis ( rodin tinas) požymis, jei yra nurodytas. Kriminalistikoje nusikaltimo vykdymo b das suprantamas kaip nusikaltimo subjekto veiksm visuma rengiant, vykdan bei slepian nusikaltim , t.y. pažeid jo veiksmai iki nusikaltimo padarymo, nusikaltimo padarymo metu ir po nusikaltimo, suformuojantys tam tikrus p dsakus.

Kompiuterini nusikaltim vykdymo b d išmanymas palengvina kompiuterini nusikaltim tyrim , nes kiekvienas b das palieka atitinkamus p dsakus, padeda apib dinti nusikalt lio asmenyb ir kryptingiau formuoti versijas, atsižvelgiant metodus ir j taikymo s lygas, b tinos tam technines priemones, šaltinius, iš kuri jos gautos ir kt.

Visi kompiuterini nusikaltim vykdymo ir nusl pimo b dai turi savo individualius, tik jiems b dingus požymius, pagal kuriuos galima juos atpažinti ir suskirstyti atskiras apibendrinan ias grupes. Pagrindinis klasifikuojantis požymis yra **metodas**, kurio pagalba nusikalt lis vykdo tiksling poveik kompiuterin s technikos priemon ms ir kompiuterinei informacijai. JAV Nacionalinio kompiuterinio saugumo instituto duomenimis, pagrindiniai kompiuterini nusikaltim metodai, kuriais neteis tai užvaldoma informacija, yra šie:

- pasiklausymo rangos panaudojimas;
- nuotolinis fotografavimas;
- elektroninio spinduliavimo per mimas;
- akustinio spinduliavimo per mimas ir spausdintuvo teksto atk rimas;
- mistifikacija (prisidengimas teis ta sistemos užklausa);
- informacijos kaupikli ir pramonini atliek (šiuokšli ) pagrobimas ar surinkimas;
- informacijos nuskaitymas iš kit vartotoj masyv ;
- informacijos kaupikli kopijavimas, veikiant apsaugos priemonės;
- apsimetimas registruotu vartotoju;
- programini sp st panaudojimas;
- neteis tas prisijungimas prie rangos ar ryšio linij ;
- apsaugos sistem sugadinimas.

V.B.Vechovas, laikydamasis kompiuterinio nusikaltimo traktavimo pla i ja prasme,

skiria šias apibendrintas metod grupes<sup>30</sup>:

1. kompiuterin s technikos pagrobimas;
2. informacijos per mimas;
3. nesankcionuota prieiga prie kompiuterin s sistemos ar kompiuterin s informacijos;
4. manipuliavimas duomenimis ar valdymo komandomis;
5. kompleksiniai metodai.

Pirmajai grupei priskiriami tradiciniai nusikaltim vykdymo b dai, kuriais nusikalt lis siekia pasisavinti svetim turt (t.y. bet koki kompiuterin technik , rengin ) ir vykdo vagyst ar grobim .

Antrajai kompiuterini nusikaltim vykdymo b d grupei priskiriami tokie b dai, kuriais nusikalt lis kompiuterin informacij gauna panaudodamas audiovizualinio ir elektromagnetinio informacijos per mimo metodus, taikomus ir teis saugos pareig n operatyvin s paieškos metu. Šiai grupei priklauso:

1. Pasyvus (bekontaktinis) per mimas, vykdomas nuotoliniu b du perimant elektromagnetin spinduliavim , sklindžiam veikian ios kompiuterin s rangos:

a) optini (vaizdo) signal , sklindan i matom , infraraudon j ir ultravioletini spinduli diapazone, per mimas (vykdomas naudojant optines, optines elektronines, televizines, lazerines, foto ir kitas vaizdo informacijos per mimo priemones);

b) akustini (garso) signal , sklindan i oro, vandens ar kietoje terp je, per mimas (vykdomas naudojant akustines, hidroakustines, viroakustines, lazerines ir seismines priemones);

c) elektromagnetini signal , sklindan i techniniais pagrindini ir pagalbini priemoni bei sistem kanalais, kaip parazitini informacini lauk per mimas: šalutinio elektromagnetinio spinduliavimo ir trukdži , parazitini aukšto dažnio signal moduliacij , parazitini informacini srovi ir tamp , sukuriam d l signalo elektroakustinio transformavimo radijo ir elektros ryši , radijotransliaciniuose, apsaugos ir priešgaisrin s signalizacijos, televizijos, kompiuterini sistem tinkluose ir kt.

2. Aktyvus (kontaktinis) per mimas, vykdomas tiesiogiai prisijungus prie kompiuterin s sistemos arba prie duomen perdavimo sistemos, panaudojant varias operatyvines technines ir specialiai pagamintas (pritaikytas) priemones, kai kuriais atvejais panaudojant slaptus kanalus. Šiuo atveju nusikalt lis gali tikslingai paveikti vis kompiuterin sistem , jos sud tines dalis, prieigos sankcionavimo sistem , duomen perdavimo kanalus ir pa i kompiuterin informacij .

---

<sup>30</sup>

, 1998. C .21.

Tre iajai grupei priskiriami kompiuterini nusikaltim vykdymo b dai, galinantys gauti neteis t prieig prie kompiuterin s sistemos, pavyzdžiui, pasinaudojant „legendos“ metodu („elektrikas“, „santehnikas“, „telefon meistras“ ir kt.), taip pat nesankcionuoto prisijungimo prie kompiuterin s informacijos perdavimo sistemos, perimant abonento kreipimosi tinkl valdym , metodu ir pan.

Ketvirtajai grupei priskiriami kompiuterini nusikaltim vykdymo b dai, susij su einan i ir išeinan i duomen bei kompiuterin s technikos valdymo komand manipuliavimo metod panaudojimu. Šie metodai naudojami labai dažnai ir gerai žinomi ekonomini nusikaltim tyrimo tarnyb pareig nams, pavyzdžiui, buhalterin s apskaitos einan i ir išeinan i duomen pakeitimas automatizuoto dokument apdorojimo proceso metu arba ty inis programos pakeitimas, kuris s lygoja nesankcionuot informacijos sunaikinim , blokavim , modifikavim arba kopijavim , taip pat kompiuteri , j sistemos ar tinklo darbo sutrikdymas (naudojami populiarieji b dai „Trojos arklys“, „Saliami“, „Aitvaras“, „Laiko bomba“ ar „Login bomba“, „Liukas“, kompiuteriniai virusai ir pan.).

Penktajai grupei priklauso kompleksiniai kompiuterini nusikaltim vykdymo b dai, kai nusikalt lis panaudoja kelis skirting grupi b dus, iš kuri vienas visada b naudojamas kaip pagrindinis, o kiti vykdo pagalbines funkcijas, pavyzdžiui naudojami nusikaltimo p dsakams nusl pti.

J.M.Baturinas skiria tris pagrindines kompiuterini nusikaltim vykdymo b d grupes: per mimo, neteis tos prieigos ir manipuliacij <sup>31</sup>. Reikia pasteb ti, jog daugelio Rusijos ir kit Europos šali specialist nuomon d l tokio kompiuterini nusikaltim vykdymo b d klasifikavimo iš esm s sutampa, ta iau nurodoma ir ketvirtoji – kompleksini metod grup . vertinus kompiuterini nusikaltim vykdymo b d ypatumus, autor s manymu, ši j klasifikacija pagal metodus yra optimaliausia:

1. per mimo metodai;
2. neteis tos prieigos metodai;
3. manipuliacij metodai;
4. kompleksiniai metodai.

### **1. Per mimo metodai:**

1) tiesioginis per mimas – kai prisijungimas vykdomas tiesiogiai prie ryšio kanal ar prie duomen perdavimo rangos mazg (per mimo objektu gali b ti kabelin s ar laidin s sistemos, radijo ar palydovinio ryšio sistemos);

---

<sup>31</sup>

.- oc , 1991. C .22.

2) elektromagnetinis per mimas – vykdomas per rangos šalutinį spinduliavimą (vaizduoklio, spausdintuvo, ryšio sistemą), be to, pakankamai dideliu atstumu nuo spinduliuojančio objekto.

Netiesioginio (nuotolinio) per mimos metodams priskirtini ir audio per mimas (informacijos nuskaitymas per vibroakustinį kanalą) bei video per mimas (informacijos gavimas panaudojant videooptinį rangą).

E. Melik priskiria šiai grupei ir „šiukšlių surinkimo“ metodą<sup>32</sup>, t.y. informacinio proceso atliekų, kurios gali būti fizinio pobūdžio (popierius, skaitos, kitos šiukšlės) ir elektroninio pobūdžio (duomenų paieška ir atstatymas), rinkimą.

## 2. Netiesiogiosios prieigos metodai

Šiai grupei priskiriami nusikaltėlių veiksmai, siekiant netiesiogiai prieiti prie kompiuterio ir jame saugomos informacijos ar kitų išteklių. Šie metodai turi savo specialius pavadinimus, žinomus viso pasaulio kompiuterinių technologijų specialistams:

“Sekimas paskui kvailį” (*pigbacking*) – tai netiesioginis patekimas uždaras zonas, sekant paskui teisėtą vartotoją arba kartu su juo.

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

“Silaužimas” (*hacking*) – šis metodas paprastai naudojamas siskverbimui svetimas informacinės sistemos, naudojantis specialia programine ranga, parenkant identifikuojančius teisėto vartotojo požymius (paprastai slaptažodžius ir vardus).

“Laisvas parinkimas (laisva atranka)” (*browsing*) – tai prisijungimas prie kompiuterio vienkartinę apsilankius apsaugos sistemos vietas ar trukumus bei vėliau jais naudojantis pagal poreikį.

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

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

“Maskaradas (apsišaukimas)” (*masquerading*) – tai siskverbimas kompiuterinėse sistemose, apsimetant teisėtu vartotoju, sužinojus jo kodą ar slaptažodį, jei nėra galimybių papildomai identifikuoti asmenį.

“Mistifikacija” (*spoofing*) – šis metodas techniškai pakankamai sudėtingas, kai

<sup>32</sup>

prisijungimo laikas: 2006-06-08.

// <http://www.melik.narod.ru>;

pažeid jas, formuodamas teisingas užklausas ir atsakymus, imituoja serverio darbą, sukurdamas vartotojui prisijungimo prie sistemos spūdį, taip jį suklaidindamas ir gaudamas dominančią informaciją, pvz., vartotojo kodus.

„Avarin programa“ – šis metodas remiasi ta aplinkybe, kad paprastai apsaugos sistemas diegiamos specialios programos, kurios naudojamos ypatingais atvejais, jei sutrinka sistemos darbas, ir skirtos greitai apeiti apsaugą. Turėdamos toki programinius priemonius, pažeid jas gali prieiti prie visų kompiuterinio tinklo išteklių.

„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. Manipuliacij metodai**

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

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

Kodo pakeitimas – tai informacijos vedimo, 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.

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

„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. Tai vizualiai užmaskuotas būdas, nes „Trojos arklio“ programai rašoma šalia kitos programos arba vedama jos viduryje ir tik tuomet pagrindinė programa atlieka vienokio arba kitokio pobūdžio pakeitimus. Literaturoje minimos dvi „Trojos arklio“ atmainos: 1) „Trojos kirminas“ – tai programinis modulis, kai programos darbo algoritmas, be pagrindinių funkcijų, vedama veiksmų algoritmo funkcija, kuri atlieka automatiškai „Trojos arklio“ atsinaujinimą, o tinkle tokios programos save automatiškai kopijuoja kitus kompiuterius; 2) „Trojos matrioška“ – tai ypač sunkiai aptinkamas programinis modulis, kuris sukuria „Trojos arklio“ ir baigęs užduotį pats susinaikina programiniu lygiu.

„Trojos arklio“ būdo loginė modifikacija yra kompiuteriniai virusai. Kompiuteriniu

virusu vadinama speciali programa, kuri sugeba savarankiškai prisijungti prie kit program (užkr sti jas) ir jas paleidžiant vykdyti vairius neplanuotus, nepageidaujamus veiksmus: trinti duomenis ir informacij , gadinti failus ir katalogus, perpildyti kompiuterio atmint , sutrikdyti jo darb . Dažniausiai užkre iamos \*.com, \*.exe, \*.bat, \*.sys, \*.do\*, \*.xl\* tipo bylos. Virusai, kurie skai iuojami t kstan iais, skirstomi kelias grupes: standartiniai *COM-EXE-TSR* virusai, Stels (*Stealth*) virusai, polimorfiniai (*polymorphic*) virusai, „kompiuteriniai kirminai“ (*worm*), makrovirusai ir kt.

Saliami ataka (*salami attack*) – buhalterin ms operacijoms takoti naudojama Trojos arklio taktika, pagr sta aritmetini sum apvalinimu (kitaip tariant, s skait apvalinimo metu gaut liekan pasisavinimas).

Login bomba (*logic bomb*) – slaptas komand rinkinio terpimas program , kuris turi prad ti veikti tam tikromis s lygomis.

Laiko bomba (*time bomb*) – login s bombos atmaina, kurios veikimo s lyga yra tam tikras laiko momentas ar laiko intervalas.

Asinchronin ataka – tai labai sud tingas programinis metodas, kur gali sudaryti dviej ar keli vartotoj , kuri komandas sistema apdoroja vienu metu, komand sukeitimas ar kitoks operacin s sistemos veiklos sutrikdymas, pažeidžiantis ar apsunkinantis informacijos apdorojimo procesus.

#### **4. Kompleksiniai metodai**

Šiai grupei priskiriami nusikalt li veiksmai, kuriais siekiama neteis tai prieiti prie kompiuterio, j tinklo ir saugom ištekli , perimti informacij bei manipuliuojama duomenimis arba kompiuterio komandomis, t.y. nusikalstamiems tikslams pasiekti kompleksiskai naudojami keli skirting grupi b dai. Optimaliausias konkre iomis aplinkyb mis nusikaltimo b das pasirenkamas ir naudojamas kaip pagrindinis, o kiti naudojami pagalbin ms funkcijoms vykdyti, paprastai nusikaltimui maskuoti, p dsakams nusl pti.

Apibendrinant galima konstatuoti, kad praktiskai ne manoma pateikti vis kompiuterini nusikaltim vykdymo b d išsamaus s rašo, nes j turinys gali b ti sudarytas iš vairiausi veism derini , priklausan i nuo pažeid jo išradingumo, kvalifikacijos ir intelekto. Dažniausiai minimi šie veiksmai: kenk jišk kompiuterini program ar kaupikli su tokiomis programomis naudojimas arba platinimas; kompiuterin s informacijos per mimas; neteis ta prieiga prie kompiuterin s informacijos; manipuliacija duomenimis ar valdan iomis programomis; kompiuterin s technikos, ryši rangos, kompiuterin s informacijos apsaugos, konfidencialios kompiuterin s informacijos apdorojimo, saugojimo ir perdavimo priemoni eksploatavimo taisykli

pažeidimas; kompiuterinis informacijos blokavimas, modifikavimas, kopijavimas, sunaikinimas, panaudojant specialiai sukurtas, pritaikytas, užprogramuotas technines priemones ir kt. Tačiau, nepaisant kompiuterinio nusikaltimo vykdymo būdų vaizdų, juos galima sugrupuoti pagal metodus keturias grupes: 1) per mimos; 2) neteisėtos prieigos; 3) manipuliaciją; 4) kompleksinius.

Galima tik apgailestauti, kad Lietuvos Respublikos vidaus reikalų ministerijos Nusikalstamų veikų žinybiniame registre nėra kaupiami detalūs duomenys apie nusikalstamų veikų, kurių pasikėsinimo dalykas - kompiuterinė informacija ir sistemos, o priemonė - kompiuterinė technika ar internetas, vykdymo būdus, nes nusikalstamos veikos statistinė kortelė (10 kortelių) tokio pobūdžio veikos pagal padarymo būdą skirstomos tik dvi apibendrintos grupės: „panaudojant kompiuterinį rangą“ (20 proc.) ir „pasinaudojant netikra mokymų kortele“ (80 proc.) (žr. 4 priedo 4 lentelę), be to, atlikus minėto registro duomenų analizę, paaiškėjo, jog tyrėjai, pildydami statistines korteles, fabuloje taip pat nenurodo tiksli nusikalstamų veikų padarymo būdą ar metodą.

Siekiant gauti praktinius duomenis apie kompiuterinio nusikaltimo vykdymo būdus, buvo atlikta Lietuvos kriminalinės policijos biuro Nusikaltimų tyrimo vyriausiosios valdybos Nusikaltimų elektroninėje erdvėje tyrimo skyriaus (NEETS) pareigūnų apklausa, pateikiant elektroninį klausimyną (žr. 5 priedas). Apibendrinus NEETS pareigūnų atsakymus, darytina išvada, jog Lietuvoje dažniausiai naudojami šie kompiuterinio nusikaltimo vykdymo būdai: 1) tiesioginis per mimas, priklausantis per mimos metodų grupei; 2) silaužimas (hacking), priklausantis neteisėtos prieigos metodų grupei; 3) „Trojos arklys“ ir kompiuteriniai virusai, priklausantys manipuliacijų metodų grupei.

#### 4.4. KOMPIUTERINI NUSIKALTIM PRIETAISAI IR PRIEMON S

Universaliausia ir plaiausiai naudojama kompiuterini nusikaltim vykdymo priemon , žinoma, yra asmeninis kompiuteris, kuriame diegta speciali programin ranga ir atitinkami išoriniai renginiai. Tačiau rengiant, vykdant ir nuslepiant tokio pob džio nusikalstamas veikas, naudojami vairiausi prietaisai bei priemon s, kurie kriminalistikos metodiniuose leidiniuose paprastai suskirstomi dvi apibendrintas grupes: bendruosius techninius ir specialiuosius kompiuterinius.

##### 1. Bendrieji techniniai prietaisai ir priemon s

Bendrieji techniniai prietaisai ir priemon s naudojami kompiuterio, kompiuteri tinklo ar informacin s sistemos veiklai sutrikdyti ir informacijai gauti, pakeisti, sunaikinti ar blokuoti. Šie prietaisai ir priemon s gali b ti standartiniai, legaliai sigyti ir pritaikomi kompiuteriniams nusikaltimams vykdyti arba savadarbiai, specialiai modifikuoti, užprogramuoti.

Bendr j technini prietais ir priemoni grupei priskiriami:

vair s montavimo rankiai, elektros montavimo instrumentai ir medžiagos;

vairios magnetin s medžiagos ir technin s priemon s, sukurian ios kryptin magnetin lauk ;

elektromagnetinio spinduliavimo registravimo renginiai;

garso ir vaizdo rašymo ranga;

pasiklausymo ranga;

kontroliniai matavimo prietaisai ir renginiai;

ryši sistem priemon s ir j komponentai.

