MYKOLO ROMERIO UNIVERSITETO
TEISĖS FAKULTETO
KRIMINALISTIKOS KATEDRA

RENATA KAČINSKAITĖ

NEAKIVAIZDINIŲ STUDIJŲ
BAUDŽIAMOSIOS TEISĖS IR KRIMINOLOGIJOS PROGRAMA

TEMA

KOMPIUTERINIAI NUSIKALTIMAI IR JŲ TYRIMO YPATUMAI

Magistro baigiamasis darbas

Darbo vadovas – doc. dr.
Ryšardas Burda

Vilnius, 2006

TURINYS

ĮVADAS

Pasaulio valstybėms sukūrus globalų kompiuterinį tinklą ir vieningą informacinę erdvę, kompiuterinis nusikalstamumas taip pat įgavo tarptautinį pobūdį, nes modernių informacinių bei telekomunikacinių technologijų teikiamos galimybės – muitinės procedūrų ir kitų teisinių apribojimų praktiškai nevaržomas duomenų srautų judėjimas, informacijos mainų greitis ir anonimiškumas – aktyviai naudojamos tiek teisėtais, tiek neteisėtais tikslais. Įvertinusi šias aplinkybes, Lietuvos Respublika, kurianti informacinei visuomenei egzistuoti būtiną infrastruktūrą, integruotą į globalius tinklus, turėtų pasirengti sparčiai kintančioms asmens ir visuomenės bendravimo formoms, naujiems socialinio ir ekonominio gyvenimo organizavimo būdams, o kartu ir naujai nusikaltimų rūšiai, susijusiai su informacinių technologijų panaudojimu, automatiniu kompiuterinių 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 kėsinamasi į visuomeninius santykius kompiuterinės informacijos apdorojimo procese ir kompiuterinės informacijos saugumą, bazė, tačiau didele problema, manome, lieka šios srities terminologijos teisinis neapibrėžtumas, be to, dar nėra parengtos kompiuterinių nusikaltimų tyrimo metodikos, pagrįstos susistemintomis teorinėmis žiniomis ir patikrintos praktikoje. Tikėtina, jog tai sąlygoja teisės teoretikų ir praktikų nuomonių dėl kompiuterinių nusikaltimų ir jų tyrimo metodų įvairovė bei vieningos pozicijos stygius.

Atsižvelgiant į minėtų problemų aktualumą bei praktinę patirtį dirbant teisinį darbą informacijos saugos ir elektroninių ryšių srityje, autorės buvo pasirinktas baigiamojo magistro darbo **tyrimo objektas** – baudžiamojo įstatymo numatytos visuomenei pavojingos veikos, darančios žalą visuomeniniams santykiams kompiuterinės informacijos tvarkymo srityje.

Šio darbo **tyrimo dalykas** – baudžiamojo įstatymo numatytų visuomenei pavojingų veikų, darančių žalą visuomeniniams santykiams kompiuterinės informacijos tvarkymo srityje, mokslinio apibūdinimo, teisinio reglamentavimo raidos ir kriminalistinės charakteristikos bei tyrimo metodikos ypatumai.

Pradedant tyrimą, autorės iškeliama **hipotezė,** jog kompiuteriniai nusikaltimai, atsižvelgiant į jų pagrindinių struktūrinių elementų, technologijos savitumą (pasikėsinimo dalyko skaitmeninę formą, automatizaciją, duomenų perdavimo tinklų panaudojimą), yra atskira nusikaltimų rūšis, kuri ženkliai skiriasi nuo tradicinių nusikaltimų bei nėra tapati nusikaltimų elektroninėje erdvėje sąvokai, o kompiuterinių nusikaltimų išskirtinės savybės sąlygoja ir šių nusikaltimų tyrimo ypatumus.

Taigi baigiamojo magistro **darbo tikslas** – išanalizavus mūsų valstybės ir tarptautinę praktiką teorine mokslo doktrinos bei praktine teisėkūros ir teisėsaugos institucijų veiklos prasme, apibrėžti modernios nusikaltimų rūšies – kompiuterinių nusikaltimų – sampratą bei nustatyti esminius jų tyrimo ypatumus. Pagrindiniai šio **darbo uždaviniai**, siekiant nurodyto tikslo, yra tokie: atlikti Lietuvos ir Europos Sąjungos bei kitų šalių patirties kompiuterinių nusikaltimų teisinio reglamentavimo srityje analizę, apibūdinti kompiuterinių nusikaltimų savybes, rūšis bei pateikti baudžiamąją teisinę ir kriminalistinę jų charakteristiką, taip pat išanalizuoti kompiuterinių nusikaltimų tyrimo metodikos specifiką, nustatyti tyrimo veiksmų bendruosius ir specialiuosius reikalavimus bei pateikti rekomendacijas, kaip išvengti esminių šios rūšies nusikaltimų tyrimo klaidų, kurios galėtų sąlygoti kompiuterinės informacijos praradimą ar sugadinimą, rasti ir tinkamai užfiksuoti Įkalčius, turinčius Įrodomąją vertę teisminio bylos nagrinėjimo metu.

Rašant darbą, vertinant surinktą medžiagą ir darant išvadas, naudoti teoriniai bei empiriniai **tyrimo metodai**: lyginamasis, lyginamasis istorinis, analitinis, apibendrinimo, dedukcinis, statistinis, dokumentų analizės, profesinės patirties apibendrinimo ir kiti. Statistiniai duomenys, kurių analizę atliko autorė, pateikti iš Vidaus reikalų ministerijos Nusikalstamų veikų žinybinio registro bei Įtariamų, kaltinamų ir teistų asmenų žinybinio registro. Siekiant gauti praktinių duomenų apie kompiuterinių nusikaltimų tyrimo ir informacinių sistemų saugos ypatumus bei problemas, Įvertinti surinktą teorinę medžiagą bei pagrĮsti išvadas, buvo apibendrinta ikiteisminio tyrimo Įstaigų pareigūnų, taip pat Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos informacijos saugos specialistų profesinė patirtis.

Šio darbo pagrindinė dėstomoji dalis **susideda iš trijų skyrių**, suskirstytų Į poskyrius: pirmajame skyriuje „*Kompiuterinių nusikaltimų samprata ir teisinis reglamentavimas*“ nagrinėjama nusikalstamų veikų, susijusių su kompiuterinėmis technologijomis bei informacijos saugos pažeidimu, apibrėžimo problemos, kompiuterinio nusikaltimo sampratos ypatybės ir raida, kompiuterinių nusikaltimų rūšys ir klasifikacija, šių nusikaltimų teisinio reglamentavimo Europos Sąjungos valstybėse ir Lietuvoje pagrindiniai bruožai; antrajame skyriuje „*Kompiuterinių nusikaltimų apibūdinimo kriminalistiniai aspektai*“ pateikiama kompiuterinių nusikaltimų kriminalistinė charakteristika, analizuojami kompiuterinių nusikaltimų subjekto, Įvykdymo laiko, vietos ir būdų, taip pat prietaisų ir priemonių būdingi bruožai; trečiajame skyriuje „*Kompiuterinių nusikaltimų tyrimo metodikos ypatumai*“ apibūdinama šių nusikaltimų tyrimo metodika, nagrinėjama kompiuterinių nusikaltimų Įrodinėtinos aplinkybės, tipinės tyrimo situacijos ir kriminalistinės tyrimo užduotys, atskirų tyrimo veiksmų atlikimo bendrieji ir specialieji reikalavimai, akcentuojama specialiųjų žinių panaudojimo ir ekspertizės skyrimo svarba ir ypatumai, analizuojamos pagrindinės kompiuterinių nusikaltimų tyrimo klaidos. Darbo pabaigoje pateikiamos išvados ir rekomendacijos, pagrĮstos atlikto tyrimo rezultatais.

I. KOMPIUTERINIŲ NUSIKALTIMŲ SAMPRATA IR TEISINIS REGLAMENTAVIMAS

1. KOMPIUTERINIO NUSIKALTIMO SAMPRATA

Įvertinus Lietuvos bei tarptautinę praktiką tiek teorine mokslo darbų, tiek praktine Įstatymų leidybos prasme, galima konstatuoti, kad šiuo metu nėra suformuota vieninga kompiuterinio nusikaltimo samprata. Tiesa, siekiant Įvardinti visuomenei pavojingas bei teisės aktų draudžiamas veikas, vykdomas panaudojant kompiuterius, jų tinklus ar kompiuterizuotas informacines sistemas (toliau – informacinės sistemos), paprastai vartojamas kompiuterinio nusikaltimo terminas *(angl. computer crime, rus. компьютерное преступление)*, tačiau dažnai sutinkami ir kiti terminai: kompiuterių naudojimo arba su kompiuterių naudojimu susijęs nusikaltimas *(angl. computer-related crime)*, elektroninis arba kibernetinis nusikaltimas *(angl. cyber crime)*, informacinis nusikaltimas ar nusikaltimas informatikai *(pranc. delit informatique)*, informacinės visuomenės nusikaltimas ir kt.

Teisės darbuose minima, kad kompiuterinio nusikaltimo terminas pirmą kartą buvo pavartotas maždaug septintajame praėjusio amžiaus dešimtmetyje Jungtinių Amerikos Valstijų (toliau – JAV) mokslinėje literatūroje. Vėliau šis terminas paplito ir kitų šalių praktikoje.

Galima pagrĮstai teigti, jog teisiškai tikslingiausia būtų kompiuterinio nusikaltimo sąvoką apibrėžti baudžiamosios teisės požiūriu. Baudžiamosios teisės požiūriu kompiuterinius nusikaltimus reikėtų suprasti kaip baudžiamojo Įstatymo numatytą visuomenei pavojingą veiką, kuria kėsinamasi Į visuomeninius santykius informacijos apdorojimo procese ir kompiuterinės informacijos saugumą kaip nusikaltimo objektą, o nusikaltimo dalykas arba Įrankis būtų kompiuterinė informacija, kompiuteris, kompiuterinis tinklas arba informacinė sistema.

Išanalizavus Europos Sąjungos, JAV, Rusijos ir kitų valstybių mokslo darbuose pateiktą kompiuterinių nusikaltimų sampratų Įvairovę, galima išskirti dvi pagrindines požiūrio Į šiuos nusikaltimus kryptis: kompiuterinių nusikaltimų traktavimas plačiąja prasme ir siaurąja prasme.

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

a) nusikaltimo dalykas yra kompiuterinė informacija (ar pats kompiuteris) arba

b) nusikaltimo priemonė (Įrankis) yra kompiuteris. Reikia atkreipti dėmesĮ Į tai, kad pastaruoju atveju veikų objektas gali būti skirtingas, vadinasi prie jų gali būti priskirtas ir autorių teisių pažeidimas, ir sukčiavimas, jei jie Įvykdyti panaudojant kompiuterius. O atsižvelgiant Į dalyko platų traktavimą, kompiuteriniu nusikaltimu bus laikoma ir kompiuterio vagystė.