##### 2. Specialieji kompiuteriniai prietaisai ir priemon s

2.1. Technin ranga – tai patys kompiuteriai ir kita kompiuterin technika (taip pat ir ranga, kuri n ra kompiuterin bendr j prasme, pvz., perprogramuojama mikroschema PIC), išoriniai renginiai.

2.2. Programin ranga – tai ir standartin , laisvai platinama ranga (kurios poveikio rezultatai yra lengvai prognozuojami bei analizuojami) ir specialios programin s priemon s (kuri poveik tirti žymiai sud tingiau) – komand arba mnemokod sistema, valdanti informacinius procesus, kurios pagalba vykdomos vairios manipuliacijos su kompiuterine informacija.

Speciali j kompiuterini prietais ir priemoni grupei priskiriama:

vairios elektronin s skai iavimo technikos r šys (asmeniniai kompiuteriai, kompiuteri tinklo ar telekomunikacinio tinklo darbo ir tarnybin s stotys (serveriai), judriojo



(mobilaus) ryšio renginiai, turintys duomen perdavimo internetu funkciją, bankomatai, kasos aparatai, turintys fiskalinės atminties bloką, elektroninės užraš knygučių ir kt.);

išoriniai renginiai (vaizdo kontrolės renginiai (displėjus, monitorius), valdymo renginiai (klaviatūra, manipulatoriai – pelė, specialus pieštukas, sensorinis ekranas), spausdinimo renginiai (rašaliniai, lazeriniai spausdintuvai), informacijos video vedimo renginiai (skeneris, skaitmeninė foto ar video kamera) bei grafinio vedimo renginiai (planšetas, didžitaizeris), plastikiniai kortelių nuskaitymo renginiai (optiniai, magnetiniai, elektromagnetiniai) ir kt.;

kompiuterinės informacijos perdavimo ir priėmimo ranga (vidiniai ar išoriniai modemai, kita telekomunikacinė ranga);

duomenų perdavimo tinklo techninė ranga (sujungimo kabeliai, jungtys, nuoseklūs prievadai (portai), maitinimo renginiai, techninė kompiuterinės informacijos apsaugos nuo nesankcionuotos prieigos ranga ir kt.);

kenkėjiškos kompiuterinės programos (kompiuteriniai virusai, „Trojos arklys“ ir kitos), kompiuterinės informacijos apsaugos sistemos veikimo programos (apsaugos kodų veikimo (nulaužimo) programa, prieigos kodų generatorius, kriptografinė apsaugos dešifravimo ranga ir kt.).

Lietuvos Respublikos vidaus reikalų ministerijos Nusikalstam veik žinybiniame registre nėra kaupiami detalūs duomenys apie nusikalstam veikas, kurių pasikėsinimo dalykas – kompiuterinė informacija ir sistemos, padarymo prietaisus ir priemones. Nusikalstamos veikos statistinėje kortelėje (10 kortelė) tokio pobūdžio veikų priemonės, vadinamos informatikos priemonėmis, skirstomos tik tris apibendrintas grupes: kompiuterinė technika (74), internetas (75), netikra mokėjimo kortelė (76), nedetalizuojant, kokie tiksliai kompiuteriniai prietaisai ir priemonės buvo panaudoti konkrečiai nusikalstamai veikai vykdyti ar nuslėpti (žr. 4 priedo 5 lentelė). Nuo 2003 m. gegužės 1 d. iki 2006 m. rugsėjo 1 d. buvo užregistruota 573 nusikalstamos veikos, kurių padarymo priemonė – kompiuterinė technika, 111 nusikalstam veikų, kurių padarymo priemonė – internetas, ir 584 nusikalstamos veikos, kurių padarymo priemonė – netikra mokėjimo kortelė.

### III. KOMPIUTERINI NUSIKALTIM TYRIMO METODIKOS YPATUMAI

#### 5. KOMPIUTERINI NUSIKALTIM TYRIMO VEIKSMAI

##### 5.1. RODIN TINOS APLINKYB S

Tiriant kompiuterin nusikaltim , tyr jui b tina išsiaiškinti, kokios aplinkyb s rodin tinos šiuo konkre iu atveju, nes kaip tik tai leis tinkamai suformuluoti tyrimo užduotis. Žinoma, kad patraukti baudžiamojon atsakomyb n asmen galima tik tuomet, kai nustatoma, jog konkre ti jo veika atitinka baudžiamojo kodekso straipsnio nustatyt abstrak i nusikaltimo sud t , ta iau kompiuterinio nusikaltimo atveju tyr jui b tinos ne tik baudžiamosios teis s materialin s ir procesin s žinios, kriminalistikos žinios, bet ir specialios informacini technologij žinios.

Daugelyje kriminalistikos metodikos darb pateikiamas toks apibendrintas rodin tin aplinkybi s rašas: nusikaltimo sud ties elementai; kvalifikuojan ios aplinkyb s, sunkinan ios ir lengvinan ios atsakomyb aplinkyb s bei šalinan ios baudžiam j atsakomyb aplinkyb s. V.B.Vechovas bei kiti mokslininkai, apibendrindami nusikaltim , susijusi su kompiuterini technologij panaudojimu, tyrimo praktik , si lo detalizuoti rodin tin aplinkybi s raš , atsižvelgiant šios r šies nusikaltim specifik <sup>33</sup>.

vertinus kompiuterini nusikaltim ypatybes, galima nurodyti šias pagrindines aplinkybes, kurios tur t b ti nustatytos ir rodytos kompiuterini nusikaltim bylose:

1. nusikaltimo vykdymo faktas ir tiesiogin kompiuterin s informacijos bei jos apdoravimo priemoni saugumo pažeidimo priežastis (t.y., ar veika yra nusikaltimas, ar kitos r šies teis s pažeidimas, ar nelaimingas atsitikimas – nenugalimos j gos aplinkybi (*forse majore*) pasekm , pvz., oro s lyg , gamtos katastrof , vidini technini gedim ar sutrikim );

2. nusikalstamo pasik sinimo objektas ir dalykas (tai turi lemiam reikšm tyr jui pasirenkant vienoki ar kitoki nusikaltimo tyrimo metodik ); kompiuterin s informacijos kategorija (vieša, bendro naudojimo ar nevieša, slaptinta);

3. nusikaltimo vykdymo b das (ar nusikaltimas vykdytas tiesioginiu, ar nuotoliniu b du; jei nuotoliniu b du,- ar naudojant vietin (lokal ) kompiuteri tinkl ar internet , ar kitus telekomunikacinius kanalus, ir kt.);

4. nusikaltimo vykdymo vieta (konkre ti tos mon s, staigos, organizacijos, kito objekto, teritorijos dalies vieta, kur vykdytas nusikaltimas);

5. nukent j s asmuo (fizinis ar juridinis asmuo); objekto, kuriame vykdytas nusikaltimas, pavadinimas, paskirtis, darbo režimas;

6. nusikaltimo vykdymo priemon s (bendrosios technin s rangos ar kompiuterin s

<sup>33</sup>

, 1998. C .24.

techninis ir programinis rangos tipas, rėšis, modelis, funkcini paskirtis, techninis bkl ir kitos charakteristikos; konkretaus terminalo ar tinklo srities registracijos, abonentinis numeris, kodas, šifras, darbo dažnis);

7. kompiuteri tinklo ar informacin s sistemos darbo režimas (darbo su kompiuterine informacija, jos apdorojimo ir apsaugos priemon mis tvarka);

8. nusikaltimo vykdymo laikas (laikotarpis).

9. žalos dydis ir jos sud tis.

10. tarnybin s funkcijos, veiksmai ir technologinio proceso operacijos, su kuriais susij s nusikaltimas;

11. asmen , atsaking ir tiesiogiai susijusi su gamybos technologija, informacijos apdorojimu, naudojimu ar administraciniu valdymu, s rašas;

12. nusikaltimo subjektas ( tariamojo asmenyb s charakteristika, ar turi praktini geb jim ir specialii žini , kokios srities ir kokio lygio žinios b tinos nusikaltimui vykdyti); jei nusikaltim vykdo grup asmen , jos sud tis ir kiekvieno nario vaidmuo;

13. nusikaltimo motyvai ir tikslai (naudos siekimas, kerštas, chuliganiškos paskatos, asmenini intelekto galimybi demonstravimas, kito nusikaltimo nusl pimas ir kt.);

14. priežastinio ryšio buvimas tarp veikos ir atsiradusi pasekmi (b tina rodyti, kad konkretaus tariamo asmens veiksmai, kurie jam inkriminuojami, buvo atsiradusi pasekmi priežastimi);

15. priežastys ir s lygos, paskatinusios vykdyti ir nusl pti nusikaltim (normini teis s akt , instrukcij , taisykli , darbo tvarkos reglamentavimo tr kumai ir pažeidimai, vykdyti tre i j asmen , kuri b tent ir d l koki priežas i , ar šie asmenys neturi b ti patraukti baudžiamojon atsakomyb n už pažeidimus, kurie sudar s lygas vykdyti tiriam nusikaltim );

16. kam buvo žinomi nusikalt li ketinimai;

17. kas dalyvavo nuslepiant nusikaltim ar jo p dsakus.

## 5.2. TIPINIS TYRIMO SITUACIJOS IR KRIMINALISTINIS TYRIMO UŽDUOTYS

Kompiuteriniams nusikaltimams būdingas ypač didelis latentškumas (manoma, jog jis gali siekti iki 90 proc.). Asmenys, rengiantys kompiuterinį nusikaltimą, paprastai labai tiksliai ir detalčiai planuoja savo veiksmus, iš anksto numato pdsakslpimo būdus, panaudoja varias nusikalstamos veikos maskavimo priemones, pasitelkdami subjektyvius ir objektyvius faktorius, (pavyzdžiui, prastus kompiuterinio darbo sutrikimus, ryšio, maitinimo rangos gedimus, trumpuosius jungimus kabelių sistemose ir kt.), todėl ypač sudėtinga aptikti tokius nusikaltimus pasirengimo stadijoje bei rasti vykdytą nusikaltimą pdsakslpimus. Be to, nukentėjusis nuo kompiuterinio nusikaltimo asmuo dažnai nėra labai suinteresuotas nusikaltimo sulaikymu, o pats nusikaltėlis, jei būna sulaikomas, linkęs reklamuoti savo pasiekimus. Tai lemia šios priežastys: kompiuterinio nusikaltimo aukos dažniausiai mano, jog ši nusikaltimo padaryta žala yra mažesnė, nei nuostoliai, kuriuos gali sukelti jo atskleidimas (pvz., kredito staigios reputacijos praradimas), o patys kompiuteriniai nusikaltėliai, atskleidusį nusikaltimą, tampa žymūs tiek nusikalstamo, tiek legalaus verslo sferose (pasaulio praktikoje žinomas ne vienas atvejis, kai kompiuteriniams silaužliams pasiūlydavo darbą informacinių technologijų saugos sistemose).

Taigi, kompiuterinius nusikaltimus tiriantys pareigūnai susiduria su vairiomis kliūtimis: pirma, ypač kruopščiai parengtais intelektualiais nusikaltimais, antra, netipišku nukentėjusio ir nusikaltėlio elgesiu. Vadinasi, aptikti šiuos nusikaltimus pdsakslpimus sudėtinga, o nusikaltimo tyrimas km priklauso nuo to, kiek ir kokios informacijos surenka tyrėjai. Svarbu tai, kad profesionaliai ir operatyviai atliktas tyrimas, tinkamai panaudotos specialiosios informacinių technologijų žinios bei programinė ranga padeda rasti nusikaltimo pdsakslpimus kompiuteryje ir jo tinkle bei nustatyti nusikaltimo veiksmų seką.

Pirminis tyrimas, operatyvinių veiksmų visuma, jo atlikimo nuoseklumas priklauso nuo konkrečios tyrimo situacijos. Tyrimo situaciją lygoja tyrimo turima pradinė kriminalistinių požymių svarbi informacija. Ikitiesminis tyrimas paprastai pradedamas šiais atvejais: gavus fizinių ar juridinių asmenų pareiškimus, pranešimus; tyrėjui, prokurorui gavus duomenis, surinktus vykdant operatyvinius paieškos veiksmus, arba tiesiogiai aptikus nusikaltimo požymius; paskelbus atitinkamą informaciją spaudoje, kitose masinėse informacijos priemonėse, taip pat ir Internete. Paprastai prieš pradėdant tyrimą yra atliekamas pirminis medžiagos, gautos teisėsaugos institucijų, patikrinimas, tyrėjai gali iš anksto susipažinti su surinkta medžiaga, kartu su operatyviniu darbuotoju pasirinkti taktinius požymių tinkamiausius tyrimo metodus, nustatyti pirminio tyrimo veiksmų, organizacinių ir kitų priemonių pobūdį ir vykdymo nuoseklumą. Kompiuterinio nusikaltimo tyrimas km dažnai lemia tyrimo veiksmų operatyvumas ir glaudus bendradarbiavimas su kompiuterinių technologijų srities specialistu.

Vykdyt pirmin medžiagos patikrinim , tyr jas turi gauti kuo tikslesnius duomenis apie pasik sinimo objekt , jo buvimo viet ir fizin s apsaugos s lygas, veiklos pob d , gamybos, valdymo, dokument administravimo proces technologinius ypatumus, apskaitos ir atskaitingumo tvark , naudojamos kompiuterin s technikos charakteristikas, informacijos apsaugos organizavimo principus. Be to, b tina žinoti s raš ir tarnybines pareigas t asmen , kurie turi tiesiogin ar netiesiogin prieig prie kompiuterin s informacijos, jos apdorojimo priemoni , tapusi nusikalstamo pasik sinimo objektu.

Galima pamin ti šiuos tipinius pasirengimo vykdyti kompiuterin nusikaltim , jo vykdymo ar nusl pimo požymius: suklastot ar neatitinkan i duomen aptikimas kompiuteryje, j tinkle ar informacin je sistemoje, dažni rangos darbo sutrikimai, nesankcionuotas fail sistemos strukt ros, kompiuterio programin s ar technin s rangos, sistemos ar tinklo konfig racijos pakeitimas, vartotoj nusiskundimai d l sutrikusios prieigos prie kompiuterio, tinklo ar kompiuterin s informacijos, nereglamentuotos prieigos prie kompiuterio, tinklo ar atskir vartotoj kompiuterin s informacijos užfiksavimas, darbo su kompiuterine informacija taisykli pažeidimas, padid j s kai kuri darbuotoj ar kit asmen d mesys saugomai kompiuterinei informacijai, tartinas konkretaus vartotojo kreipimasis tam tikros kategorijos duomenis ar kompiuterin informacij , atskir duomen kopijavimo atvejai be rimt priežas i , išorini asmenini informacijos kaupikli naudojimas vairiais motyvais darbo vietoje, konfidencialios informacijos atskleidimo atvejai arba slapto jos gavimo priemoni aptikimas, nustatyt darbo su kompiuteriu, tinklu ar kompiuterine informacija taisykli pažeidimai.

Siekiant tiksliai išsiaiškinti nukent jusiojo (fizinio ar juridinio asmens) veiklos ypatumus, tyr jui reikia išanalizuoti žinybinius norminius teis s aktus, susipažinti su informaciniais dokumentais. Svarbu pabr žti, kad pradedant kompiuterinio nusikaltimo tyrim , b tina pasitelkti specialistus, turin ius profesionali žini ir patirties kompiuterin s informacijos apdorojimo bei apsaugos srityje.

Kriminalistikos mokslo darbuose skiriamos kelios tipin s kompiuterini nusikaltim tyrimo situacijos. Atsižvelgiant duomen apie vykdyt nusikaltim gavimo šaltin , skiriami šie atvejai: nukent j s asmuo savarankiškai aptinka kompiuterin nusikaltim , numano, kas yra kaltininkas, ir praneša tai teis saugos staigai; nukent j s asmuo savarankiškai aptinka kompiuterin nusikaltim , ta iau nežino kaltininko ir praneša tai teis saugos staigai; vykdyto kompiuterinio nusikaltimo duomenys paaišk ja iš kit šaltini (dažniausiai teis saugos pareig nams tiriant kit nusikaltim ).

Tiriant ekonominius nusikaltimus, vykdytus panaudojant kompiuterin rang , (suk iavim , turtin s žalos padarym apgaule arba piktnaudžiaujant pasitik jimu) skiriamos šios

tipin s tyrimo situacijos<sup>34</sup>: tariamasis sulaikytas nusikaltimo vietoje su kaliais; tariamojo asmenyb nenustatyta, taiau žinomas jo nusikaltimo padarymo b d as ir vieta (panaudojus atokius nusikaltimo padarymo b dus); žinomi tik nusikaltimo padariniai.

Apibendrinant kriminalistikos teorijos bei praktikos darbuose nurodomas kompiuterini nusikaltim tipines tyrimo situacijas ir atsižvelgiant turim duomen apie nusikaltim ir tariam j išsamum , galima išskirti tris pagrindines situacijas:

1) n ra duomen apie nusikaltimo vykdymo b d ir tariamojo asmenyb , žinomos tik pasekm s, nukent jusysis;

2) yra duomen apie nusikaltimo vykdymo b d , bet n ra duomen apie tariamojo asmenyb ;

3) yra duomen apie nusikaltimo vykdymo b d , tariamojo asmenyb ir kitas aplinkybes;

4) tariamasis sulaikytas nusikaltimo vietoje su kaliais.

Atsižvelgiant ši situacij pob d , parenkami ir atliekami atitinkami tyrimo veiksmai: vykio vietos ir kompiuterin s rangos apži ra; dokument , kompiuterin s rangos ar kompiuterin s informacijos laikmen po mis arba krata siekiant juos surasti; asmens sulaikymas; tariamojo apklausa; kompiuterin s ir kitos rangos ekspertiz bei kiti veiksmai.

Pirmojoje ir antrojoje situacijoje, kai n ra duomen apie tariam j , paprastai imamasi ši operatyvin s paieškos, organizacin i ir kit priemoni bei atliekami šie tyrimo veiksmai:

1) nukent jusiojo apklausa;

2) vykio vietos apži ra, dalyvaujant pakviestiems specialistams;

3) operatyvini paieškos priemoni organizavimas, siekiant nustatyti nusikaltimo vykdymo priežastis, tariamuosius, aptikti nusikaltimo p dsakus, daiktinius rodymus;

4) kompiuterin s ir kitos rangos, kompiuterin s informacijos, jos laikmen , dokument apži ra, pirminis tyrimas ir po mis, dalyvaujant pakviestiems specialistams;

5) liudytoj apklausa;

6) tariam asmen , vykdan i konkre ias funkcijas, informacijos apdorojimo procesus, susijusius su nusikaltimu, ar atsaking už informacijos apsaug , apklausa;

7) tariam j darbo vietos ir gyvenamosios vietos krata;

8) ekspertizi skyrimas (kompiuterin s technin s ir programin s rangos, kompiuterin s spausdinimo rangos, radiotechnin s, technin s, buhalterin s ir kit ).