Kompiuterinių nusikaltimų sąvoką plačiąja prasme aiškina Vokietijos ir Austrijos

baudžiamosios teisės teoretikai, kurie apibrėžia kompiuterinius nusikaltimus kaip baudžiamąją veiką, kurią vykdant kompiuteris yra jos priemonė (instrumentas) arba objektas[1].

Vienas iš plačiausių traktavimo pavyzdžių yra su kompiuteriais susijusių nusikaltimų *(angl. computer-related crime)* terminas, apimantis visas kriminalizuotas veikas, kurioms Įvykdyti panaudojamas kompiuteris, informacinė sistema ar elektroninė erdvė (pvz., tikrovės neatitinkančių, asmens garbę ir orumą žeminančių duomenų skleidimas internete).

Atkreiptinas dėmesys Į tai, kad šiuo metu vis populiaresnis ir plačiai naudojamas elektroninių nusikaltimų *(angl. cybercrime)* terminas paprastai atitinka kompiuterinių nusikaltimų sampratą plačiąja 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[2]. Vis dėlto būtina pastebėti, jog Europos Komisijos komunikate Tarybai ir Europos Parlamentui (COM (2000) 890 final) bei Konvencijos dėl elektroninių nusikaltimų paaiškinamajame memorandume[3] vartojamas elektroninių nusikaltimų terminas ir nurodoma, jog Konvencijoje yra kriminalizuojamos veikos, susijusios su kompiuteriniais nusikaltimais, taigi elektroninius nusikaltimus galima būtų traktuoti kaip kompiuterinius nusikaltimus plačiąja prasme, vykdomus panaudojant elektroninę erdvę.

Antrosios krypties atstovai, aiškinantys kompiuterinių nusikaltimų sąvoką siaurąja prasme, kompiuteriniams nusikaltimams priskiria tik tokias baudžiamojo Įstatymo nustatytas visuomenei pavojingas veikas, kurios atitinka du kriterijus:

a) šios veikos yra nurodytos specialiuose baudžiamojo Įstatymo 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.

Įvertinus užsienio valstybių bei Lietuvos Įstatymų leidybos praktiką, galima daryti išvadą, jog šiuo metu vyrauja kompiuterinių nusikaltimų samprata siaurąja prasme.

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

[1] International review of penal law: computer crimes and other crimes against information technology.- Wurzburg, Germany, 1992. P.133.
[2] Civilka M., Lamanauskas T., Osinaitė G. ir kt. Informacinių technologijų teisė.- Vilnius, 2005. P.511.
[3] 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 tarptautinį standartą 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 kompiuterinę techninę, programinę įrangą arba duomenis“[4]. Nepaisant šio termino apibrėžimo, Lietuvos Įstatymų leidėjo valia naujajame Baudžiamajame kodekse kompiuteriniai nusikaltimai įvardijami kaip „nusikaltimai informatikai“ (BK XXX skyrius „Nusikaltimai informatikai“: 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 įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti). Reikia pastebėti, jog „nusikaltimų informatikai“ terminas nevienareikšmiškai sutiktas Lietuvos teisės specialistų. Tarkime, šį terminą kritiškai vertina dr. D.Štitilis, S.Toliušis leidinyje „Informacinių technologijų teisė“[5]. Galima konstatuoti, kad tiek pats terminas „nusikaltimas informatikai“, tiek šio Baudžiamojo kodekso skyriaus pavadinimas nėra tikslūs, nes šių nusikaltimų rūšinis objektas – informatika – Tarptautinių žodžių žodyne[6] pirmiausia apibrėžiama kaip mokslo šaka ar tam tikra žinių visuma, o kompiuteriniais nusikaltimais ne tik nesiekiama kėsintis į mokslo žinių visumą, bet priešingai naudojamasi informatikos mokslo žiniomis kaip priemone nusikaltimams daryti. Reikia pastebėti, kad Lietuvos Įstatymų leidėjas „informatikos“ terminą traktavo plačiąja prasme kaip su informatikos mokslu susijusią praktinę veiklą, tuomet BAUDŽIAMOJO KODEKSO saugoma vertybė galėtų būti aiškinama kaip saugus ir netrukdomas kompiuterinės informacijos tvarkymas, kompiuterių tinklo ar informacinės sistemos valdymas ir kontrolė. Taigi, nusikaltimai informatikai galėtų būti įvardinti kaip nusikaltimai kompiuterinės informacijos saugumui**,** nes vertybė, į kurią kėsinamasi šiais nusikaltimais, yra teisės aktų ginamas informacijos saugumas.

R.Petrausko ir D.Štitilio leidinyje „Kompiuteriniai nusikaltimai ir jų prevencija“ pateikiamas kompiuterinio nusikaltimo apibrėžimas, suformuluotas baudžiamosios teisės požiūriu: „kompiuterinis nusikaltimas - tai baudžiamojo įstatymo numatyta visuomenei pavojinga veika, daranti žalą visuomeniniams santykiams, saugant, vartojant ir platinant kompiuterinę informaciją“[7].