Tre iojoje situacijoje, kai yra duomen apie nusikaltimo vykdymo ir nusl pimo b dus, tariamojo asmenyb ir kitas aplinkybes, tyr jas, atlik s pirmin gautos medžiagos analiz ,

---

<sup>34</sup> Burda R. Kompiuterin s rangos panaudojimas ekonominiams nusikaltimams (kai kurie kriminalistin s charakteristikos ir tyrimo metodikos ypatumai) // Jurisprudencija, 1999. T.12(4). P.71.

( vertinant jos išsamumą , baudžiamojo proceso normų vykdymą ir perdavimo ikiteisminio tyrimo staigoms tvarką ), imasi šie veiksmai :

- 1) operatyvini paieškos priemoni ir tariamojo sulaikymo su kalbais organizavimas;
- 2) sulaikytojo krata;
- 3) sulaikyto asmens apklausa;
- 4) sulaikytojo darbo vietos ir gyvenamosios vietos krata;
- 5) vykių vietos apžiūra, dalyvaujant pakviestiems specialistams;
- 6) liudytojų apklausa, ryšiai tarp sulaikytojo ir asmenų, susijusių su vykdytu nusikaltimu, nustatymas;
- 7) nukentėjusiojo apklausa;
- 8) tariamąjį apklausa;
- 9) kompiuterinės ir kitos rangos, kompiuterinės informacijos, jos laikmenys, dokumentų apžiūra, pirminis tyrimas ir požiūris, dalyvaujant pakviestiems specialistams;
- 10) dokumentų, patvirtinančių tariamojo tapatybę ir specialią žiniatūrą, taip pat dokumentų (vis formų ir laikmenų), charakterizuojančių gamybines ar informacijos apdorojimo operacijas, kurių metu buvo vykdyti pažeidimai ir nusikalstami veiksmai, požiūris ir apžiūra;
- 11) asmenų, paminėtų tyrimams perduotuose dokumentuose kaip padariusių pažeidimus ar atsakingų už konkrečią darbo sritį pagal nustatytus pažeidimų faktus, apklausa;
- 12) asmenų, susijusių su atitinkamomis gamybinėmis ar informacijos apdorojimo operacijomis ar tariamais ryšiais su nusikaltėliu, apklausa;
- 13) ekspertizės skyrimas (kompiuterinės techninės ir programinės rangos, kompiuterinės spausdinimo rangos, radiotechninės, techninės, buhalterinės ir kitos).

Ketvirtojoje tyrimo situacijoje, kai tariamasis sulaikytas nusikaltimo vietoje su kalbais, atliekami šie tyrimo veiksmai:

- 1) sulaikytojo krata;
- 2) sulaikyto asmens apklausa;
- 3) sulaikytojo darbo vietos ir gyvenamosios vietos krata;
- 4) vykių vietos apžiūra, dalyvaujant pakviestiems specialistams;
- 5) kiti veiksmai, kaip ir trečiojoje situacijoje.

Nurodyti tyrimo, operatyvini ir organizaciniai veiksmai bei priemonės nuoseklumas gali būti keičiamas, atsižvelgiant į situacijos pasikeitimus. Visose tyrimo situacijose rekomenduojama atlikti žinybini norminių teisės aktų, informacinių dokumentų, kompiuterinės rangos eksploatavimo taisyklių ir darbo su kompiuterine informacija tvarkos analizę, organizuoti konsultacijas su atitinkamais specialistais; išreikalauti dominančio laikotarpio kontrolini

patikrinim , inventorizacij ir revizij medžiag (informacijos apdorojimo taisykli laikymosi, neviešos ar slaptintos informacijos apsaugos, elektronini dokument apyvartos, vertybi apskaitos ir kt.) ir atlikti jos analiz ; gauti b tin informacij iš kontroliuojan i , inspektuojan i ir licencijuojan i staig (mokes i inspekcijos ir kt.).

Kompiuterini nusikaltim tyrimo užduotis yra surinkti ir užfiksuoti šiuos duomenis:

- a) baudžiamojo statymo numatytos veikos požymius;
- b) šia veika padarytos žalos pob d ir dyd ;
- c) priežastin ryš tarp veikos ir jos pasekmi , nustatant kaltininko veiksm pob d , nusikaltimo padarymo b d ;
- d) kaltininko ty i .

Apibendrinant tai, kas išd styta, galima konstatuoti, kad tipin se kompiuterini nusikaltim tyrimo situacijose pagrindiniai pirminiai tyrimo veiksmai yra šie: vykio vietos apži ra, kompiuterin s rangos apži ra (paties kompiuterio ir kit rengini ), liudytoj apklausa, nukent jusiojo apklausa, dokument po mis (pirmiausia, elektronini dokument , fiksuojan i svarbius tyrimui duomenis – tariamojo prisijungimo prie sistemos laik ir b d (tai vadinamieji „log failai“).

Jei tariamasis nesulaikytas, greta min t pirmini tyrimo veiksm , b tina organizuoti jo paiešk , taip pat, pasitelkus nukent jus asmen ir specialistus, nustatyti nusikaltimo padarymo b do ypatybes.

Jei asmuo sulaikytas nusikaltimo vietoje arba iš karto po nusikaltimo padarymo, atliekami šie pirminiai tyrimo veiksmai: sulaikyto asmens krata; sulaikyto asmens apklausa; sulaikyto asmens darbo ir gyvenamosios vietos krata.



### 5.3. ATSKIR TYRIMO VEIKSM ATLIKIMO YPATUMAI

vertinus kompiuterini nusikaltim specifines ypatybes (latentiškum , k sinimosi objekto nematerialum , s lygin sl pimo paprastum ), reikia pabr žti apži ros, kratos ir po mio svarb s kmingam ši nusikaltim tyrimui.

Kriminalistikos teorijos darbuose apži ra apibr žiama kaip procesinis tyrimo veiksmas, kurio metu statymo nustatyta tvarka tyr jas savo jutiminius organais ir nesud tingais instrumentiniais metodais observuoja, analizuoja, fiksuoja ir atlieka kitus veiksmus su objektais, susijusiais su tiriamu vykiu<sup>35</sup>. Pagrindinis apži ros tikslas – rasti, užfiksuoti, surinkti ir paimti informacij , jos laikmenas ir kaupiklius apie nusikalstamos veikos požymi turint vyk

Krata – tai toks procesinis prievartos tyrimo veiksmas, kurio metu prievarta apieškomos patalpos, vietov s ir kiti objektai, taip pat asmenys, turint tiksl rasti ir paimti nusikalstamos veikos rankius, nusikalstamu b du gytus daiktus bei vertybes, nusikalstamos veikos p dsakus, dokumentus ir kitus daiktus, turin ius reikšm s bylos tyrimui<sup>36</sup>.

Vertingi rodymai gali b ti aptikti kre iant tariam j darbo, mokslo ir gyvenam sias vietas, tarnybinės patalpas, taip pat pa ius tariamuosius. Rengiantis atlikti krat , b tina atidžiai išnagrini ti bylos aplinkybes ir surinkti orientacin medžiag apie kratos objekt , jos vykdymo viet ir kre iam asmen . Kompiuterini nusikaltim bylose ieškoma ne tik vairi kompiuterini priemoni ,kaupikli ,laikmen ir juose esan ios kompiuterin s informacijos, bet ir dokument , ryšio priemoni , kit technini priemoni ir prietais (taip pat ir savadarbi ), buitini elektrotechnini rengini ir prietais , medžiag ir kt. Ypatingas d mesys skirtinas daiktams, kuriuose yra kodai, prieigos slaptažodžiai, identifikaciniai numeriai, elektroniniai konkre i kompiuterini sistem ir tinkl vartotoj adresai, sijungimo ir darbo sistemose ar tinkluose algoritmai, b tina atkreipti d mes užrašus, telefon knygetes, žinynus, katalogus (popierinius ir elektroninius, rašytus telefon aparat ir kit elektronini rengini atmint). Paprastai kompiuterini nusikaltim bylose svarbu rasti mokslinius bei informacinius leidinius, metodin medžiag apie informacines technologijas, kompiuterin s informacijos apdorojim , apsaug , perdavim ir gavim (tiek teis t , tiek neteis t ), garso ir vaizdo kasetes, spausdint kompiuterin informacij , taip pat ir tariamojo išsilavinim liudijan ius dokumentus.

Po mis – tai toks procesinis prievartos tyrimo veiksmas, kuris atliekamas tuomet, kai reikia paimti daiktus bei dokumentus, turin ius reikšm s bylai, kai žinoma j buvimo vieta, t.y., kur ir pas k jie yra<sup>37</sup>. Tiriant kompiuterini nusikaltim bylas, po mio objektai dažniausiai yra šie: asmeniniai kompiuteriai; informacijos kaupikliai ir laikmenos; vair s dokumentai (popieriniai ir

<sup>35</sup> Burda R., Krišk i nas R., Latauskien E.ir kt. Kriminalistikos taktika ir metodika.- Vilnius, 2004. P.23.

<sup>36</sup> Ten pat. P.55.

<sup>37</sup> Ten pat. P.55.

elektroniniai), aprašantys ar reglamentuojantys varias operacijas, technologinius procesus, susijusius su kompiuterinės informacijos apdorojimu, kaupimu, sukrimu, perdavimu ir apsauga, kompiuterinių tinklų ir informacinių sistemų funkcionavimu; specialios techninės priemonės, skirtos slaptam informacijos gavimui, modifikavimui ar sunaikinimui ir kt. Be to, atliekamas parašų pavyzdžių, dokumentų ir blankų fragmentų, informacijos kaupiklių ruošinių, programų išėjimo kodų, juodraščių ir kitų pavyzdžių po šiuos lyginamajam tyrimui atlikti.

Visi kompiuteriniai nusikaltimai bylų tyrimo veiksmai turi būti atliekami griežtai laikantis baudžiamojo proceso normų, nes nuo to priklausys gautų duomenų rodomoji vertė bylos teismo nagrinėjimo metu, be to, svarbu laikytis šių reikalavimų:

tyrimo veiksmai turi būti iš anksto parengti ir detalai suplanuoti;

tyrimo veiksams tinkamai atlikti turi būti iš anksto paruošta reikalinga ranga ir medžiagos;

atliekant tyrimo veiksmus, turi dalyvauti specialistai, tiksliai žinantys savo užduotis, teises ir pareigas; kviestiniai privalo turėti minimali specialią kompiuterinės informacijos apdorojimo srities žinią (asmeninio kompiuterio vartotojo lygiu), tyrėjai ir specialistai – būtinai žinią apie darbą su kompiuterine technine ir programine ranga (svarbiausia – kompiuterinės informacijos išsaugojimas, jos nepakeičiamas).

Atliekant apžvalgą, kratą ar poimimą, svarbu aptikti bei tinkamai surinkti tiek tradicinius, tiek netradicinius pėdsakus, kurie paprastai skirstomi dvi grupės<sup>38</sup>:

1. daiktinius pėdsakus, kuriems priskiriami tradiciniai kriminalistiniai pėdsakai – pirštų, rankų, biologiniai asmens pėdsakai, mikrodalelės ir kt. bei netradiciniai – elektroniniai kortelės, elektroniniai raktai, vartotojo identifikavimo ranga pagal biometrinius duomenis (pirštų pėdsakus, rankos geometrinius požymius, raštą, balsą);

2. intelektinius pėdsakus, kuriuos galima suskirstyti tris grupes:

2.1. kompiuteriniai rinkmenų struktūros pokyčiai (failų ar katalogų pavadinimų, dydžio ir turinio, standartinių rekvizitų pakeitimas, naujų failų ar katalogų atsiradimas);

2.2. anksčiau užprogramuotos kompiuterio ekrano spalvos, vaizdėlių, spausdintuvo ar kitos rangos tarpusavio suderinamumo pakitimai ir pan.;

2.3. neprastas kompiuterio darbas: suliktųjų operacinių sistemų, pelytų valdymo darbas, netikėti simboliai atsiradimas, prastų komandų nestandartinis vykdymas ir pan.

Konkrečiau kompiuterinio nusikaltimo pėdsakai gali būti labai varūs, jie priklauso nuo kompiuterinės techninės ir programinės rangos panaudojimo būdų bei nusikaltimo pobūdžio.

Atsižvelgiant tai, jog tiriant kompiuterinius nusikaltimus nepakanka profesinių

---

<sup>38</sup> Burda R. Kompiuterinės rangos panaudojimas ekonominiams nusikaltimams (kai kurie kriminalistinės charakteristikos ir tyrimo metodikos ypatumai) // Jurisprudencija, 1999. T.12(4). P.71.

teisinių žinių, visuose kriminalistikos metodologijos darbuose tyrėjui patariama esant galimybei pasitelkti informacinių technologijų specialistus atliekant bet kurį tyrimo veiksmą.

Vykiant kompiuterinės techninės bei programinėsrangos apžiūrą, kratos ar poimimą, svarbu elgtis ypač atidžiai, atsižvelgti kompiuterinės informacijos saugojimo, pildymo priemonių ir būdų ypatybes, numatyti kaltininko priešiškus veiksmus bei kitus faktorių poveikio informacijai galimybes.

Pasiruošiant vykio vietas apžiūrai ar kratai būtina laikytis šių taisyklių<sup>39</sup>:

- a) niekam neleisti liesti kompiuterinėsrangos;
- b) neišjunginti patalpose elektros;
- c) jei pastate elektra atjungta, būtina ištraukti iš kištukinių lizdų kompiuterinęrangą, kol ji visiškai bus jungta;
- d) tyrėjai neturi liesti kompiuterio klaviatūros, jungiklių, jei nežino šių veiksmų padarinių;
- e) jei patalpose kartu su kompiuterine ranga yra lengvai užsidegiantis medžiagas, sprogmenys ir pan., iki darbo su kompiuteriais pradžios būtina šias medžiagas izoliuoti;
- f) jei pavojingame medžiagose ne manoma atskirti nuo kompiuterinėsrangos, būtina evakuoti žmones.

Prieš pradėdant vykio vietas apžiūrą ar kratą, būtina imtis visų manomų apsaugos priemonių:

- a) nustatyti visose patalpose esančių žmonių asmenybes; tai ypač svarbu siekiant rasti kompiuterinėsrangos specialistus, kuriems tikrinama monitonorių (staigų) nura pagrindiniai darbovietai;
- b) atlikti visose patalpose esančių žmonių kratą; ieškant darbų su kompiuteriu liečiančių užrašų, neleisti jiems pasinaudoti nuotolinio valdymo renginiais, kuriais gali būti paveikti kompiuteriai;
- c) neleisti kratomiesiems pažeisti ar sunaikinti kompiuterinėsrangos, kitus renginius, diskus, disketes ir pan.;
- d) išsiaiškinti, ar yra kompiuterinėsrangos apsaugos sistema;
- e) nustatyti, ar yra informacijos sunaikinimo programa, kuria būtų galima nesankcionuotai pasinaudoti;
- f) nustatyti, kokia tyrėjui nežinoma techninė ranga yra patalpoje.

vertinus kompiuterinį nusikaltimą būdingus bruožus, būtina pabrėžti, jog atliekant tyrimo veiksmus svarbios šios aplinkybės:

- 1) informacijos laikmenas bei jose saugomą informaciją gali pažeisti ar sunaikinti

---

<sup>39</sup> Burda R. Kompiuterinėsrangos panaudojimas ekonominiams nusikaltimams (kai kurie kriminalistinės charakteristikos ir tyrimo metodikos ypatumai) // Jurisprudencija, 1999. T.12(4). P.72.

vair s fiziniai veiksniai – sm giai, sukr timai, aukšta temperat ra, staig s temperat ros svyravimai, dr gm ir kt.;

2) jei informacija saugoma magnetiniuose diskuose, stiprus elektromagnetinis laukas gali visiškai suardyti jos login strukt r nuotoliniu b du, be akivaizdaus, t.y. matomo, fizinio kontakto su ja;

3) bet koks neatsargus elgesys su kompiuterine ranga gali pažeisti ar sunaikinti informacij ;

4) informacija gali b ti užšifruota taikant atitinkamus algoritmus, kuriems vienintelis raktas gali b ti ne tik slaptažodis, bet ir tam tikras pri jimo b das, žinomas tik savininkui;

5) duomenys, svarb s nusikaltimo atskleidimui ir tyrimui, gali b ti saugomi laikmenose, esan iose ne kaltininko, bet kit vartotoj kompiuterin je rangoje.

Atsižvelgiant nurodytas aplinkybes, tyr jui, atliekan iam konkre ius kompiuterinio nusikaltimo tyrimo veiksmus, b tina:

a) atliekant apži r , krat ar po m , tur ti ir naudoti elektromagnetini lauk nustatymo ir matavimo prietaisus;

b) griežtai laikytis saugaus darbo reikalavim bei b ti ypatingai atidžiu fiksuojant, transportuojant ir saugant kompiuterin technik bei informacijos laikmenas kaip daiktinius rodymus;

c) savarankiškai, be specialisto pagalbos, neatlikti su kompiuterine technika joki veiksm , kuri rezultat negalima iš anksto tiksliai numatyti;

d) neleisti jokiems asmenims, esantiems tyrimo veiksmo vykdymo vietoje, liesti kompiuterin rang , informacijos laikmenas, jungti ir išjungti kompiuterius ar kitus elektroninius renginius;

e) numatyti galimus veiksmus, kuri konkre ioje situacijoje gali imtis tariamieji, siekdami sunaikinti informacij ( rodymus), ir užkirsti jiems keli .

Atkreiptinas d mesys tai, jog siekiant išsaugoti kompiuterinius duomenis, reikia atidžiai vertinti konkre ias tyrimo aplinkybes ir pasirinkti tinkamus darbo su kompiuterine ranga metodus. Kartais kriminalistikos rekomendacijose nurodoma, jog b tina nedelsiant išjungti kompiuter iš elektros maitinimo šaltinio, jei yra pagrindo manyti, kad svarbi bylai informacija gali b ti pažeista ar sunaikinta, ta iau dažnai b tent toks kompiuterio išjungimas gali lemti informacijos praradim . Tarkime, jei kaltininkas saugo darbo rezultatus ar priemones šifruotame PGP diske, prie kurio prieiti galima tik vedus slaptažod , staigus ir netik tas kaltininkui tyrimo veiksmas leist aptikti rodymus, o kompiuterio išjungimas ir keliasdešimt sekundži , sugaišt diskui uždaryti, padarys informacij visiškai neprieinama.

Toliau bus detaliau išnagrini ti pagrindiniai kompiuterini nusikaltim tyrimo

veiksmi, kuriuos paprastai nurodo dauguma kriminalistikos darb autori (pvz., E.Melik, V.B.Vechovas, J.M.Baturinas ir kiti):

- 1) vykio vietos apži ra;
- 2) kompiuterin s technikos apži ra ir po mis;
- 3) kompiuterin s informacijos laikmen apži ra, nusikalstamo poveikio jai p dsak paieška ir po mis;
- 4) speciali j žini panaudojimas ir ekspertiz s skyrimas.