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

[4] Lietuvos Standartas LST ISO/IEC 2382-1: 1996. Informacijos technologija. Terminai ir apibrėžimai. D.1. P.21.
[5] Civilka M., Lamanauskas T., Osinaitė G. ir kt. Informacinių technologijų teisė.- Vilnius, 2005. P.528.
[6] Tarptautinių žodžių žodynas.- Vilnius, 1985. P.213.
[7] Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija.- Vilnius, 2000. P.7.

duomenų tvarkymo sąvokos, analogiją, galima būtų patikslinti minėtą apibrėžimą ir išdėstyti jį taip: kompiuterinis nusikaltimas – tai baudžiamojo įstatymo numatyta visuomenei pavojinga veika, daranti žalą visuomeniniams santykiams, 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 kitokį veiksmą arba veiksmų rinkinį.

Lietuvos rytų kaimynių – Rusijos, Baltarusijos, Ukrainos – baudžiamosios teisės teoretikai tai pat susiskirstę į dvi grupes, tačiau vis dėlto didesnė jų dalis kompiuterinių nusikaltimų sąvoką aiškina siaurąja prasme ir apibrėžia šiuos nusikaltimus kaip veikas:

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

b) kurioms būdingas bendras pasikėsinimo objektas – visuomeniniai santykiai, susiję su saugiu automatizuotu informacijos apdorojimu.

Šios nuostatos laikosi V.S.Komisarovas, B.V.Zdravomislovas, V.B.Čechovas. Pavyzdžiui, V.S.Komisarovas teigia, jog kompiuteriniai nusikaltimai – tai „tyčinės visuomenei pavojingos veikos (veikimas ar neveikimas), darančios žalą ar sukeliančios grėsmę visuomeniniams santykiams, susijusiems su saugiu informacijos ar informacijos resursų kūrimu, naudojimu, platinimu ar jų apsauga“[8]. Minėti mokslininkai pabrėžia, kad kompiuteriniais nusikaltimais vadintinos tos veikos, kurios numatytos baudžiamojo įstatymo ir pažeidžia asmenų teisėtus interesus, susijusius su automatizuotu duomenų apdorojimu.

Tačiau yra ir tokių baudžiamosios teisės specialistų, kurie kompiuterinių nusikaltimų sąvoką aiškina plačiąja prasme, pavyzdžiui I.A.Voronovas, P.D.Bylenčiukas, M.Dutovas. P.D.Bylenčiuko teigimu, kompiuterinių nusikaltimų grupei priskirtinos visos neteisėtos veikos, kuriomis kėsintasi į elektroninės informacijos tvarkymą kaip objektą ir kurios įvykdytos elektroninio informacijos tvarkymo dėka, vadinasi kompiuteriniais nusikaltimais laikomas ir sukčiavimas, pasinaudojant magnetinėmis kortelėmis, sukčiavimas, susijęs su mokėjimais už tarptautinius pokalbius bei kiti nusikaltimai telekomunikacijų sferoje, neteisėtas elektroninių mokėjimų tinklo naudojimas, neteisėtas programinės įrangos naudojimą ir kt.[9] I.A.Voronovas kompiuterinius nusikaltimus apibrėžia kaip visus neteisėtus veiksmus, vykdomus pasitelkus skaičiavimo techniką ir telekomunikacijų priemones, kurių objektas yra informaciniai santykiai[10]. A.V.Sorokinas pabrėžia, kad kalbant apie kompiuterinius nusikaltimus, reikėtų skirti dvi jų grupes,

---

[8] Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность // Юридический мир, 1998. Стр.13.

[9] 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.

[10] Воронов И.А. Некоторые проблемы действующего законодательства по вопросам уголовной ответственности за преступления в сфере использования электронно-вычислительных машин // http://www.crime-research.org/ library/voron.htm; prisijungimo laikas: 2006-05-02.

t.y. nusikaltimus, susijusius su neteisėtu kompiuterių darbo trikdymu, ir nusikaltimus, kuriems Įvykdyti naudojami kompiuteriai kaip būtina priemonė, taigi šiuo atveju kompiuteriniams nusikaltimams priskiriamos visos neteisėtos veikos, vykdomos panaudojant kompiuterĮ (pvz., dokumentų klastojimas, sukčiavimas ir kt.)[11] .

J.M.Baturino teigimu, dauguma tradicinių nusikaltimų rūšių modifikavosi dėl skaičiavimo technikos panaudojimo jiems Įvykdyti, vadinasi tikslinga kalbėti tik apie nusikaltimų kompiuterinius aspektus, neišskiriant šių nusikaltimų kaip rūšies, nes teisiniu požiūriu kompiuterinių nusikaltimų negali būti[12]. Prieš kompiuterinių nusikaltimų termino vartojimą pasisako ir V.V.Krilovas, kurio manymu tinkamesnis yra informacinių nusikaltimų terminas, nes Rusijos baudžiamajame kodekse išskirti Į atskirą skirsnĮ nusikaltimai kompiuterinės informacijos srityje yra tik informacinių nusikaltimų dalis, kurią jungia kompiuteris kaip bendra informacijos apdorojimo priemonė[13].