### 5.3.1. VYKIO VIETOS APŽIŪRA

Kriminalistikos mokslo darbuose vykio vietos apžiūra apibrėžiama kaip neatidėliotinas procesinis tyrimo veiksmas, kurio metu tiesiogiai ištiriama, suvokiama organoleptiniais ir techniniais būdais ir užfiksuojama vykio, turinio nusikalstamos veikos požymiai, vieta, jos aplinka, randami, tvirtinami, preliminariai ištiriami ir paimami nusikaltimui iširti reikalingi objektai bei jų lokalinės struktūros<sup>40</sup>. Bendras vykio vietos apžiūros uždavinys – susipažinti su vykio vietos situacija, aplinka, rasti ir užfiksuoti su tiriamuoju vykiu susijusius pėdsakus, o tiriant kompiuterinį nusikaltimą bylas, vykio vietos apžiūros pagrindinis tikslas – konkretios kompiuterinės rangos, kuri yra nusikalstamo pasikėsinimo dalykas arba priemonė ir turi nusikalstamos veikos pėdsakus, nustatymas. Kriminalistikos teoriniuose ir praktiniuose darbuose atliekant šį tyrimo veiksmą siūloma naudoti ekscentrinę taktinę būdą („nuo centro – iki periferijos“), kur „centru“ (vykio vietos apžiūros išėties tašku) laikoma konkreti kompiuterinė ranga (arba kompiuterinės informacijos kaupiklis, laikmena). Vertinus konkrečią tyrimo situaciją, operatyviniame tyrimo grupės rekomenduojama traukti šiuos asmenis: tyrėją, kurio specializacija – kompiuteriniai nusikaltimai (grupės vadovas); kriminalistą, išmanant šios kategorijos nusikaltimų tyrimo ypatumus; kompiuterinį technologijų specialistą; telekomunikacinių tinklų technologijų specialistą (nuotolinis prieigos atvejis); operatyvinius darbuotojus; apylinkės galiotinį; apsaugos pareigūną (jei vykio vieta ar joje esanti kompiuterinė sistema yra saugomas objektas); kinologą.

Prireikus šią grupę gali būti traukti nesuinteresuoti vairių sričių specialistai, žinantys tiriamo objekto darbo specifiką (inžinieriai elektrikai, palydovinio ryšio specialistai, ryšių sistemų operatoriai, informacinių sistemų administratoriai, finansininkai, buhalteriai ir kt.).

Vykiant vykio vietos apžiūrai, rekomenduojama fotografuoti ir filmuoti, užfiksuojant tyrėjo ir specialistų veiksmų nuoseklumą, taip pat gautus rezultatus. Jei apžiūros metu naudojamos kompiuterinės priemonės ir specialios techniniai renginiai, tai pažymima protokole, nurodant jų individualius požymius (tipas, pavadinimas, gamyklinis numeris ir kt.).

Atsižvelgiant tai, kad kompiuterinė informacija (nusikaltimo ir nusikaltimo pėdsakai) gali būti sunaikinta ne tik naudojant valdymo renginius (klaviatūra, pelė), bet ir vienkartinio trumpalaikio kompiuterinės rangos jungimu ar išjungimu arba ryšio linijos tarp renginių nutraukimu, apžiūros pradžioje būtina nustatyti, kurie kompiuteriniai renginiai ar kiti elektrotechniniai renginiai ar prietaisai yra jungti ar išjungti, ir išlaikyti juos to paties būsenos iki specialistas baigs apžiūrą, tai pat turi būti apsaugoti visi maitinimo rangos jungimo taisyklės, esantys vykio vietoje.

<sup>40</sup> Burda R., Krikšėnas R., Latauskienė E. ir kt. Kriminalistikos taktika ir metodika.- Vilnius, 2004. P.26.

vykio vietos apžūros protokole turi būti aprašyti šie faktiniai duomenys<sup>41</sup>:

objekto, kuriame vykdytas nusikaltimas, pavadinimas ir paskirtis;

geografiniai, techniniai ir konstrukciniai vietovės ir patalpos ypatumai (artimiausia objekto aplinka, fiziniai ir technologiniai duomenys, prieigos keliai, ryšiai, elektros ir kitos komunikacijos, susijusios su kompiuterinės rangos sumontavimu ir eksploatavimu, taip pat maitinimo grandinių pagrindinės charakteristikos);

objekto apsaugos sistemos ypatumai, kompiuterinės rangos ir kompiuterinės informacijos apsaugos būklė, rėžiniai, išdėstymas, pagrindinės techninės charakteristikos;

kompiuterinių renginių išdėstymas vienas kito atžvilgiu, maitinimo ir ryšio linijų atžvilgiu;

kompiuterinės rangos technologinį sujungtys su kita ranga, taip pat ir esančia už apžūros teritorijos ribas (nustatoma tiriant ryšio kabelius ir laidus, vedančius nuo apžūros kompiuterinės rangos, tokiu būdu apžūros teritorija gali išsiplėsti);

kompiuterinės rangos išdėstymas ventiliaciniai ir kitą angų statybinėse konstrukcijose, durys ir langų angos, vaizdo stebėjimo techniniai priemonių atžvilgiu, darbo vietų atžvilgiu;

kiti techniniai elektros, elektroninių renginių, prietaisų, priemonių, esančių toje patalpoje kartu su kompiuterine ranga (telefonų, kitų ryšio priemonių, biuro organizacinės technikos, garso ir vaizdo magnetofonų, autoatsakiklių, elektroninių rašomųjų mašinelių, apšvietimo prietaisų, garsiakalbių, televizorių, radijo imtuvų ir kt.), charakteristikos.

Ypatingai kruopščiai protokole turi būti aprašytos aptiktos kenkėjiškos kompiuterinės programos ir laikmenos su jomis; kompiuterinės programos, slygojančios nesankcionuotus vartotojo veiksmus ar turinčios tokos galutiniam technologinio proceso rezultatams ir jų laikmenos; slapto kompiuterinės informacijos ir magnetinių kaupiklių gavimo, sunaikinimo ar blokavimo techninės priemonės; specifiniai nusikaltimo ir nusikaltimo padarai. Kriminalistikos darbuose paprastai nurodomi šie tipiniai kompiuteriniai nusikaltimų padarai, aptinkami apžūros metu:

pirštų atspaudai ant kompiuterinės rangos, apsaugos ir signalinės rangos, jų klaviatūros, jungiamųjų ir maitinimo laidų, jungčių, kištukinių lizdų, kištukų, perjungiklių, mygtukų, maitinimo tampo perjungiklių ir kt.;

silaužimo rankos, apsaugos ar signalinių renginių sugadinimo, sunaikinimo ar modifikavimo padarai;

jungiamųjų laidų ir izoliacinių medžiagų likučiai, lydmetalių, kanifolijos ar flusio lašai, jungiamųjų laidų spaudimo, lydymo, dūrimo, pjovimo ar klįjavimo prie jų pašaliniai daiktai ar

<sup>41</sup>

, 1998. C p.32.

tais p dsakai;

specialios registravimo, steb jimo, testavimo rangos duomenys (darbo su kompiuterine informacija elektroninio registravimo žurnalo duomenys, vaizdo ir garso rašymo priemoni duomenys ir pan.).

Apži ros metu gali b ti rasti šie dokumentai, j laikmenos ir kaupikliai, svarb s kompiuterini nusikaltim tyrimui:

informaciniai, apskaitos dokumentai, susij su kompiuterin s rangos darbu ir kompiuterin s informacijos naudojimu (techninis pasas arba j pakei iantis dokumentas; operatoriaus žurnalas arba technologini operacij , prieigos prie kompiuterin s sistemos ir prie konfidencialios informacijos automatinio fiksavimo protokolas; kompiuterini kaupikli , užsakym (užduo i ar užklaus ), program , rašyt kaupikliuose, apskaitos žurnalai; broko sunaikinimo apskaitos žurnalai; konfidencialios informacijos ir kaupikli su ja trynimo aktai);

dokumentai, susij su prieigos teis tumu (elektroniniai prieigos raktai, slaptažodžiai, asmeniniai identifikavimo numeriai (PIN kodai), elektroninis parašas ir kitos sankcionuoto vartotojo identifikavimo ir autentifikavimo priemon s);

registravimo ir buhalteriniai dokumentai (licencijos ir licencin s sutartys; kompiuterin s technin s ir programin s rangos, informacijos apsaugos priemoni , informacijos apskaitos protokol ir elektronini dokument format atitikimo nustatytiems reikalavimams sertifikatai; sutartys (susitarimai) d l kompiuterin s rangos naudojimo ir prieigos prie kompiuterin s informacijos su atitinkam dokument kompletu; atsiskaitymo ir kiti buhalteriniai dokumentai, atspindintys vartotojo atsiskaitymus už jam suteiktas paslaugas, parduotas prekes ar vykdytus kreditinius atsiskaitymus);

kontroliniai apskaitos dokumentai (kompiuterin s technin s ir programin s rangos, apsaugos sistem diegimo, konfig ravimo, derinimo, remonto ir techninio aptarnavimo darb registravimo žurnalas; gedim ir sutrikim registravimo žurnalas; apsaugos signalizacijos darbo trikdži ir suveikimo atvej registravimo žurnalas; informacijos saugumo režimo kontrolini patikrinim , revizij , tarnybini ar kit patikrinim aktai; suvestin s ataskaitos ir kontroliniai atskir darbo sri i , operacij ar laiko interval duomenys);

dokumentai, reglamentuojantys darbuotoj v veiksmus (pareigybi aprašymai, pareigin s instrukcijos, darbo su kompiuterin mis sistemomis, programine ranga, apsaugos priemon mis, operatoriaus darbo nestandartin mis (avarin mis) situacijomis instrukcijos ir kt.).

Paskesn min t dokument apži ra leidžia nustatyti kompiuterinio nusikaltimo vykdymo b d , nusikalt lio panaudotas priemones ir medžiagas, disponavim specialiomis žiniomis ir g džiais, iškelti versijas d l priežastini ryši .



### 5.3.2. KOMPIUTERIN S TECHNIKOS PRIEMONI APŽI RA IR PO MIS

Kompiuterin s technikos priemoni apži ra – tai neatid liotinas procesinis tyrimo veiksmas, kurio metu siekiama rasti ir užfiksuoti su tiriamuoju vykiu susijusius p dsakus, leisian ius nustatyti, kas, koku tikslu ir kokiomis aplinkyb mis vykdo nusikaltim , išsiaiškinti vykio detales ir nusikaltimo vykdymo mechanizm bei nustatyti kompiuterin s rangos technin b kl . Visuose kriminalistikos teoriniuose ir praktiniuose darbuose pabr žiama, jog vykdyti kompiuterin s technikos priemoni apži r b tina dalyvaujant informacini technologij specialistui.

Prad jus apži r , pirmiausia reikia išsiaiškinti kompiuterin s rangos paskirt , nustatyti, jungta ji ar ne, patikrinti jos darbingum ir tai, ar jos atmintin je yra kompiuterin informacija, nustatyti, ar ranga prijungta prie ryšio linij ar kit technini rengini . Po to b tina prad ti materialii p dsak ant jos korpuso, atskir detali ir laidini sujungim , valdymo priemoni (klaviat ros, pel s) paiešk .

Atsižvelgiant kompiuterin s informacijos b dingas ypatybes, kriminalistikos rekomendacijose nurodoma, kad vykdant kompiuterin s technikos apži r neleistina naudoti ši priemoni :

- 1) magnetini medžiag ir instrument (magnetini milteli , šepet li ir kt.);
- 2) technin s rangos, sukurian ios elektromagnetin lauk ar trukdžius (elektrostatini ieškikli (EPI-2), elektromagneto), metalo ieškikli , galing apšvietimo prietais , ultravioletinius ir infraraudonuosius spindulius skleidžian i prietais ir kt.;
- 3) r gštini ar šarmini medžiag ir šildymo prietais , kad išvengti kompiuterin s technikos ir informacijos, nusikalt lio ir nusikaltimo p dsak sunaikinimo ar pažeidimo.

Min tas medžiagas ir prietaisus galima naudoti tik laikantis ypating atsargumo priemoni , ne mažiau kaip 1 metro atstumu nuo kompiuterin s rangos ir jos jungiam j laid .

Po kompiuterin s technikos apži ros dažniausiai atliekamas jos po mis ir tolesnis ekspertinis tyrimas. Kadangi kompiuterin s technikos po mis vykdomas siekiant, kad v liau j ištirt informacini technologij specialistas ar ekspertas, labai svarbu tinkamai atlikti po mio veiksmus – nustatyta tvarka demontuoti kompiuter ir kitus renginius j aptikimo vietoje bei supakuoti juos taip, kad laboratorijoje ar kitoje specialioje tyrimo vietoje b t galima s kmingai sujungti tiksliai atkuriant pirmin model .

Atkreiptinas d mesys tai, kad kompiuterin s technikos apži ros bei po mio veiksm metodika gali b ti dvejopa ir priklauso nuo kompiuterio b senos tyrimo veiksmo atlikimo momentu, t.y. svarbiausia, ar kompiuteris aptinkamas neveikiantis (išjungtas) ar veikiantis (jungtas).

Pirmasis atvejis, kai kompiuteris neveikia (yra išjungtas), informacijos išsaugojimo

požiuriu yra paprastesnis. Šiuo atveju tyrėjui rekomenduojama atlikti tokius veiksmus:

- 1) tiksliai nurodyti kompiuterio ir kitų išorinių renginių radimo vietą protokole bei pridedamoje schemoje;
- 2) tiksliai ir detalai aprašyti kompiuterio ir kitų išorinių renginių sujungimo tvarką, akcentuojant konkrečias jungiamųjų laidų ir kabelių ypatybes (specifikacijas, sujungimo grandžių kiekį, spalvą ir kt.);
- 3) nufotografuoti arba padaryti vaizdo rašius visų renginių sujungimo vietų prieš juos atjungiant;
- 4) išjungti kompiuterį iš elektros maitinimo šaltinio ir laikantis darbų saugos reikalavimų atjungti išorinius renginius;
- 5) atskirai supakuoti laikmenas (disketes, magnetines juostas) pakuotes, nekaupiančias statinio elektros krūvio;
- 6) atskirai supakuoti kiekvieną renginį, jungiamuosius laidus ir kabelius;
- 7) ypatingai atidžiai ir atsargiai supakuoti bei gabenti pagrindinę informacijos kaupiklį – kietąjį diską (vin ester).

Antruoju atveju, kai kompiuteris veikia, tyrimo veiksmų eiga informacijos išsaugojimo požiuriu žymiai sudėtingesnė. Šiuo atveju tyrėjas, neturėdamas pakankamą informacinių technologijų srities specialiąsias žinias, negali operatyviai užfiksuoti kokių nors. Tokiomis aplinkybomis pagrindinis tyrimo uždavimas – išsaugoti ir perduoti specialistui ar ekspertui kompiuterinę techniką ir joje esančią informaciją nepakitusi, taigi tyrėjas privalo paaisyti anksčiau išvardintą bendrą pobūdžio rekomendaciją ir papildomai atlikti šiuos veiksmus:

- 1) nustatyti, kokia programa ar programos tyrimo veiksmo atlikimo momentu vykdomos veikiančios kompiuteryje;
- 2) detalai aprašyti vaizdą displejaus ekrane, jei būtina padaryti jo nuotrauką ar vaizdo rašius;
- 3) išsaugoti operatyvinę atmintyje esančią informaciją atskiroje laikmenoje;
- 4) tinkamai sustabdyti programų vykdymą;
- 5) nustatyti, ar kompiuteris turi išorinių renginių, skirtų nuotolinei prieigai prie sistemos, pvz., modemų, ir užfiksuoti protokole juos būklę, po to nutraukti prieigos per šiuos renginius galimybes;
- 6) aprašyti protokole ne tik savo veiksmus, bet ir jų rezultatus bei atsakomąsias kompiuterio reakcijas;
- 7) tinkamai išjungti kompiuterį ir atlikti visus veiksmus pagal modelį, kai kompiuteris neveikia.

Kompiuterinės technikos apžiūros protokole fiksuojami šie pagrindiniai duomenys:

- jos tipas (paskirtis), pavadinimas, konfig racija, spalva ir gamyklinis numeris (serijinis, inventorinis arba gaminio apskaitos numeris);
- jungiam j ir maitinimo laid tipas (paskirtis), spalva ir kiti individual s požymiai;
- b sena apži ros metu ( jungta ar išjungta);
- technin b kl – išorinis vaizdas, korpuso b kl , komplektacija (blokai, mazgai, detal s, sujungimai tarp j , darbingumas), naudojamo informacijos kaupiklio tipas;
- maitinimo šaltinio tipas, jo technin s charakteristikos ir b kl (darbin tampa, srov s dažnis, darbin apkrova, ar yra saugiklis, stabilizatorius, tinklo filtras, prijungtos prie jo rangos kiekis, kištukini lizd skai ius ir kt.);
- ar yra kompiuterin s rangos žeminimas, jo technin b kl ;
- technin s galimyb s prie kompiuterin s rangos prijungti išorinius renginius, kompiuterin s rangos prijungimo prie išorini rengini ar prie ryšio linij charakteristika;
- kompiuterin s rangos pažeidimai, standarte nenumatyti konstrukciniai pakeitimai kompiuterin s rangos architekt roje, jos atskirose detal se (dalyse, blokuose), ypa tie, kurie gal jo atsirasti d l nusikalstamos veikos; nusikalstamos veikos p dsakai (kompiuterin s rangos korpuso pažeidimo, patekimo korpuso vid , nesankcionuoto technin s rangos prijungimo prie kompiuterin s sistemos, piršt ir kt. p dsakai);
- kompiuterin s rangos išd stymas erdv je išorini r engini ir kitos elektrotechnin s rangos atžvilgiu; tikslu kompiuterin s rangos sujungim su kita technine ranga tvarka;
- apdorojamos informacijos kategorija (vieša, bendro naudojimo ar nevieša, slaptinta);
- aptikt informacijos laikmen (diskeli , kompaktini disk (CD, DVD), USB rakt ) duomenys (tipas, mark , užrašai ant lipduko ir pan.);
- kompiuterin s rangos ir joje apdorojamos informacijos apsaugos sistemos priemoni ypatyb s (jei yra apsaugos sistema, nurodyti slaptažodžius, kitus algoritmus, jimo ir iš jimo kompiuterio programas b dus) ir kt.

Siekiant užtikrinti kompiuterin s rangos ir joje esan ios informacijos saugum , b tina apži r ti ir, jei manoma, paimti vis kratomojoje mon je ar staigoje esan i kompiuterin rang . Ant paimam kompiuteri maitinimo lizd , jungikli reikia užklijuoti tyr jo užpildytus ir pasirašytus lapelius, informacijos laikmenas (diskelius ir kompaktinius diskus) b tina paimti kartu su pakuote arba d žute, kurioje saugomos, atskiri diskeliai pakuojami aliuminio folij ir užantspauduojami pagal bendr sias taisykles. Jei kompiuterin s rangos paimti ne manoma, atlikus apži r , b tina kompiuterin rang išjungti ir užantspauduoti, patalpoje atjungti elektr , užantspauduoti elektros skydel ir užtikrinti jos fizin apsaug .

### 5.3.3. KOMPIUTERINIS INFORMACIJOS LAIKMENŲ APŽIŪRA, NUSIKALSTAMO POVEIKIO JAI PDSAK PAIEŠKA IR PŪMIS

Kriminalistikos metodikos darbuose skiriami du kompiuterinis informacijos bei nusikalstamo poveikio jai pdsak paieškos atvejai:

- 1) informacijos bei nusikalstamo poveikio jai pdsak paieška kompiuteriniuose laikmenose ir kitoje kompiuteriniame rangoje (kitais tariant, skaitmeniniuose formos);
- 2) informacijos bei nusikalstamo poveikio jai pdsak paieška nekompiuteriniame rangoje (neskaitmeniniuose formos).

Kompiuterinė informacija gali būti kaupiama virose laikmenose – magnetiniuose, optiniuose, magnetooptiniuose ir kitokiose atmintiniuose – kietajame diske, lankiniuose diskuose, kompaktiniuose diskuose, rezervini kopijose, renginiuose laikmenose, taip pat operatyviniuose atmintiniuose, jei vykdomos programos (tačiau ši informacija yra sunku išsaugoti, nes ji visada prarandama išjungiant kompiuterį ir paprastai prarandama nutraukiant programos vykdymą). Informacijos laikmenų tyrimas ir analizė vykdomi tik dalyvaujant informacinių technologijų specialistui ar ekspertui.

Laikmenose gali būti užfiksuoti vairo pobūdžio duomenys, paprastai skiriamos šios duomenų grupės:

- vartotojų identifikaciniai duomenys, slaptažodžiai, kodai, prisijungimo vardai;
- techniniai duomenys;
- renginių schemas ir grafiniai vaizdai;
- dokumentų tyrimai;
- kenkėjiškos programos, virusai, jų kodai bei kriptavimo priemonės ir kt.

Pabrėžtina tai, jog informacijos paieška būtina atlikti visoje failų sistemoje, nepaisant vardų bei priedvardžių (plūtinai), skaitant paslėptuosius failus ir jų struktūras. Ypač atidžiai reikia iširti vadinamuosius „log failus“ (programos veiklos registrus, kuriuose gali būti užfiksuota svarbi vairo veiksmų atlikimo informacija, laikas ir data).

Siekiant užfiksuoti nusikaltėlio bendravimo su kitais asmenimis duomenis, būtina iširti elektroninio pašto programų bazes, „online“ bendravimo programų pranešimų bazes (ICQ, Odigo ir kt.), laikinai programas naršyklėse atmintiniuose (spartinančių atmintin – „keš“).

Išimti ir užfiksuoti informaciją paprastai rekomenduojama kartu su jos laikmena, išskyrus nedidelius teksto ar vaizdo duomenis, kuriuos gana paprastai ir efektyviai galima fiksuoti išspausdinant popieriuje.

Atliekant kompiuterinį informacijos paiešką, galima aptikti ir šias svarbius dokumentus nekompiuteriniame rangoje:

- popierinius dokumentus, su vykdyto nusikaltimo pdsakais, pvz., priegos

slaptažodžius ir kodus, telefonini pokalbi išklotines, s skaitas, užrašus ir kt.;

- popierinius dokumentus, likusius išoriniuose renginiuose, pvz, spausdintuvuose ar kopijuokliuose, d l nusikalt lio neapdairumo;
- technin s ir programin s rangos dokumentus;
- darbo su kompiuteriu dokumentus ar norminius teis s aktus, reglamentuojan ius darbo su konkre ia kompiuterine ranga, informacine sistema ar tinklu, tvark , rodan ius, kad tariamasis j žinojo ir s moningai pažeid ;
- tariamojo ar kaltinamojo asmeninius dokumentus.

Kriminalistikos metodikos darbuose rekomenduojama kompiuterin s informacijos laikmen (dažniausiai lanks i j disk , kompaktini disk , kietojo disko ir kt.) apži r atlikti naudojant taktin b d „nuo bendro prie atskiro“, dalyvaujant informacini technologij specialistui. Prad jus apži r , pirmiausia reikia aprašyti individualius laikmenos požymius (nurodoma tipas, r šis, paskirtis, spalva, dydis, išvaizda, pavadinimas, gamyklinis ir individualus numeris, ar yra lipdukas ir užrašai ant jo, ar yra fizini korpuso pažeidimo žymi ir p dsak ant jo, apsaugos nuo kompiuterin s informacijos trynimo ir rašymo elemento b sena), po to yra atliekama laikmenoje esan ios kompiuterin s informacijos apži ra.

Prieš pradedant apži r , tyrimo veiksmo protokole reikia nurodyti:

- 1) apži rai naudojamos kompiuterin s technikos duomenis ir pagrindinius jos programin s rangos rekvizitus (tipas, r šis, pavadinimas, gamyklinis arba registracijos numeris, versijos numeris, juridinis adresas ir (arba) programinio produkto autorius);
- 2) programos, kurios pagalba buvo testuojama kompiuterin sistema ir jos programin ranga, siekiant nustatyti ar joje n ra kenk jiškos programin s ar technin s rangos, rekvizitus.

Analizuojant laikmenoje esan i kompiuterin informacij , b tina nustatyti duomenis, turin ius ryš su tiriamu vykiu. Didel s apimties informacijos apži ros procesui spartinti galima naudoti automatizuotos paieškos pagal reikšmin žod funkcij , kuri yra standartiniame kompiuteri programin s rangos pakete. Apži ros procesas papildomai turi b ti fiksuojamas fotografuojant ar filmuojant. Aptikus nusikaltimo p dsakus, b tina išspausdinti vis arba dal kompiuterin s informacijos ir prid ti j prie tyrimo veiksm protokolo, nurodant naudoto spausdinimo renginio individualius požymius (tip , r š , pavadinim , numer ).

Apži ros protokole taip pat nurodomi šie duomenys:

- laikmenos apsaugos nuo nesankcionuoto panaudojimo individual s požymiai (holograma, br kšninis kodas, šrifto iškilumas, perforacija, fluorescavimas, asmeninio parašo ar savininko nuotraukos laminavimas, j dydis, spalva, išvaizda ir kt.);

- laikmenos ir jos apsaugos klastojimo ar kitokio neteis to poveikio požymiai;
- vidin laikmenos specifikacija (serijinis numeris, kodas, talpa);
- laikmenos talpos užimtos ir laisvos dalies dydis;
- sugadint zon , sektori , klasteri , cilindr kiekis ir numeriai;
- rašyt program , fail , katalog skai ius (j išd stymo laikmenoje strukt ra, pavadinimai, vardai ir(arba) prievardžiai (pl tiniai), dydis (apimtis), taip pat ir tas, kur užima j pavadinimai, suk rimo (arba paskutinio pakeitimo) data ir laikas, specialios žym s (pvz., sisteminis, archyvinis, pasl ptas, tik skaitymui arba rašymui ir kt.);
- pasl pt arba ištrint fail (program ), jei toki buvo, rekvizitai (pavadinimas, dydis, suk rimo ar sunaikinimo data ir laikas).

#### 5.3.4. SPECIALI J ŽINI PANAUDOJIMAS IR EKSPERTIZ S SKYRIMAS

Lietuvoje informacini technologij ekspertiz s, tyrimus atlieka ir specialist išvadas teikia Lietuvos teismo ekspertiz s centro Kompiuterini tyrim skyrius, Lietuvos policijos Kriminalistini tyrim centro Kriminalistini tyrim valdybos Informacini technologij tyrimo skyrius, Valstyb s saugumo departamento specializuotas padalinys. Lietuvos teismo ekspertiz s centro, kuriame informacini technologij ekspertiz s (tyrimai) atliekamos nuo 1995 m., duomenimis<sup>42</sup>, b tent šios ekspertiz s tampa vienos iš paklausiausi , pastaraisiais metais ženkliai išaugo metinis skiriam tyrim skai ius (plg., 2002 m. – 57 tyrimai, 2005 m. – 120 tyrim ).

Speciali j žini panaudojimo ir ekspertini tyrim klausimai bei problemos buvo nagrin jami Baltijos valstybi teis saugos pareig nams skirtame tarptautiniame Baltijos regiono seminare „Kompiuterini nusikaltim ikiteisminis tyrimas ir teisminis nagrin jimas“, 2003 m. vykusiame Tartu (Estijoje). Šiame seminare buvo aptarti tiek bendrieji teoriniai, tiek specialieji technologiniai klausimai, pvz., speciali program , skirt kompiuterini sistem ekspertizei (ESCAP, CART), darbo aspektai.

Atsižvelgiant kompiuterini nusikaltim ypatybes bei vertinus kompiuterin s programin s ir technin s rangos kaip kriminalistinio objekto sud tingum , b tina pasteb ti, jog šios r šies nusikaltim byl s kmingam tyrimui ypa didel reikšm turi tinkamas speciali j žini panaudojimas. Atkreiptinas d mesys tai, kad paprastai tyr jas neturi pakankam speciali j informatikos srities žini ir technini g dži , b tin saugiam informacijos po miui, be to, tyr jo prielaidos apie tai, kad viename ar kitame kompiuteryje arba kompiuterin je laikmenoje gali b ti saugoma svarbi tiriamai bylai informacija, dažniausiai yra paremtos tikimybe, tyr jas neturi rodan i duomen , geriausiu atveju disponuoja tik operatyvine informacija. Kriminalistikos mokslo darbuose daroma išvada, kad kompiuterin ranga yra gana sud tingas kriminalistinis objektas, kur tiriant b tina panaudoti specialias žinias<sup>43</sup>. Galima konstatuoti, jog specialist dalyvavimas vykdant kompiuterini nusikaltim byl ikiteismin tyrim b tinas, nes speciali j žini panaudojimas labai svarbus vykdant kratas, apži ras, po mius ir kitus tyrimo veiksmus. A.N.Jakovlevo<sup>44</sup> ir kit mokslinink teigimu, specialiosios žinios tur t b ti panaudojamos rengiantis atlikti tyrimo veiksmus, vykdant nusikaltimo vietas ir kompiuterin s technikos apži r , krat ar po m , tardymo metu, akistatos metu, tiriamojo eksperimento metu.

V.B.Vechovo darbuose pabr žiama, kad specialist dalyvavimas turi b ti privalomas

<sup>42</sup> Informacini technologij tyrim galimyb s // <http://www.ltec.lt/naujienos.php?item=56>; prisijungimo laikas 2006-10-01.

<sup>43</sup> Burda R.. Kompiuterin s rangos panaudojimas ekonominiams nusikaltimams (kai kurie kriminalistin s charakteristikos ir tyrimo metodikos ypatumai) //Jurisprudencija, 1999. T.12(4). P.73.

<sup>44</sup>

tiriant kompiuterinius nusikaltimus ir rekomenduojama, atsižvelgiant bylos ypatybes, kaip nešališkus ekspertus pasitelkti programuotojus, informacini ir telekomunikacini sistem analitikus, kompiuterini tinkl operatorius, ryši priemoni ir telekomunikacin s rangos inžinierius, informacini sistem saugos specialistus, kompiuterin s technikos aptarnavimo specialistus, kompiuterizuotos finansin s apskaitos ir bank operacij specialistus<sup>45</sup>. Tokie specialistai tur t b ti kvie iami iš mokslo, švietimo ir kit staig ar moni , kurios užsiima informacini ir telekomunikacini technologij tyrimu, saugos užtikrinimu, kompiuterin s rangos eksploatacija bei prieži ra. Patariama nesinaudoti nukent jusio juridinio asmens specialist paslaugomis, nes šie asmenys gali b ti suinteresuoti nusl pti staigos informacin s sistemos eksploataavimo ir saugumo spragas, be to, yra didel tikimyb , kad nusikaltimas gal jo b ti vykdytas vieno iš j .

Apibendrinant kompiuterini nusikaltim tyrimo praktik , pasteb tina, kad speciali j žini panaudojimas ir ekspertiz s atlikimas gali lemti nusikalstamos veikos kvalifikavim ir b ti svarbiu, o kai kuriais atvejais vieninteliu duomen , rodan i nusikaltimo požymius, gavimo b du, tod l atliekant šios r šies nusikaltim ikiteismin tyrim rekomenduojama specialistus traukti kuo anks iau. Specialistai ir ekspertai gali pad ti tyr jui išspr sti šiuos klausimus: kokia yra tiriamos kompiuterin s rangos sud tis ir s ranka (konfig racija), ar galima šios rangos pagalba atlikti veiksmus, inkriminuojamus tariamajam (kaltinamajam); kokie informaciniai resursai yra šioje rangoje; koku b du gali b ti vykdyta nesankcionuota prieiga prie tiriamos rangos ar kompiuterin s sistemos; ar kompiuterin informacij buvo bandoma sunaikinti, pakeisti, kopijuoti; ar rastos laikmenos (failai, bylos) yra informacijos, esan ios konkre ioje kompiuterin je rangoje, kopijos; ar išspausdinti popieriuje tekstai yra programos ar atlikt programos pakeitim išeities kodai ir kokia yra šios programos paskirtis arba koks yra atlikt pakeitim rezultatas; ar laikmenos, programos yra užkr stos virusais ir jeigu taip, tai kokiais b tent; ar pateiktas kodas n ra virusinis; ar tariamojo (kaltinamojo) veiksmiais buvo pažeistos nustatytos darbo su informacine sistema, kompiuteriu taisykl s, informacini resurs naudojimo tvarka; ar darbo taisykli pažeidimas tur jo priežastin ryš su informacijos sunaikinimu, pakeitimu, kopijavimu ir kt.

Daugelyje kriminalistikos mokslo darb pabr žiama ekspertizi svarba kompiuterini nusikaltim tyrimui ir nurodoma, kad tiriant tokius nusikaltimus paprastai skiriamos šios ekspertiz s: kompiuterin s rangos; programin s rangos; kompiuterin s spausdinimo rangos; kompiuterini laikmen .

Lietuvos teismo ekspertiz s centro duomenimis ekspertams dažniausiai pateikiami informacini technologij tyrimo objektai yra šie: nešiojamieji asmeniniai kompiuteriai,

---

<sup>45</sup>

.. , 1998;  
.. , 1996.



kompiuteri sisteminiai blokai, delninukai, spausdintuvai, skeneriai, mobiliojo ryšio telefono aparatai, mokymų kortelės, įvairios informacijos laikmenos, lyginamieji (dokumentai, banknotai ar kiti) pavyzdžiai<sup>46</sup>.

Kompiuterinės rangos ekspertizės skyrimo problemos aptartos V.Kligio ir V.Jankausko straipsnyje „Informacinių technologijų ekspertizė LTEC: dabartis ir perspektyva“<sup>47</sup>, leidinyje „Teismo ekspertizės skyrimo klausimai“<sup>48</sup>, kompiuterinės spausdinimo rangos ekspertizės ypatybės nagrinėjo A.Deringas, Z.Rinkevičius ir L.Sakalauskas straipsnyje „Kompiuteriniais spausdintuvais išspausdinti dokumentai kriminalistinis tyrimas“<sup>49</sup>.

Iki nutarimo dėl ekspertizės skyrimo pirmo rekomenduotina pasikonsultuoti su specialistu dėl jos tikslų, klausimų formulavimo, pateikiamos medžiagos pobūdžio. Kompiuterini nusikaltimų tyrimo metu skiriamoms kompiuterinėms techninėms ir programinėms ekspertizėms keliami šie tikslai:

1. visos arba dalies kompiuterinės informacijos, esančios laikmenose, taip pat ir netekstinės formos (sudėtinas formatas – programavimo kalbos forma, elektroniniai lentelės, duomenų bazės ir kt.) atkūrimas ir išspausdinimas (pagal tam tikras temas ar reikšminius žodžius);
2. kompiuterinės informacijos, anksčiau saugotos laikmenose, o vėliau ištrintos arba pakeistos, atkūrimas;
3. kompiuterinės informacijos (dokumentai, failai, programos) sukūrimo, pakeitimo, sunaikinimo, kopijavimo datos ir laiko nustatymas;
4. kompiuterinės informacijos (dokumentai, failai, programos), esančių laikmenoje, parengimo vietas ir būdus, autorystės nustatymas;
5. užkoduotos kompiuterinės informacijos iššifravimas, slaptažodžių parinkimas ir apsaugos sistemos veikimas;
6. kompiuterinės sistemos ir informacijos tyrimas, siekiant nustatyti, ar yra programiniai ar techniniai moduliai ir modifikacijos, lygojančios nesankcionuotą informacijos sunaikinimą, blokadimą, pakeitimą arba kopijavimą, kompiuterinių, jų sistemos ar tinklo darbo sutrikdymus;
7. galimų informacijos nutekėjimo kanalų iš kompiuterinių, jų sistemos ar tinklo, taip pat patalpų nustatymas;
8. galimų nesankcionuotų prieigos prie statymų saugomos kompiuterinės

<sup>46</sup> Informacinių technologijų tyrimų galimybės // <http://www.ltec.lt/naujienos.php?item=56>; prisijungimo laikas 2006-10-01.

<sup>47</sup> Kligys V., Jankauskas V. Informacinių technologijų ekspertizė LTEC: dabartis ir perspektyva // Vilnius: M. Romerio universitetas, 2005;

<sup>48</sup> Teismo ekspertizės skyrimo klausimai. Informacinis laiškas.- Vilnius, 1996. P.4.

<sup>49</sup> Deringas A., Rinkevičius Z., Sakalauskas L. Kompiuteriniais spausdintuvais išspausdinti dokumentai kriminalistinis tyrimas // Kriminalinė justicija: Lietuvos teisės akademijos mokslo darbai.- Vilnius, 1997. T.7-8.

informacijos ir jos laikmen b d nustatymas;

9. kompiuteri , j sistemos ar tinklo technin s b kl s, nusid v jimo, taip pat individuali kompiuterin s sistemos pritaikymo konkre iam vartotojui požymi nustatymas;

10. atskir asmen , minim byloje, profesin s kvalifikacijos informatikos ar programavimo srityje nustatymas, konkre ios kompiuterin s sistemos vartotojo žini ir g dži lygmens nustatymas;

11. konkre i asmen , pažeidusi kompiuteri , j sistemos ar tinklo eksploatavimo taisykles, nustatymas;

12. priežas i ir aplinkybi , paskatinusi vykdyti kompiuterin nusikaltim , nustatymas;

13. kompiuterin s rangos, išorini rengini , magnetini laikmen , programini produkt vert s nustatymas;

14. techninio pob džio dokument vertimas ir kt.