Kaip jau buvo minėta, kompiuterinio nusikaltimo sąvoka pirmiausia buvo pavartota JAV mokslinėje literatūroje. D.Parkerio teigimu, kompiuterinis nusikaltimas – tai visos tyčinės veikos, susijusios su kompiuteriais, dėl kurių nukentėjusysis patyrė ar galėjo patirti žalą, o nusikaltimo subjektas turėjo ar galėjo gauti iš to naudos. Bet toks apibrėžimas, viena vertus, labai išplečia kompiuterinių nusikaltimų ratą ir apima paprastą kompiuterio vagystę, o kita vertus, nėra pakankamai išsamus, nes neapima veikų, padarytų dėl neatsargumo arba nesiekiant naudos. Vis dėlto galima konstatuoti, jog JAV baudžiamosios teisės darbuose vyrauja kompiuterinių nusikaltimų sampratos aiškinimas plačiąja prasme, t.y. kompiuterinis nusikaltimas apibrėžiamas kaip bet koks baudžiamosios teisės pažeidimas, kuriam padaryti arba ištirti naudojamos kompiuterinių technologijų žinios[14], nors tokiu atveju dalis tradicinių nusikaltimų būtų Įtraukti Į kompiuterinių nusikaltimų kategoriją, jei jų tyrimui būtų naudojamos kompiuterinės technikos žinios.

Atsižvelgdama Į kompiuterinio nusikaltimo sąvokos traktavimo prieštaravimus bei tarptautinės bendruomenės susirūpinimą sparčiai plintančiais moderniais nusikaltimais, susijusiais su neteisėtu elektroninės erdvės panaudojimu, 1983 m. Ekonominio bendradarbiavimo ir plėtros organizacija (OECD, liet. EBPO) sudarė ekspertų komitetą kompiuterinių nusikaltimų teisinio vertinimo problemoms spręsti. EBPO ataskaitoje kompiuterinis nusikaltimas buvo apibrėžtas kaip bet koks neteisėtas, neetiškas arba nesankcionuotas elgesys, susijęs su automatiniu kompiuterinių

---

[11] Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика расскрытия и расследования.- Курган, 1999. Стр.11.
[12] Воронов И.А. Понятие преступлений в сфере высоких технологий // http://www.crime-research.org/library/cyberpon.htm; prisijungimo laikas: 2006-05-02.
[13] там же.
[14] American Criminal Law Review.- Georgetown university law center, 1998. P.505.

duomenų apdorojimu ir siuntimu, tačiau nebuvo nurodyta, kokios teisės šakos atžvilgiu toks elgesys yra neteisėtas[15].

1989 m. Europos Tarybos Nusikaltimų tyrimo komitetas nagrinėjo baudžiamosios teisės problemas, susijusias su kompiuteriniais nusikaltimais, tačiau buvo nutarta kompiuterinių nusikaltimų sąvokos nereglamentuoti, tokiu būdu paliekant Europos Sąjungos valstybėms narėms sąlyginę laisvę kriminalizuoti šios srities veikas, atsižvelgiant Į teisinės sistemos ypatumus bei istorines tradicijas.

Atsižvelgiant Į kompiuterinio nusikaltimo sąvokos traktavimo prieštaravimus, 1994 m. Kriminalinės policijos tarptautinėje apžvalgoje kompiuterinių nusikaltimų srityje teigiama, jog terminai „kompiuterinis nusikaltimas“ ir „nusikaltimas, susijęs su kompiuteriais“ bus vartojami, kalbant tiek apie tradicinius nusikaltimus (sukčiavimas, klastojimas, vagystė ir kt.), tiek apie moderniuosius nusikaltimus (neteisėta prieiga ir kt.)[16].

Apibendrinus Įvairių valstybių patirtĮ bandant apibrėžti kompiuterinių 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 kėsinamasi Į visuomeninius santykius informacijos apdorojimo procese ir kompiuterinės informacijos saugumą kaip nusikaltimo objektą.

Įvertinus užsienio valstybių bei Lietuvos Įstatymų leidybos praktiką, galima daryti išvadą, jog šiuo metu vyrauja kompiuterinių nusikaltimų samprata siaurąja prasme. Taigi, kompiuterinĮ nusikaltimą galima būtų apibrėžti kaip baudžiamojo Įstatymo numatytą visuomenei pavojinga veiką, darančią 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 kitokĮ veiksmą arba veiksmų rinkinĮ.

[15] Sieber U. The international handbook of computer crime. 1986.
[16] 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. KOMPIUTERINIŲ NUSIKALTIMŲ KLASIFIKACIJA IR RŪŠYS

Baudžiamosios teisės ir kriminalistikos mokslo darbuose galima aptikti įvairių kompiuterinių nusikaltimų klasifikacijų, kurios paremtos skirtingais klasifikavimo kriterijais. Įvertinus mokslinės doktrinos pateiktą klasifikacijų įvairovę, galima sąlyginai išskirti keturias dideles jų grupes: pirmajai grupei priklausytų tų autorių klasifikacijos, kurių pagrindas – nusikaltimų įvykdymo būdas, antrajai grupei galima būtų priskirti klasifikacijas, sudarytas atsižvelgiant į kompiuterio panaudojimo pobūdį vykdant nusikaltimą, trečiajai atstovautų autoriai, klasifikuojantys kompiuterinius nusikaltimus pagal poveikį kompiuterinei informacijai, o ketvirtajai grupei priklausytų klasifikacijos, kurių pagrindas – baudžiamųjų įstatymų saugomas interesas.

Dažniausiai kompiuteriniai nusikaltimai klasifikuojami pagal jų įvykdymo būdą. Pavyzdžiui, J.M.Baturinas[17], apibendrinęs tipinius kompiuterinių nusikaltimų įvykdymo būdus, išskyrė tris pagrindines kompiuterinių nusikaltimų rūšis:

1. Kompiuteriniai nusikaltimai, vykdomi neteisėto perėmimo būdais (metodais);
2. Kompiuteriniai nusikaltimai, vykdomi neteisėtos prieigos būdais (metodais);
3. Kompiuteriniai nusikaltimai, vykdomi manipuliacijos būdais (metodais).

Kita dalis mokslininkų klasifikuoja kompiuterinius nusikaltimus, atsižvelgdami į kompiuterio panaudojimo pobūdį vykdant nusikaltimą. Remdamasis šiuo kriterijumi, Markas Ekenvaileris[18] pasiūlė suskirstyti kompiuterinius nusikaltimus į tris pagrindines grupes, kurios, savo ruožtu, toliau suskirstomos į pogrupius:

1. Kompiuteriniai nusikaltimai, kai kompiuteris ar kitas elektroninis įrenginys yra teisės pažeidimo *objektas*, o nusikaltėlio tikslas – pagrobti įrangą, informaciją arba pakenkti ar kitaip neteisėtai paveikti informacinę sistemą:

kompiuterinės įrangos pasisavinimas (šiai grupei priklauso tradiciniai įprastų nusikaltimų rūšių įvykdymo būdai, kai nusikaltėlis siekia pasisavinti svetimą turtą);

informacijos pagrobimas;

paslaugų pagrobimas (neteisėtos prieigos prie sistemos gavimas, siekiant neatlygintinai pasinaudoti jos teikiamomis paslaugomis);

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

“pėdsakų slėpimas” (šiai grupei priklauso nusikaltimai, vykdomi siekiant paslėpti savo

---

[17] Батурин Ю.М. Проблемы компьютерного права.- Москва: Юриздат, 1991.

[18] Экенвайлер М. Преступная деятельность, совершаемая с использованием режима «онлайн» (Тезисы докладов на международной конференции «Проблемы борьбы с новыми видами экономических преступлений в России и США», 20–21 мая 1997 года). // http://www.uic.ssu.samara.ru/~cclub/navigator/uglaw.htm; prisijungimo laikas: 2006-05-01.

vardą ir buvimo vietą).

2. Kompiuteriniai nusikaltimai, kai kompiuteris naudojamas kaip nusikaltimo Įvykdymo *priemonė*:

tradicinių nusikaltimų Įvykdymo priemonė (pvz., sukčiavimo, klastojimo);

kompiuterinių nusikaltimų Įvykdymo priemonė (neteisėto poveikio kitam kompiuteriui ar sistemai priemonė).

3. Kompiuteriniai nusikaltimai, kai kompiuteris naudojamas kaip *atminties Įrenginys* (pvz., po Įsilaužimo Į sistemą yra sukuriamas specialūs failų katalogai, skirti nusikaltėlio programinėms priemonėms, sistemos slaptažodžiams, pavogtų kreditinių kortelių numeriams ar kt. saugoti). Reikia pastebėti, kad šios nusikaltimų grupės išskyrimas kelia abejonių, nes jei kompiuteris panaudojamas kaip atminties Įrenginys, t.y. nusikaltimo Įvykdymo priemonė, tai pats nusikaltimas galėtų būti priskirtas antrajai grupei.

Atkreiptinas dėmesys Į klasifikacijas, pagrĮstas poveikio kompiuterinei informacijai kriterijumi. Tokios klasifikacijos pavyzdžiu galėtų būti pakankamai išsami V.A.Meščeriakovo kompiuterinių nusikaltimų klasifikacija[19], suskirstanti neteisėtas veikas Į penkias pagrindines grupes ir pogrupius :

1. Neteisėtas informacijos užvaldymas (Įsigijimas) arba išskirtinių naudojimosi ja teisių pažeidimas:

neteisėtas informacijos kaip duomenų, dokumentų visumos užvaldymas (išskirtinių valdymo teisių pažeidimas);

neteisėtas informacijos kaip prekės užvaldymas;

neteisėtas informacijos kaip idėjos (algoritmo, uždavinio sprendimo būdo) užvaldymas.

2. Neteisėtas informacijos pakeitimas:

neteisėtas informacijos kaip duomenų visumos pakeitimas;

neteisėtas informacijos kaip idėjos pakeitimas ir pristatymas kaip savo nuosavybės (algoritmo pakeitimas);

neteisėtas informacijos kaip prekės pakeitimas, siekiant pasinaudoti jos naudingomis savybėmis (apsaugos pašalinimas).

3. Neteisėtas informacijos sunaikinimas:

informacijos kaip duomenų visumos sunaikinimas;

informacijos kaip prekės sugadinimas.

4. Neteisėtas informacijos sukūrimas (veikos, sukuriant (generuojant) informaciją su

[19] Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации. //Конфидент, С.Петербург, 1999, N°4–5.

nustatytomis savybėmis):

informacijos, darančios žalą valstybei, visuomenei ar asmeniui, platinimas informacinių tinklų telekomunikaciniais kanalais;

kompiuterinių virusų ir kitų kenkėjiškų programų kūrimas ir platinimas;

nusikalstamas neatsakingumas kuriant programinę Įrangą, algoritmą pažeidžiant nustatytas technines normas ir taisykles.

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

neteisėtas automatizuotų sistemų resursų panaudojimas (atminties, laiko ir kt.);

informacinis telekomunikacinių tinklų mazgų blokavimas (melagingų iškvietimų srauto sukūrimas).