Kompiuterin s technin s ir programin s ekspertiz s gali b ti identifikacin s arba neidentifikacin s, be to, tiriant kompiuterini nusikaltim bylas, dažnai skiriamos šios kriminalistin s ekspertiz s: daktiloskopin s, odorologin s, trasologin s, grafologin s, fonoskopin s, autoryst s nustatymo, radiotechnin s, dokument ekspertiz s, polimerini medžiag ir gamini iš j ekspertiz s.

Apibendrinant galima konstatuoti, kad speciali j žini panaudojimas ir ekspertiz s turi ypa didel reikšm kompiuterini nusikaltim s kmingam tyrimui, ta iau pasteb tina ir tai, jog plintant nusikaltimams elektronin je erdv je, teis saugos institucijoms b tina kaupiti žinias apie informacini sistem veikimo bei saugumo užtikrinimo principus, proced ras, darbo su kompiuterine informacija metodus bei kelti pa i teis saugos pareig n speciali j kvalifikacij ir kurti specialius padalinius kovai su kompiuteriniu nusikalstamumu, nes vienkartinis informatikos specialist ar ekspert traukimas tiriant bylas n ra pakankamai efektyvus ir negali užtikrinti mokliškai pagr stos šios r šies nusikaltim tyrimo metodikos suformavimo. Atsižvelgiant vyraujan ias nusikalstamumo tendencijas bei pasaulin praktik , 2001 m. Lietuvos kriminalin s policijos biuro Nusikaltim tyrimo vyriausiojoje valdyboje buvo steigtas specializuotas Nusikaltim elektronin je erdv je tyrimo skyrius, kurio misija<sup>50</sup> – užtikrinti Konvencijos d l elektronini nusikaltim reikalavim gyvendinim , užkardyti, tirti ir atskleisti rengiamus, daromus ar padarytus nusikaltimus elektronin je erdv je – pasauliniame interneto tinkle bei korporatyvin se informacin se sistemose – intranete, taip siekiant užtikrinti Lietuvos visuomen s ir informacini technologij saugum šioje sferoje.

---

<sup>50</sup> Aplinkyb s, d l kuri buvo kurtas Nusikaltim elektronin je erdv je tyrimo skyrius – NEETS (angl. CYBERPOLICE) // [http://www.cyberpolice.lt/index\\_.asp?DL=L&TopicID=2](http://www.cyberpolice.lt/index_.asp?DL=L&TopicID=2); prisijungimo laikas 2006-10-14.

## 6. PAGRINDINIS KOMPIUTERINIS NUSIKALTIMŲ TYRIMO KLAIDOS

Šiuo metu Lietuvoje dar nėra parengtos kompiuterinio nusikaltimų tyrimo metodikos, pagrindinės susistemintos teorinės žinios ir patikrintos praktikoje. Tikima, jog tai sulygoja teisės teoretikų ir praktikų nuomonių dėl kompiuterinio nusikaltimų ir jų tyrimo metodų, kurie gana stipriai skiriasi nuo tradicinių nusikaltimų, vairov bei vieningos pozicijos stygius. Galima pagrįstai teigti, kad šios kategorijos baudžiamajam bylų tyrimo klaidas dažniausiai lemia nepakankamas ikiteisminio tyrimo tyrimo pasiruošimas tiek teoriniu, tiek praktiniu požiūriu bei kalbėjimasis, susijusi su kompiuteriniais nusikaltimais, specifika, nes šie kalbėjimai gali būti lengvai pakeisti ir prarasti rodome gali kompiuterinės technikos požiūriu metu bei atliekant tolesnį tyrimą.

Siekiant išvengti esminių kompiuterinio nusikaltimų tyrimo klaidų, pirmiausia, kaip jau buvo minėta, rekomenduojama visus tyrimo veiksmus vykdyti dalyvaujant informacinių technologijų specialistui, o kompiuterinės technikos tyrimą atlikti kriminalistinės laboratorijos specialistų lygomis, esant galimybei, pasitelkti atitinkamus informacinių ar telekomunikacinių technologijų ir informacijos saugos ekspertus. Tačiau praktika rodo, jog ikiteisminio tyrimo pareigūnai dėl įvairių priežasčių ne visada gali pasinaudoti specialistų ir ekspertų pagalba, nes ekspertizei atlikti reikia laiko, o vykdant pirminius kompiuterinio nusikaltimų tyrimo veiksmus, pvz., kompiuterinės technikos požiūriu, dažnai labai svarbus netikėtumo efektas ir operatyvumas, leidžiantys aptikti kalbėjimus ir išsaugoti būtina rodome informaciją. Atsižvelgiant į šias aplinkybes, būtina ikiteisminio tyrimo tyrimo kompetentingumas, teorinės žinios ir praktiniai gūdžiai lemia kompiuterinio nusikaltimų tyrimo sėkmę, o jo klaidomis gali pasinaudoti kaltinamojo gynėjas bylos teisminio nagrinėjimo metu.

Kriminalistikos mokslo darbuose nurodoma, jog kompiuterinio nusikaltimų tyrimo klaidos gali būti dvejopos:

- 1) bendrosios klaidos, kurios yra padaromos teisės saugos institucijų pareigūnų, atliekančių kompiuterinio nusikaltimų tyrimo veiksmus, ir
- 2) techninės klaidos, susijusios su informacijos apsaugos priemonėmis, diegtomis kompiuteriuose j tiesiogini vartotojai.

V.A.Golubevas ir kiti kriminalistikos bei informacinių technologijų saugos specialistai, apibendrinami praktinės teisės saugos institucijų veiklos rezultatus, pabrėžia, jog dažniausiai pasitaiko šios pagrindinės kompiuterinio nusikaltimų tyrimo klaidos<sup>51</sup>:

- 1) leidžiama dirbti su tiriamuoju kompiuteriu jo savininkui, tiesioginiam vartotojui ar

<sup>51</sup>

kitam suinteresuotam asmeniui;

2) netinkamai atliekami veiksmai su tiriamuoju kompiuteriu ar informacijos laikmenomis;

3) tiriamasis kompiuteris nepatikrinamas dėl virusų ar programinių užsklandų.

Daugelis informacinių technologijų saugos specialistų pabrėžia, jog viena iš esminių ikiteisminio tyrimo tyrimų klaidų yra leidimas dirbti su tiriamuoju (apžėrimu, konfiskuotu) kompiuteriu jo savininkui arba vartotojui, prašant jį jungti ar išjungti kompiuterį, parodyti kompiuteryje saugomą informaciją ar kitokios pagalbos. Suinteresuotas asmuo, juo labiau išmanantis informacinių technologijų veiklos principus geriau nei tyrimas, gali nepastebimai ištrinti, pakeisti ar užšifruoti informaciją ir sunaikinti kalinius, pasinaudodamas menkiausia galimybe dirbti kompiuteriu tiesiog tyrimo veiksmo metu. Vertinus šiuos grėsmes, tyrimui draudžiama leisti liesti kompiuterį ar dirbti juo kompiuterio savininkui ar vartotojui, be to, būtina padaryti kompiuterinės informacijos rezervines kopijas, prieš leidžiant kam nors su ja dirbti.

Kita kompiuterinė nusikaltimų tyrimo klaida – netinkamai atliekami veiksmai su tiriamuoju kompiuteriu ar informacijos laikmenomis – gali sudaryti galimybę kaltinamojo gynėjui teismo bylos nagrinėjimo metu paneigti teismui pateiktos programinės rangos autentiškumą, t.y. jos atitikimą tai rangai (jos b senai), kuri buvo kompiuteryje po miono metu. Siekiant išvengti šios problemos, būtina vykdant bet kokią operaciją su kompiuteriu, užfiksuoti jo b sen tyrimo veiksmo vykdymo metu, kitaip tariant, teis saugos pareigūnui rekomenduojama užantspauduoti kompiuterį tokios b senos, kokios jis rastas, neišjungiant jo ar nejungiant, monės, staigos ar organizacijos atstovo, savininko ar kvieštinio akivaizdoje, arba, jei priimamas sprendimas apžėrinti kompiuterį vietoje, būtina padaryti kopijas vis kietųjų ar lankstųjų diskų, kurie bus paimami kaip kaliniai.

Kriminalistikos metodikos darbuose pabrėžiama, kad kompiuteris pirmiausia yra specialisto tyrimo objektas, todėl iki jis bus perduotas specialistui ar ekspertui, tyrimams rekomenduojama susilaikyti nuo bet kokių veiksmų su kompiuteriu arba griežtai laikytis b tina saugos priemonių (sukurti rezervines kopijas, naudoti apsaugą nuo pakeitimų). Jeigu tiriamajame kompiuteryje yra diegta apsaugos sistema (prieigos kodas, slaptažodis ar kt.), tai netinkamas jo jungimas gali slygoti informacijos, esančios kietajame diske, sunaikinimą, todėl neleidžiama aktyvuoti tokio kompiuterio naudojant jo paties operacinę sistemą. Nusikaltėliai dažnai modifikuoja operacinę sistemą, diegdami programas, skirtas kietajame ar kituose diskuose saugomai informacijai sunaikinti (pavyzdžiui, komanda DIR, naudojama disko katalogo parodymui, gali būti pakeista taip, kad ji vykdytų bus suformatuotas kietasis diskas), be to, tokios kenkėjiškos programos gali sunaikinti tiek duomenis, tiek paties save, todėl vėliau, bylos teismo nagrinėjimo metu, sunku rodyti, ar tiriamajame kompiuteryje tokio pobūdžio programos buvo diegtos tyčia, ar tai neatsargaus kompiuterinio kalio tyrimo, nekompetentingo tyrimų elgesio pasekmės.

Dažnai, kai tiriamasis kompiuteris yra apkrėtas virusais, teismo byloje nagrinėjimo metu kaltinamojo gynėjai sudaroma galimybė atmesti kaltinimus, apkaltinus tyrėjus nekompetentingumu, dėl neatsargumo ar tyčia užkrėtus kompiuter virusais, nes rodyti, kad virusas buvo kompiuteryje iki apžiūros momento ne manoma, jei tyrėjai kompiuterio tinkamai nepatikrino ir to procesiškai neužfiksavo, o panašaus pobūdžio kaltinimas verčia suabejoti visu eksperto darbu ir jo išvad teisingumu. Siekiant išvengti treiosios klaidos, kai tiriamasis kompiuteris nepatikrinamas dėl viruso ar programinių užsklandų, pasekmių, būtina tyrimo veiksmo metu pasitelkti specialistą, kuris patikrintų visas informacijos laikmenas (kietuosius, lanksiuosius diskus ir kitas laikmenas) specialia programine priemone pagalba, pakraudamas tiriamąjį kompiuterį naudojant ne jo operacinę sistemą, bet iš specialiai paruošto kietojo ar kito disko.

Apibendrinami praktinės teisės saugos institucijų veiklos rezultatus, vairi šalies specialistai (pvz., Ukrainos specialistai tarptautiniame konferencijoje „Informacinės technologijos ir saugumas“<sup>52</sup>, JAV specialistai anksčiau minėtame tarptautiniame Baltijos regiono seminare „Kompiuteriniai nusikaltimai ikiteisminis tyrimas ir teisminis nagrinėjimas“), pateikia tokias pagrindines rekomendacijas, skirtas ikiteisminio tyrimo pareigūnams, tiriantiems kompiuterinius nusikaltimus, leisiančias išvengti esminiai nusikaltimų tyrimo klaidai bei rasti ir tinkamai užfiksuoti kompiuterinius kaltinimus: vykdant bet kurį tyrimo veiksmą (ypač kompiuterinės rangos ir informacijos paiešką), tikslinga nuopat pradėti pasitelkti informacinių technologijų specialistą; iki tyrimo veiksmo pradžios svarbu turėti apibrėžtą pirminę informaciją apie tyrimo objektą (kompiuterio, jo operacinės sistemos, išorinį renginį, ryšio priemonių tipą, modelį ir kitus duomenis); vykdant kompiuterio ar kompiuterinės sistemos paiešką, būtina tinkamai sužymėti ir nufotografuoti jo elementus bei jungtis; atliekant tyrimo veiksmą pirmiausia būtina padaryti rezervinę kompiuterinės informacijos kopiją; svarbu surasti ir padaryti laikiną (fail) kopijas; būtina patikrinti Swap File; esant galimybei, reikia surasti ir sulyginti tekstinių dokumentų kopijas. Atliekant kompiuterinį nusikaltimų tyrimo veiksmus, tyrėjai turi žinoti ne tik saugaus darbo su kompiuterine informacija taisykles, bet ir išmanyti apsaugos priemones (programines bei technines), kurias naudoja nusikaltėliai, siekdami sunaikinti ar pakeisti kompiuterinę informaciją.

Pabrėžtina tai, kad kompiuterinį nusikaltimų tyrimo veiksmo metu būtina griežtai laikytis baudžiamojo proceso normų ir visus elektroninius kaltinimus, esančius kompiuteryje, kompiuteriniame tinkle ar informaciniame sistemoje, surinkti teisėtai būdais, kad jie galėtų būti pripažinti rodymais teisme. Tuo tarpu užsienio valstybių patirtis rodo, kad labai dažnai, kaltinamojo gynėjai pastangomis, elektroniniai rodymai teisme nėra pripažinti dėl ikiteisminio tyrimo pareigūnų klaidų. Todėl labai svarbu vykdant kompiuterio ar kompiuterinės sistemos paiešką tinkamai sužymėti

<sup>52</sup>

ir nufotografuoti j elementus bei jungtis, nes kompiuterio ar j sistemos b kl s ūklus užfiksavimas ir dokumentavimas atliekant pirminio tyrimo veiksmus leidžia teisingai sumontuoti rang , pajungti visus jos elementus ir tiksliai atkurti jos b kl laboratorijos s lygomis. Fotografuojant reikia užfiksuoti priekini s ir užpakalin s kompiuterio dalies bei išorini rengini vaizdus stambiu planu.

Vykdam tyrimo veiksm , b tina padaryti rezervin kompiuterin s informacijos kopij , ta iau daryti informacijos (disko, byl , fail ) kopijas naudojantis tik standartin mis rezervinio kopijavimo programomis nepakanka, nes daiktiniai rodymai gali egzistuoti sunaikint ar pasl pt byl pavidalu, o duomenis susietus su šiomis bylomis (failais), galima išsaugoti tik pasinaudojus specialia programine ranga (paprastai naudojamos tokios programos kaip SafeBack, o lankstiems diskams kopijuoti pakanka naudoti DOS program Diskcopy). Laikmenos, kurias numatoma kopijuoti informacij , turi b ti iš anksto paruoštos (jos turi b ti tuš ios, be jokios kitos informacijos) ir saugomos specialiose apsaugin se pakuot se.

Atkreiptinas d mesys tai, kad daugelis tekstini redaktori ir duomen bazi valdymo program kaip šalutin normalaus programin s rangos veikimo rezultat sukuria laikinus failus, kurie dažniausiai yra pa ios programos sunaikinami darbo seanso pabaigoje, ta iau duomenys, esantys šiuose failuose, gali b ti labai naudingi bylai (pvz., galima atkurti fail , jei išeities failas buvo užkoduotas arba sukurtas tekstinis failas buvo išspausdintas, bet nebuvo išsaugotas diske). Nauding duomen galima rasti ir Microsoft Windows operacin s sistemos rankiuose, susijusiuose su kompiuterin s informacijos analize, t.y. Swap File, kuris dirba kaip disko atmintin , didžiul duomen baz su daugybe skirting laikin informacijos fragment , tarp kuri gali b ti aptinkamas net ir visas dokumento tekstas. Tyr jas turi atkreipti d mes ir viariose laikmenose, kietajame diske aptiktas tekstinio dokumento kopijas, kurias b tina sulyginti naudojant paprast tekstin redaktori , nes nežymiai besiskirian ios vieno dokumento kopijos gali atskleisti svarbios bylai informacijos ir tur ti rodom j vert .

Apibendrinant tai, kas išd styta, galima konstatuoti, kad ikiteisminio tyrimo pareig n ir pasitelkt specialist bendras profesionalus darbas vykdam kompiuterinio nusikaltimo pirminio tyrimo veiksmus leidžia išvengti esmini šios r šies nusikaltim tyrimo klaid , kurios gal t s lygoti kompiuterin s informacijos praradim ar sugadinim , bei rasti ir tinkamai užfiksuoti kompiuterinius kal ius, turin ius rodom j vert teisminio bylos nagrin jimo metu.

## IŠVADOS

1. Apibendrinus Lietuvos ir kit valstybi patirt bandant apibr žti kompiuterini nusikaltim s vok , galima padaryti išvad , jog šiuo metu n ra pasiekta vieningo sutarimo nei tarptautiniu, nei nacionaliniu mastu, ta iau nepaisant to, daugelis valstybi kriminalizavo didži j dal veik , kuriomis k sinamasi visuomeninius santykius kompiuterin s informacijos apdorojimo procese ir kompiuterin s informacijos saugum kaip nusikaltimo objekt .

Galima konstatuoti, jog iškelta hipotez , jog kompiuteriniai nusikaltimai, atsižvelgiant j pagrindini strukt rini element , technologijos savitum (pasik sinimo dalyko skaitmenin form , automatizacij , duomen perdavimo tinkl panaudojim ), yra atskira nusikaltim r šis, kuri ženkliai skiriasi nuo tradicini nusikaltim bei n ra tapati nusikaltim elektronin je erdv je s vokai, o kompiuterini nusikaltim išskirtin s savyb s s lygoja ir ši nusikaltim tyrimo ypatumus, pasitvirtino.

Kompiuterin nusikaltim galima b t apibr žti kaip baudžiamajo statymo numatyt visuomenei pavojinga veik , daran i žal visuomeniniams santykiams automatizuotai tvarkant kompiuterin informacij , t.y. atliekant su ja bet kur veiksm – rinkim , užrašym , kaupim , saugojim , klasifikavim , grupavim , jungim , keitim (papildym ar taisym ), teikim , paskelbim , naudojim , logines ir (ar) aritmetines operacijas, paiešk , skleidim , naikinim ar kitok veiksm arba veiksm rinkin .Lietuvos Respublikos baudžiamajame kodekse terminas „kompiuterinis nusikaltimas“ n ra apibr žtas, taigi jis oficialiai n ra teisintas *de jure*, ta iau kalbant apie veikas, susijusias su kompiuterin mis technologijomis bei elektronine erdve, dažniausiai vartojamas *de facto*. Nusikaltim elektronin je erdv je s voka yra platesn , apimanti ir kompiuterinius nusikaltimus, ir kitas nusikalstamas veikas, susijusias ne tik su kompiuterini , bet ir su telekomunikacini technologij panaudojimu.