U.Sieberio kompiuterinių nusikaltimų klasifikacija parengta atsižvelgiant Į baudžiamojo Įstatymo saugomus interesus[20]:

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

Įstatymai, saugantys minėtus interesus, paprastai skirstomi Į ekonominių interesų apsaugos; privatumo apsaugos; intelektinės nuosavybės teisių apsaugos; apsaugos nuo nelegalaus ir žeidžiančio turinio informacijos.

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

1) kompiuterinis Įsilaužimas ar Įsibrovimas *(hacking)*;
2) kompiuterinis šnipinėjimas *(espionage)*;
3) programinės Įrangos ir kitoks piratavimas;
4) kompiuterinis sabotažas *(sabotage)*;
5) kompiuterinis prievartavimas *(extortion)*;
6) kompiuterinis sukčiavimas *(fraud)*.

Privatumo pažeidimai. Mokslo darbuose asmens privatumo pažeidimai dažniausiai skirstomi Į dvi rūšis:

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

Būtina paminėti, jog ne už visus privatumo pažeidimus numatoma baudžiamoji

[20] 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. Neteisėtos veikos, susijusios su informacijos privatumo pažeidimu:

1) susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimas;

2) neteisėtas informacijos apie privatų asmens gyvenimą rinkimas;

3) neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas.

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

1) autorių teisių pažeidimai;

2) gretutinių teisių pažeidimai.

Pastebėtina, kad intelektinės nuosavybės teisių pažeidimai yra ekonominio pobūdžio. Šie nusikaltimai yra labai paplitę elektroninėje erdvėje, nes programinės Įrangos, muzikos, literatūros, fotografijos ir kitus kūrinius lengva kopijuoti ir platinti, todėl autorių ir gretutinių teisių saugomų intelektinių kūrinių atgaminimas bei platinimas be teisės aktų nustatyto leidimo internete pasitaiko ypač dažnai.

Neteisėto turiniu 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 Įranga. Neteisėto turinio informacijos skleidimas internete sparčiai plinta, tai lemia elektroninės erdvės 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 teisėtvarkos ir teisėsaugos institucijų darbą ir bendradarbiavimą tiriant kompiuterinius nusikaltimus, pasižyminčius globalizacijos tendencija.

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

– nesankcionuota prieiga ir perėmimas (QA);

– kompiuterinių duomenų pakeitimas (QD);

– kompiuterinis sukčiavimas (QF);

– neteisėtas kopijavimas (QR);

– kompiuterinis sabotažas (QS);

– kiti kompiuteriniai nusikaltimai (QZ).

Kiekviena kompiuterinių nusikaltimų grupė detalizuojama nurodant jai priskirtus nusikaltimus, turinčius savo indeksą (žr. 1 priedas).

1989 m. Europos Taryba priėmė Rekomendaciją R(89)9 dėl kompiuterinių nusikaltimų[21], skirtą Europos Sąjungos valstybėms, kurioje siūloma tobulinant nacionalinius teisės aktus, reglamentuojančius kompiuterinius pažeidimus ar nusikaltimus, vadovautis pateikiamais dviem tokio pobūdžio veikų sąrašais: 1) minimaliu sąrašu, kuriame nurodytos aštuonios pavojingos veikos, susijusios su kompiuterinėmis technologijomis, kurias rekomenduojama Įtraukti Į nacionalinius teisės aktus, ir 2) papildomu sąrašu, kuriame nurodytos keturios mažiau pavojingos veikos, kurios nėra privalomai Įtrauktinos Į nacionalinius teisės aktus.

Minimalus sąrašas:

1. Sukčiavimas naudojant kompiuterį *(Computer-related fraud)*.

2. Klastojimas naudojant kompiuterį *(Computer forgery)*.

3. Kompiuterinių duomenų arba programų sunaikinimas arba sugadinimas *(Damage to computer data or computer programs)*.

4. Sabotažas naudojant kompiuterį *(Computer sabotage)*.

5. Neteisėtas priėjimas (neteisėta kreiptis) prie kompiuterinių sistemų *(Unauthorised access)*.

6. Neteisėtas informacijos kompiuterinėse sistemose perėmimas *(Unauthorised interception)*.

7. Neteisėtas apsaugotų kompiuterinių programų dauginimas ir platinimas *(Unauthorised reproduction of a protected computer program)*.

8. Neteisėtas kompiuterinių lustų (mikroschemų) topografijų dauginimas ir platinimas *(Unauthorised reproduction of a topography)*.

Papildomas sąrašas:

1. Kompiuterinių duomenų arba programų pakeitimas *(Alteration of computer data or computer programs)*.

2. Šnipinėjimas naudojant kompiuterį *(Computer espionage)*.

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

3. Neteisėtas kompiuterio naudojimas (laiko vagystė) *(Unauthorised use of computer)*.

4. Neteisėtas apsaugotų kompiuterinių programų naudojimas *(Unauthorised use of a protected computer program)*.

Palyginus 1995 m. Interpolo Generalinio Sekretoriato rekomendacijose „Computers and crime“ ir Europos Tarybos rekomendacijose pateiktas kompiuterinių nusikaltimų bei pažeidimų klasifikacijas, galima būtų išskirti šias pagrindines neteisėtų veikų grupes:

1. Sukčiavimas naudojant kompiuterį – tai kompiuterinių duomenų arba kompiuterinių programų įvedimas, pakeitimas, ištrynimas arba kitoks įsikišimas į duomenų apdorojimo procesą, kuris paveikia šio proceso galutinį rezultatą, padaro žalos kito asmens nuosavybei, siekiant naudos sau arba kitam asmeniui.