2. Išanalizavus Europos S jungos ir kit valstybi baudžiamosios politikos patirt , darytina išvada, jog naudojami du visuomenei pavojing veik , daran i žal visuomeniniams santykiams kompiuterin s informacijos tvarkymo srityje, teisinio reglamentavimo b dai: 1) baudžiamuosiuose statymuose numatomos atskiros specialios normos (skyriai, dalys), kurios prireikus papildomos naujomis sud timis, arba 2) taikomos tradicin s baudžiam j statym normos (reglamentuojan ios nusikaltimus nuosavybei, asmens privataus gyvenimo nelie iamumui, intelektinei nuosavybei, dorovei ir kt.). Pirmojo b do privalumas tas, jog veikos yra tiksliai apibr žiamos, o tr kumas tas, jog rizikuojama atsilikti nuo kompiuterini technologij tobul jimo; antrojo b do privalumas tas, jog nereikia keisti baudžiam j statym , ta iau tr kumas tas, jog gali b ti baudžiamos veikos, kurios n ra tokios pavojingos visuomenei, kad b t kriminalizuotos, ir kartu kyla pavojus palikti nebaudžiamomis pavojingas visuomenei veikas, kurias sunku kvalifikuoti

pagal tradicines baudžiamąjį statymų normas.

Naujajame Lietuvos Respublikos baudžiamajame kodekse veikoms, darančioms žalą visuomeniniams santykiams kompiuterinės informacijos tvarkymo srityje, paskiras atskiras XXX skyrius „Nusikaltimai informatikai“, kriminalizuotos yra penkios veikos: kompiuterinės informacijos sunaikinimas ar pakeitimas; kompiuterinės programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas; kompiuterinės informacijos pasisavinimas ir skleidimas; neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo; neteisėtas disponavimas reikmenimis, kompiuteriniais programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti. Be to pastebėti, kad veikos, nurodytos šiame skyriuje, dažnai vykdomos ne kaip atskiri nusikaltimai, bet kartu su kitais nusikaltimais ir inkriminuojamos papildomai. Tai slyginta aplinkybėmis, jog informacinės technologijos neretai panaudojamos siekiant vykdyti kitas nusikalstamas veikas.

Vertinus kompiuterinių nusikaltimų teisinį reglamentavimą Lietuvoje, galima daryti išvadą, kad šiuo metu Lietuvos teisinė bazė pakankamai papildyta ir atnaujinta normomis, susijusiomis su kompiuterinių technologijų panaudojimu bei kompiuterinės informacijos sauga, o Baudžiamojo kodekso normos iš esmės atitinka Europos Tarybos Konvencijos dėl elektroninių nusikaltimų reikalavimus. Vis dėlto reikia pastebėti, jog didelė problema Lietuvoje lieka šios srities terminijos teisinis neapibrėžtumas. Palyginus Lietuvos ir kitų Europos Sąjungos valstybių, pasirašiusių Konvenciją dėl elektroninių nusikaltimų, baudžiamosios teisės harmonizavimo patirtį, galima teigti, kad nacionaliniai statymai turi daug skirtumų tiek teisinės technikos, tiek turinio prasme, tačiau daugelyje valstybių veikos, susijusios su kompiuterinėmis technologijomis bei informacijos saugos pažeidimais, yra kriminalizuotos, nors sankcijos už analogiškas veikas gali gerokai skirtis.

3. Kompiuterinių nusikaltimų kriminalistinė charakteristika, palyginus su kitais nusikaltimais ir ši charakteristika, pasižymi savitomis ypatybėmis, kurias slygoja kompiuterinių nusikaltimų pagrindiniai struktūriniai elementai ir išskirtiniai, tik šiais nusikaltimais ir šiais būdingi bruožai.

Siekiant sėkmingai iširti kompiuterinius nusikaltimus, būtina vertinti kompiuterinės informacijos, kaip pasikėsinimo dalyko, išskirtines kriminalistines ypatybes: kompiuterinė informacija palyginti paprastai ir greitai keičiama (kinta), kopijuojama, dauginama vairia technine ranga, siunčiama vairiausiu atstumu, ribojamu tik elektroninių ryšių rangos veikimo plotu; paimant kompiuterinę informaciją (atliekant pėmdarbius), skirtingai nei materialus objektas (daiktas), ji išlieka pirminiame šaltinyje, nes prieigą prie jos gali turėti tuo pačiu metu keli asmenys, pvz., jei dirbama su informacija, esančia faile, kuriuo gali naudotis keli informacinės sistemos vartotojai.

Charakterizuojant kompiuterinių nusikaltimų subjektus, galima pateikti šiuos



lyginamuosius užsienio valstybi ir Lietuvos duomenis: 1) *amžius*: 54 proc. (Liet. 64 proc.) – 20-40 met ; 33 proc. (Liet. 22 proc.) – jaunesni kaip 20 met ; 13 proc. (Liet. 14 proc.) – vyresni kaip 40 met ; 2) *išsilavinimas*: 40 proc. (Liet. 22 proc.) – aukštasis; 40 proc. (Liet. 23 proc.) – specialusis; 20 proc. (Liet. 55 proc.) – vidurinis ir žemesnis; 3) *organizuotumas*: 62 proc. (Liet. 29 proc.) – nusikalstam grupi nariai; 38 proc. (Liet. 71 proc.) – veikia be bendrinink ; 4) intelektas: 21 proc. – aukštesnis nei vidutinis; 2 proc. – žemesnis nei vidutinis; 5) profesija: 52 proc. nusikalt li profesija susijusi su informacin mis technologijomis; 6) motyvai ir tikslai: 1) savanaudiški – didžioji dalis, 66 proc.; politiniai (terorizmas, politin s akcijos) – 17 proc.; tiriamieji – 7 proc.; chuliganiški – 5 proc.; keršto – 4 proc.

Palyginus pasaulio ir Lietuvos kompiuterini nusikaltim tendencijas bei vertinus ši nusikaltim latentiškom , galima daryti prielaid , jog šiuo metu Lietuvoje išaiškinama daugiausia santykinai nesud ting kompiuterini nusikaltim , nes daugiau nei pus juos padariusi asmen teturi vidurin ar žemesn išsilavinim , be to, mažiau nei tre dalis j yra nusikalstam grupi nariai, kai tuo tarpu kitose Europos valstyb se ir JAV didžioji dalis ši asmen priskiriami „balt j apykakli“, t.y. turin i aukšt j išsilavinim tarnautoj ir darbuotoj , kategorijai, o nusikalstam grupi nariai sudaro net šešiasdešimt procent vis padariusi kompiuterinius nusikaltimus asmen .

Atkreiptinas d mesys tai, kad kitaip nei senasis Baudžiamasis kodeksas, galiojantis Baudžiamasis kodeksas detaliai neaprašo kompiuterini nusikaltim padarymo b d , nes teisiškai netikslinga ir praktiškai neracionalu apibr žti visus b dus, kuriais galima paveikti kompiuterin informacij , ypa vertinus j dinamik . Kompiuterini nusikaltim vykdymo b d turinys gali b ti sudarytas iš vairiausi veiksm derini , priklausan i nuo pažeid jo išradingumo, kvalifikacijos ir intelekto. Ta iau, nepaisant kompiuterini nusikaltim vykdymo b d vairov s, juos galima sugrupuoti pagal metodus keturias grupes: 1) per mimo; 2) neteis tos prieigos; 3) manipuliacij ; 4) kompleksinius.

4. Teis s teoretik ir praktik nuomoni d l kompiuterini nusikaltim ir j tyrimo metod , kurie gana stipriai skiriasi nuo tradicini nusikaltim , vairov bei vieningos pozicijos stygius lemia tai, kad iki šiol Lietuvoje dar n ra parengtos kompiuterini nusikaltim tyrimo metodikos, pagr stos susistemintomis teorin mis žiniomis ir patikrintos praktikoje.

Kompiuterini nusikaltim tyrimo užduotis yra surinkti ir užfiksuoti šiuos duomenis: baudžiamojo statymo numatytos veikos požymius; šia veika padarytos žalos pob d ir dyd ; priežastin ryš tarp veikos ir jos pasekmi , nustatant kaltininko veiksm pob d , nusikaltimo padarymo b d , kaltininko ty i . Tipin se kompiuterini nusikaltim tyrimo situacijose pagrindiniai pirminiai tyrimo veiksmai yra šie: vykio vietos apži ra; kompiuterin s rangos apži ra (paties kompiuterio ir kit rengini ), kompiuterin s informacijos laikmen apži ra (fiksuojant svarbius tyrimui duomenis – tariamojo prisijungimo prie sistemos laik ir b d (vadinamuosius

„log failus“), nusikalstamo poveikio jai p dsak paieška ir po mis, liudytoj apklausa, nukent jusiojo apklausa. Jei tiriamasis nesulaikytas, greta min t pirmini tyrimo veiksm , b tina organizuoti jo paiešk , taip pat, pasitelkus nukent jus asmen ir specialistus, nustatyti nusikaltimo padarymo b do ypatybes. Jei asmuo sulaikomas nusikaltimo vietoje arba iš karto po nusikaltimo padarymo, atliekami šie pirminiai tyrimo veiksmai: sulaikyto asmens krata; sulaikyto asmens apklausa; sulaikyto asmens darbo ir gyvenamosios vietos krata.

Kriminalistikos metodikos darbuose rekomenduojama kompiuterinio nusikaltimo vykio vietos apži r atlikti naudojant ekscentrin taktin b d („nuo centro – iki periferijos“), kur „centru“ ( vykio vietos apži ros išeties tašku) laikoma konkreti kompiuterin ranga (arba kompiuterin s informacijos kaupiklis, laikmena), o kompiuterin s informacijos laikmen (dažniausiai kietojo disko, lanks i j disk , kompaktini disk ir kt.) apži r atlikti naudojant taktin b d „nuo bendro prie atskiro“.

Atsižvelgiant tai, jog tiriant kompiuterinius nusikaltimus nepakanka profesini teisini žini , visuose kriminalistikos metodikos darbuose tyr jui patariama pasitelkti informacini technologij specialist atliekant bet kur tyrimo veiksm . Vykdamt kompiuterin s technin s bei programin s rangos apži r , krat ar po m , svarbu elgtis ypa atidžiai, atsižvelgti kompiuterin s informacijos saugojimo, p dsak sl pimo priemoni ir b d ypatybes, numatyti kaltininko priešišsk veiksm bei kit faktori poveikio informacijai galimybes.

Apibendrinus kriminalistikos bei informacini technologij saugos specialist pasi lymus ir išanalizavus praktin s teis saugos institucij veiklos rezultatus, darytina išvada, jog dažniausiai pasitaiko šios esmin s kompiuterini nusikaltim tyrimo klaidos: 1) leidžiama dirbti su tiriamuoju kompiuteriu jo savininkui, tiesioginiam vartotojui ar kitam suinteresuotam asmeniui; 2) netinkamai atliekami veiksmai su tiriamuoju kompiuteriu ar informacijos laikmenomis; 3) tiriamasis kompiuteris nepatikrinamas d l virus ar programini užskland . *Pagrindin s rekomendacijos*, skirtos ikiteisminio tyrimo pareig nams, tiriantiems kompiuterinius nusikaltimus, pad sian ios išvengti esmini ši nusikaltim tyrimo klaid bei rasti ir tinkamai užfiksuoti kal ius:

1) iki tyrimo veiksm pradžios, jei manoma, reik t tur ti apibr žt pirmin informacij apie tyrimo objekt (kompiuterio, jo operacin s sistemos, išorini rengini , ryšio priemoni tip , model ir kitus duomenis);

2) atliekant tyrimo veiksmus, b tina ne tik žinoti saugaus darbo su kompiuterine informacija taisykles, bet ir išmanyti apsaugos priemones (programines bei technines), kurias naudoja nusikalt liai, siekdami sunaikinti ar pakeisti kompiuterin informacij ;

3) draudžiama leisti artintis prie kompiuterio, liesti kompiuter ar tuo labiau dirbti juo kompiuterio savininkui, vartotojui ar kitam suinteresuotam asmeniui;

4) vykdamt bet kur tyrimo veiksm (ypa kompiuterin s rangos ir informacijos

po m), reik t nuo pat pradži pasitelkti informacini technologij specialist , nes kompiuteris pirmiausia yra specialisto tyrimo objektas, tod l iki jis bus perduotas specialistui ar ekspertui, tyr jams rekomenduojama susilaikyti nuo bet koki veism su kompiuteriu arba griežtai laikytis b tin saugos priemoni ;

5) vykdant bet koki operacij su kompiuteriu, b tina užfiksuoti jo b sen tyrimo veiksmo vykdymo metu, kitaip tariant, tyr jui rekomenduojama užantspauduoti kompiuter tokios b senos, kokios jis rastas, neišjungiant jo ar ne jungiant;

6) jei esant b tinybei priimamas sprendimas apži r ti kompiuter vietoje, pirmiausia reikia padaryti rezervin kopij vis kiet j , lanks i j , kompaktini disk ir kit laikmen , kurie bus paimami kaip kal iai, b tina naudoti apsaug nuo pakeitim ; svarbu surasti ir padaryti laikin fail kopijas, patikrinti Swap File; jei manoma, reikia surasti ir sulyginti tekstini dokument kopijas;

7) tyrimo veiksmo metu pasitelktas specialistas tur t patikrinti visas informacijos laikmenas (kietuosius, lanks iuosius, kompaktinius diskus ir kitas) speciali programini priemoni pagalba, pakraudamas tiriam j kompiuter naudojant ne jo operacin sistem , bet iš specialiai paruošto kietojo ar kito disko (jei tiriamajame kompiuteryje yra diegta apsaugos sistema (prieigos kodas, slaptažodis ar kt.), tai netinkamas jo jungimas gali s lygoti informacijos, esan ios kietajame diske, sunaikinim , tod l neleidžiama aktyvuoti tokio kompiuterio naudojant jo paties operacin sistem );

8) vykdant kompiuterio ar kompiuterin s sistemos po m , b tina tinkamai sužym ti ir nufotografuoti j elementus bei jungtis;

9) tyrimo veism metu b tina griežtai laikytis baudžiamojo proceso norm ir visus ne tik tradicinius, bet ir skaitmeninius kal ius, esan ius kompiuteryje, kompiuteri tinkle ar informacin je sistemoje, surinkti teis tais b dais, kad jie gal t b ti pripažinti rodymais teisme.

Atsižvelgiant kompiuterini nusikaltim ypatybes bei vertinus kompiuterin s programin s ir technin s rangos kaip kriminalistinio objekto sud tingum , b tina pasteb ti, jog šios r šies nusikaltim byl s kmingam tyrimui ypa didel reikšm turi tinkamas speciali j žini panaudojimas ir ekspertiz s, ta iau pasteb tina ir tai, jog plintant nusikaltimams elektronin je erdv je, teis saugos institucijoms b tina kaupiti žinias apie informacini sistem veikimo bei saugumo užtikrinimo principus, proced ras, darbo su kompiuterine informacija metodus bei kelti pa i teis saugos pareig n speciali j kvalifikacij ir kurti specialius padalinius kovai su kompiuteriniu nusikalstamumu, nes vienkartinis informatikos specialist ar ekspert traukimas tiriant bylas n ra pakankamai efektyvus ir negali užtikrinti mokslišškai pagr stos šios r šies nusikaltim tyrimo metodikos suformavimo.

## SANTRAUKA

Šiame darbe „Kompiuteriniai nusikaltimai ir jų tyrimo ypatumai“ nagrinėjamos baudžiamojo statymo numatytos visuomenei pavojingos veikos, daranios žalą visuomeniniams santykiams kompiuterinės informacijos tvarkymo srityje, jų mokslinio apibūdinimo, teisinio reglamentavimo raidos ir kriminalistinės charakteristikos bei tyrimo metodikos ypatumai.

Apibendrinus Lietuvos ir kitų valstybių patirtį bandant apibrėžti kompiuterinius nusikaltimų sąvoką, galima padaryti išvadą, jog šiuo metu nėra pasiekta vieningo sutarimo nei tarptautiniu, nei nacionaliniu mastu, tačiau nepaisant to, daugelis valstybių kriminalizavo didžiąją dalį veikų, kuriomis ksinamasi visuomeninius santykius kompiuterinės informacijos apdorojimo procese kaip nusikaltimo objektus.

Kompiuteriniai nusikaltimai, atsižvelgiant į pagrindinius struktūrinius elementus, technologijos savitumą (pasiksinimo dalyko – kompiuterinės informacijos – skaitmeninė forma, duomenų perdavimo tinklų panaudojimą ir kt.), yra atskira nusikaltimų rūšis, kuri ženkliai skiriasi nuo tradicinių nusikaltimų bei nėra tapati nusikaltimams elektroninėje erdvėje sąvokai, o kompiuteriniai nusikaltimai išskirtiniais savybėmis lygoja ir šiuos nusikaltimų tyrimo specifiku.

Kompiuteriniai nusikaltimai galima būtų apibrėžti kaip baudžiamojo statymo numatytą visuomenei pavojingą veiką, daranią žalą visuomeniniams santykiams automatizuotai tvarkant kompiuterinę informaciją, t.y. atliekant su ja bet kurį veiksmą – rinkimą, užrašymą, kaupimą, saugojimą, klasifikavimą, grupavimą, jungimą, keitimą (papildymą ar taisymą), teikimą, paskelbimą, naudojimą, logines ir (ar) aritmetines operacijas, paiešką, skleidimą, naikinimą ar kitokius veiksmus arba veiksmų rinkinį. Nusikaltimams elektroninėje erdvėje sąvoka yra platesnė, apimanti ir kompiuterinius nusikaltimus, ir kitas nusikalstamas veikas, susijusias ne tik su kompiuteriniu, bet ir su telekomunikacinių technologijų panaudojimu. Lietuvos Respublikos baudžiamajame kodekse terminas „kompiuterinis nusikaltimas“ nėra apibrėžtas, taigi jis oficialiai nėra teisintas *de jure*, tačiau kalbant apie veikas, susijusias su kompiuteriniais technologijomis bei elektronine erdve, dažniausiai vartojamas *de facto*. Vertinus kompiuterinius nusikaltimų teisinį reglamentavimą Lietuvoje, galima teigti, kad šiuo metu Lietuvos teisinė bazė pakankamai papildyta ir atnaujinta normomis, susijusiomis su kompiuterinių technologijų panaudojimu bei kompiuterinės informacijos sauga, o Baudžiamojo kodekso normos iš esmės atitinka Europos Tarybos Konvencijos dėl elektroninių nusikaltimų reikalavimus. Vis dėlto reikia pastebėti, jog didelė problema Lietuvoje lieka šios srities terminijos teisinis neapibrėžtumas.

Kompiuteriniai nusikaltimai kriminalistinė charakteristika, palyginus su kitais nusikaltimų rūšių charakteristika, pasižymi savitomis ypatybėmis. Kriminalistiniu požiūriu *asmenis, darančius kompiuterinius nusikaltimus*, pagal motyvaciją santykinai galima suskirstyti tris grupes:

silauž lius m g jus (*crackers*), profesionalius nusikalt lius (*criminals*) ir vandalus (*vandals*); pagal specializacij tokie asmenys skirstomi hakerius, krekerius, karderius ir frekerius (*hacker, cracker, carder, phracker*). Siekiant s kmingai iširti kompiuterinius nusikaltimus, b tina vertinti kompiuterin s informacijos, kaip *pasik sinimo dalyko*, išskirtines kriminalistines ypatybes: kompiuterin informacija palyginti paprastai ir greitai kei iama, kopijuojama, dauginama vairia technine ranga, siun iama vairiausiu atstumu, ribojamu tik elektronini ryši rangos veikimo plotu; paimant kompiuterin informacij (atliekant po m ), skirtingai nei material objekt (daikt ), ji išlieka pirminiame šaltinyje, nes prieig prie jos gali tur ti tuo pa iu metu keli asmenys. Kompiuterini nusikaltim *vykdymo b dai* nuolat tobul ja, j turinys gali b ti sudarytas iš vairiausi veiksm derini , priklausan i nuo pažeid jo kvalifikacijos, intelekto ir naudojamos rangos lygio. Ta iau, nepaisant kompiuterini nusikaltim *vykdymo b d* vairov s, juos galima sugrupuoti pagal metodus keturias grupes: 1) per mimo; 2) neteis tos prieigos; 3) manipuliacij ; 4) kompleksinius.

Tipin se kompiuterini nusikaltim tyrimo situacijose pagrindiniai *pirminiai tyrimo veiksmi* yra šie: vykio vietos apži ra; kompiuterin s rangos apži ra (paties kompiuterio ir kit rengini ), kompiuterin s informacijos laikmen apži ra, nusikalstamo poveikio jai p dsak paieška ir po mis, liudytoj apklausa, nukent jusiojo apklausa. Jei tariamasis nesulaikytas, greta min t pirmini tyrimo veiksm , b tina organizuoti jo paiešk , taip pat, pasitelkus nukent jus asmen ir specialistus, nustatyti nusikaltimo padarymo b do ypatybes. Jei asmuo sulaikomas nusikaltimo vietoje arba iš karto po nusikaltimo padarymo, atliekami šie pirminiai tyrimo veiksmi: sulaikyto asmens krata; sulaikyto asmens apklausa; sulaikyto asmens darbo ir gyvenamosios vietos krata. Kriminalistikos metodikos darbuose rekomenduojama kompiuterinio nusikaltimo vykio vietos apži r atlikti naudojant ekscentrin taktin b d („nuo centro – iki periferijos“), kur „centru“ (vykio vietos apži ros išeities tašku) laikoma konkreti kompiuterin ranga (arba kompiuterin s informacijos kaupiklis, laikmena), o kompiuterin s informacijos laikmen (dažniausiai kietojo disko, lanks i j disk , kompaktini disk ir kt.) apži r atlikti naudojant taktin b d „nuo bendro prie atskiro“.

Atsižvelgiant tai, jog tiriant kompiuterinius nusikaltimus nepakanka profesini teisini žini , tyr jui patariama pasitelkti informacini technologij specialist atliekant bet kur tyrimo veiksm . Vykdam kompiuterin s technin s bei programin s rangos apži r , krat ar po m , svarbu elgtis ypa atidžiai, atsižvelgti kompiuterin s informacijos saugojimo, p dsak sl pimo priemoni ir b d ypatybes, numatyti kaltininko priešišk veiksm bei kit faktori poveikio informacijai galimybes.

## SUMMARY

In this work „Computer crime and its investigative singularity“ we are analyzing the deeds, dangerous for society and predicted by criminal law, harmful for public relations in the field of the computer information regulation, their scientific description, legal regulation evolution and criminalistic characteristics and singularities of investigative methodology.

Summarizing the experience of the Lithuania and other countries in making efforts to define the notion of computer crime, we can make a conclusion, that for this moment there is no common agreement neither nationally, nor internationally, but, besides that, many countries criminalized most part of the deeds, that make inroads on public relations in the process of the computer information handling, as a crime object.

Computer crimes, due to their basic structure elements, individuality of technology (digital form of the infringement object – computer information, use of data transmission networks and etc.), are the separate kind of crimes, that signally differs from traditional crimes and also is not identical to the concept of the cyber space crime, and individual characteristics of the cyber crime determines its investigative particularity.

Computer crime can be described as a dangerous deed predicted by criminal law, harmful for public relations when automatic processing of the computer information is involved, i. e. making any action with it – collecting, writing, saving, storing, sorting, grouping, merging, changing (adding or correcting), presenting, publishing, using, making logical and (or) arithmetical operations, searching, sending, destroying or making any other action or set of actions. Concept of cyber space crime is more extensive and contains computer crimes and other criminal deeds, associated with usage not only of computer technology but also telecommunications. Criminal Code of Lithuanian Republic doesn't describe the term „computer crime“, so it isn't officially legitimated de jure, but, speaking about the deeds, related to computer technology and cyber space, this term is used de facto. Evaluating legal regulation of the computer crimes in Lithuania, we can state, that at this moment Lithuanian legal basis is renewed enough with the norms, related to usage of the computer technology and computer information security, and norms of the Criminal Code mainly matches to the requirements of the European Council Convention of the cyber crimes. Although, it must to be mentioned, that big problem in Lithuania remains the legal indetermination of the terms of this field.

Criminalistic characteristic of the computer crimes, comparing to the characteristic of the other kind of crimes, distinguishes with individual qualities. In criminalistic point of view, persons, who perform computer crimes, due to the motivation could be divided into three groups: crackers, criminals, vandals; according to their specialization such persons are divided into hackers,

crackers, carders and phrackers. For the successful investigation of the computer crime, it is necessary to determine the individual characteristics of the computer information as the subject of the infringement: computer information can be relatively simply and quickly copied, changed and duplicated with the different equipment types, sent in different distances, that are limited only by the working range of the communication equipment; when executing the seizure of the computer information, differently than concrete object, it remains on the primal source, because several persons can have access to it at the same time. The ways in which computer crimes are performed are constantly improved; their content could consist of the different sets of the actions, that depends only on the qualification, intellect of the criminal and level of used equipment. However, despite the variety of the way of making computer crimes, they can be grouped, due to the methodology, into four groups: 1) interception; 2) illegal access; 3) manipulation; 4) complex.

In typical situations of the investigations of the computer crimes primal investigations acts are: inspection of the crime scene; inspection of the computer equipment (computer itself and other equipment), inspection of computer information media, search and seizure of traces of the criminal effect to it, interview of the witness, interview of the aggrieved. If the suspect is not suspended, besides the primal investigative acts, it is necessary to arrange his search, also determine the ways of making crime, invoking in this process aggrieved person and specialists. If person is suspended at the crime scene or suddenly after the crime is made, the following primal investigative acts are performed: search of the suspended person; interview of the suspended person; search of suspended person's working and living places. Criminalistic methodology recommends to perform the inspection of the computer crime scene using eccentric tactical method (from center – to peripherals), where “center” (crime scene investigation starting point) is particular computer equipment (or computer information media, storage), and inspection of the computer information media (usually hard discs, floppy discs, compact discs and etc.) should be performed using tactical method “from common to particular”.

Seeing that for the investigation of the computer crimes having good professional juridical skills is not enough, it is recommended for the investigator to involve specialist of the information technology when performing any of investigative acts. Performing the inspection, search or seizure of the computer hardware and software, it is important to act especially closely, considering the qualities of the computer information storing, trace hiding tools and methods, predicting the possible influence of the hostile acts of the criminal and other factors to the information.

## LITERATŲ RAŠAS

### I. Teisės aktai ir teismų praktika

1. Lietuvos Respublikos Konstitucija // Valstybės žinios, 1992, Nr.33-1014.
2. Lietuvos Respublikos administracinis teisės pažeidimų kodeksas // Valstybės žinios, 1985, Nr.1-1; 2006, Nr. 119-4548.
3. Lietuvos Respublikos baudžiamasis kodeksas // Valstybės žinios, 2000, Nr. 89-2741.
4. Lietuvos Respublikos baudžiamojo proceso kodeksas // Valstybės žinios, 2002, Nr. 37-1341.
5. Lietuvos Respublikos asmens duomenų teisinis apsaugos statymas // Valstybės žinios, 1996, Nr. 63-1479; 2003, Nr. 15-597.
6. Lietuvos Respublikos autorių teisių ir gretutinių teisių statymas // Valstybės žinios, 1999, Nr. 50-1598.
7. Lietuvos Respublikos statymas „Dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis ratifikavimo“ // Valstybės žinios, 2001, Nr. 32-1055.
8. Lietuvos Respublikos statymas „Dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo“ // Valstybės žinios, 2004, Nr. 36-1178).
9. Lietuvos Respublikos statymas „Dėl Konvencijos dėl elektroninių nusikaltimų Papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veiksmų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo ratifikavimo“ // Valstybės žinios, 2006, Nr. 75-2848)
10. Lietuvos Respublikos elektroninių ryšių statymas // Valstybės žinios, 2004, Nr. 69-2382.
11. Lietuvos Respublikos mokymų statymas // Valstybės žinios, 1999, Nr. 97-2775; 2003, Nr. 61-2753.
12. Lietuvos Respublikos patentų statymas // Valstybės žinios, 1994, Nr. 8-120.
13. Lietuvos Respublikos teismo ekspertizės statymas // Valstybės žinios, 2002, Nr. 112-4969.
14. Lietuvos Respublikos valstybės ir tarnybos paslapčių statymas // Valstybės žinios, 1999, Nr. 105-3019; 2004, Nr. 4-29.
15. Lietuvos Respublikos valstybės registrų statymas // Valstybės žinios, 1996, Nr.86-2043; 2004, Nr. 124-4488.
16. Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimas Nr. 451 „Dėl Valstybės informacinės sistemos steigimo ir teisinimo taisykli patvirtinimo“ // Valstybės žinios, 2004, Nr. 58-2061.
17. Lietuvos Standartas LST ISO/IEC 2382-1: 1996. Informacijos technologija. Terminai ir apibrėžimai.
18. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS



Nr. 108) // Valstybės žinios, 2001, Nr. 32-1059.

19. Konvencija dėl elektroninių nusikaltimų // Valstybės žinios, 2004, Nr.36.

20. Europos Sąjungos Tarybos 2005 m. vasario 24 d. pamatinis sprendimas 2005/222/TVR dėl kovos prieš informacines sistemas // Official Journal L: 2005 03 16 Nr.69-67.

21. Europos Sąjungos Tarybos 2003 m. gruodžio 22 d. pamatinis sprendimas 2004/68/TVR dėl kovos su seksualiniu vaikų išnaudojimu ir vaikų pornografija // Official Journal L: 2004 01 20 Nr.13-44.

22. Europos Sąjungos Tarybos 2000 m. gegužės 29 d. sprendimas 2000/375/TVR dėl kovos su vaikų pornografija internete // Official Journal L: 2000 06 09 Nr.138-1

23. Europos Parlamento ir Tarybos sprendimas Nr.276/1999/EB, patvirtinantis daugiametį Bendrijos veiksmų planą dėl saugesnio naudojimosi internetu skatinimo kovojant su neteisėtu ir žalingu turiniu pasauliniuose tinkluose // Official Journal L: 1999 02 06 Nr.33-1

24. Europos Parlamento ir Tarybos 2003 m. birželio 16 d. sprendimas Nr.1151/2003/EB iš dalies pakeičiantis sprendimą Nr.276/1999/EB, patvirtinant daugiametį Bendrijos veiksmų planą dėl saugesnio naudojimosi internetu skatinimo kovojant su neteisėtu ir žalingu turiniu pasauliniuose tinkluose // Official Journal L: 2003 07 01 Nr.162-1.

25. Computer-related crime. Council of Europe. Recommendation No R(89)9, adopted by Committee of Ministers of the Council of Europe on 13 September 1989. Strasbourg, 1990.

26. Explanatory Memorandum related to Convention on Cyber-Crime // <http://conventions.coe.int/>.

27. Aukščiausiojo Teismo Senato 1998-12-22 nutarimas „Dėl teismų praktikos sukėlimo ir turto pasisavinimo arba iššvaistymo baudžiamosiose bylose (BK 274 ir 275 str.)“ // Teismų praktika, 1999, Nr. 10 – B2-8.

## II. Specialioji literatūra

28. Bylenchuk P.D. Organized transnational computer crime: the global problem of the new millennium // <http://www.crime-research.org/library/bileng.htm>.

29. Burda R. Kriminalistikos taktika. – Vilnius: Lietuvos teisės universitetas, 2001.

30. Burda R. Kompiuterinės rangos panaudojimas ekonominiams nusikaltimams (kai kurie kriminalistinės charakteristikos ir tyrimo metodikos ypatumai) // Jurisprudencija, 1999. T.12(4).

31. Burda R., Krikščiūnas R., Latauskienė E. ir kt. Kriminalistikos taktika ir metodika.- Vilnius: Lietuvos teisės universitetas, 2004.

32. Burda R., Gudmonas S. Modernios technologijos – modernūs nusikaltimai // Justitia, 1998, Nr.4.

33. Civilka M., Lamanauskas T., Osinait G. ir kt. Informacini technologij teis / Red. Sauli nas D./ – Vilnius: NVO Teis s institutas, 2004.
34. sna R., Šttilis D. Kompiuterin s informacijos ir elektronini dokument apsauga viešajame administravime. – Vilnius: Lietuvos teis s akademija, 2000.
35. Danisevi ius P., Kazlauskas M., Palskys E. Kriminalistika. - Vilnius, 1985.
36. Deringas A., Rinkevi ien Z., Sakalauskas L. Kompiuteriniais spausdintuvais išspausdint dokument kriminalistinis tyrimas // Kriminaline justicija: LTA mokslo darbai. - Vilnius, 1997. T.7-8.
37. Fisanick Ch. A., Csonka P., Docka P. ir kt. Šiuolaikinis nusikalstamumas. /Red. Klimas T./- Kaunas: Vytauto Didžiojo universitetas, 2002.
38. International review of penal law: computer crimes and other crimes against information technology. Wurzburg, Germany, 1992.
39. Jarukaitis I., Lamanauskas T., Civilka M. ir kt. Elektronini ryši teis .– Vilnius: Eugrimas, 2005.
40. Kligys V., Jankauskas V. Informacini technologij ekspertiz LTEC: dabartis ir perspektyva // Vilnius: Mykolo Romerio universitetas, 2005.
41. Kuklianskis S. Nusikaltim tyrimo organizavimo pradmenys. - Vilnius, 1995.
42. Lamanauskas T. Informacini technologij teis s kronika // Justitia, 2001, Nr. 4–5.
43. Lamanauskas T. Informacini technologij teis s naujienos // Justitia, 2001, Nr. 1-3.
44. Malevski H. vykio vietos apži ra. – Vilnius: Lietuvos teis s akademija, 1999.
45. Marcella A.J., Greenfield R.S. Cyber forensics. A Field Manual for Collecting, Examining and Preseving Evidence of Computer Crimes. - CRC Press LLC, 2002.
46. B.Middleton. Cyber crime investigator’s field guide. - CRC Press LLC, 2002.
47. Petrauskas R., Šttilis D. Kompiuteriniai nusikaltimai ir j prevencija. - Vilnius: Lietuvos teis s akademija, 2000.
48. Sabaliauskas G. Informacijos saugumas internete: teisinink ir informatik problema // Justitia, 2001, Nr. 1-2.
49. Sieber U. The international handbook of computer crime. // <http://www.jura.uni-wuerzburg.de/sieber/>.
50. Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime-study // <http://www.jura.uni-wuerzburg.de/sieber/>.
51. Tarptautini žodži žodynas. – Vilnius, 1985.
52. Teismo ekspertizi skyrimo klausimai. Informacinis laiškas. - Vilnius, 1996.
53. United Nations Manual on Computer-Related Crime. International Review of Criminal Policy Nos, 43/44, 1994 // <http://www.uncjin.org/documents/eightcongress.html>.



70. : c / .  
 . . , . . - :  
 , 2005.
71. . . , . . . . - Moc a: -  
 , 2006, . 1.
72. :  
 , . - Moc a, 2001, . 3.
73. . - //  
<http://www.melik.narod.ru>.
74. . .  
 . // , . , 1999. 4-5.
75. . . .  
 // <http://www.mte.ru/www/toim.nsf>.
76. . . // [http://www.aha.ru/~andrew\\_r/infolaw](http://www.aha.ru/~andrew_r/infolaw).
77. . . // . -  
 Moc a, 1993, 8.
78. A. . : - ,  
 . - , 1999.
79. ,  
 „ ( „  
 „, 20–21 1997 ) //  
<http://www.uic.ssu.samara.ru/~cclub/navigator/uglaw.htm>.
80. . .  
 « » // , . , 2000. 6.

### III. Interneto šaltiniai:

81. <http://cyber-crimes.ru>  
 82. <http://conventions.coe.int>  
 83. <http://europa.eu.int/eur-lex/lex/>  
 84. <http://litlex/litlex/ll.dll>  
 85. <http://securityfocus.com>  
 86. [http://www.aha.ru/~andrew\\_r/infolaw](http://www.aha.ru/~andrew_r/infolaw)  
 87. [http:// www.cybercellmumbai.com](http://www.cybercellmumbai.com)  
 88. [http:// www.cybercrime.gov](http://www.cybercrime.gov)  
 89. [http:// www.cybercrimelaw.org](http://www.cybercrimelaw.org)

90. <http://www.cybercrimelaw.net>
91. <http://www.cyberpolice.lt>
92. <http://www.crime-research.org>
93. <http://www.csirt-handbook.org.uk>
94. <http://www.esaugumas.lt>
95. <http://www.eweek.com>
96. <http://www.jura.uni-wuerzburg.de>
97. [http://www.likit.lt/?i=terminija/enciklopedinis\\_zodynas](http://www.likit.lt/?i=terminija/enciklopedinis_zodynas)
98. <http://www.ltec.lt>
99. <http://www.melik.narod.ru>
100. <http://www.mte.ru/www/toim.nsf>
101. <http://www.nplc.lt/stat/atask.htm#IRD-ataskaitos>
102. <http://www.uic.ssu.samara.ru>
103. <http://www.uncjin.org>
104. [http://www.vrm.lt/fileadmin/Image\\_Archive/IRD/Statistika/index2.phtml?id=198](http://www.vrm.lt/fileadmin/Image_Archive/IRD/Statistika/index2.phtml?id=198)
105. [http://www3.lrs.lt/dokpaieska/forma\\_1.htm](http://www3.lrs.lt/dokpaieska/forma_1.htm)
106. [http://www3.lrs.lt/pls/inter1/dokpaieska.forma\\_1](http://www3.lrs.lt/pls/inter1/dokpaieska.forma_1)