2. Klastojimas naudojant kompiuterį – tai kompiuterinių duomenų arba kompiuterinių programų įvedimas, pakeitimas, ištrynimas arba kitoks įsikišimas į duomenų apdorojimo procesą, kai šių veiksmų tikslas yra toks pat, kaip ir teisės aktuose, numatančiuose atsakomybę už tradicinį klastojimą.

3. Sabotažas naudojant kompiuterį – tai kompiuterinių duomenų arba kompiuterinių programų įvedimas, pakeitimas, ištrynimas arba įsikišimas bei trukdymas kompiuterinėms sistemoms, siekiant sutrikdyti kompiuterinės sistemos arba telekomunikacijų tinklo darbą.

4. Kompiuterinių duomenų arba programų sunaikinimas arba sugadinimas – tai neteisėtas kompiuterinių duomenų arba kompiuterinių programų ištrynimas, sunaikinimas, sugadinimas.

5. Neteisėta prieiga prie kompiuterinių sistemų – tai neteisėtas priėjimas prie kompiuterinės sistemos arba kompiuterinio tinklo, pažeidžiant saugumo priemones.

6. Neteisėtas informacijos kompiuterinėse sistemose perėmimas – tai informacijos perėmimas nelegaliais būdais kompiuterinio tinklo viduje arba išorėje.

Siekiant suvienodinti Europos Sąjungos valstybių baudžiamąją materialinę teisę ir išvengti dvigubo baudžiamumo taisyklės neatitikimo problemų, 2001 m. Budapešte buvo priimta Konvencija dėl elektroninių nusikaltimų (priimta 2001 m. lapkričio 23 d., pasirašyta 2003 m. birželio 23 d., ratifikuota Lietuvos Respublikos 2004 m. sausio 22 d. Įstatymu Nr. IX-1974 (Žin., 2004, Nr.36), Įsigaliojo 2004 m. liepos 1 d.), kurioje pateikiama kompiuterinių nusikaltimų klasifikacija, parengta atsižvelgiant į minėtą Rekomendaciją R(89)9 dėl kompiuterinių nusikaltimų. Konvencijoje nusikaltimai buvo suskirstyti į keturias grupes pagal Įstatymų saugomą interesą:

1. Nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui:

neteisėta prieiga;

neteisėta perimtis;

neteisėtas poveikis duomenims;

neteisėtas poveikis sistemai;

neteisėtas Įtaisų naudojimas.

2. Kompiuteriniai nusikaltimai (nusikaltimai panaudojant kompiuterines technologijas):

kompiuterinis klastojimas;

kompiuterinis sukčiavimas.

3. Turinio nusikaltimai (nusikaltimai, susiję su vaikų pornografija).

4. Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais (autorių teisių pažeidimai, gretutinių teisių pažeidimai).

Jungtinių Tautų parengtoje tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalgoje pateikiama tokia kompiuterinių nusikaltimų klasifikacija[22]:

1. Manipuliavimas naudojant kompiuterĮ (kompiuterinis sukčiavimas);
2. Klastojimas naudojant kompiuterĮ;
3. Kompiuterinių duomenų ir programų sunaikinimas ir modifikavimas (kompiuterinis sabotažas);
4. Neteisėtas priėjimas prie kompiuterinių duomenų;
5. Neteisėtas kompiuterinių programų platinimas.

Išnagrinėjus minėtas Europos Tarybos ir Jungtinių Tautų parengtas kompiuterinių nusikaltimų klasifikacijas bei jų apibūdinimą, galima atrasti daug bendrų dalykų, nepaisant skirtingo konkrečios nusikaltimų rūšies Įvardijimo.

Nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui

Neteisėta prieiga *(illegal access)* – tai tyčinis ir neteisėtas priėjimas prie visos kompiuterinės sistemos arba jos dalies, t.y. isibrovimas, slaptažodžių iškodavimas ar neteisėtas naudojimasis, Įvykdytas pažeidžiant apsaugos priemones, kuris gali būti padarytas siekiant gauti kompiuterinius duomenis ar turint kitą nesąžiningą ketinimą, taip pat gali būti susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema.

Neteisėta perimtis *(illegal interception)* – tai tyčinis ir neteisėtas neviešo kompiuterinių duomenų perdavimo (srauto) Į kompiuterinę sistemą, iš jos ir jos viduje perėmimas

[22] United Nations Manual on computer-related crime. International review of criminal policy. No 43/44.

techninėmis priemonėmis, taip pat elektromagnetinės emisijos iš kompiuterinės sistemos, perduodančios tokius kompiuterinius duomenis, perėmimas, kuris gali būti įvykdytas turint nesąžiningą ketinimą arba gali būti susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema.

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

Poveikis sistemai *(system interference)*– tai tyčinis ir neteisėtas kompiuterinės sistemos darbo sutrukdymas įvedant, perduodant, sugadinant, sunaikinant, apgadinant, pakeičiant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis.

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

1) gaminimas, pardavimas, įsigijimas naudoti, įvežimas, platinimas arba kitoks galimybės naudotis suteikimas:

a) įtaiso, įskaitant kompiuterinę programą, sukurto ar pritaikyto pirmiausia anksčiau minėtiems nusikaltimams (neteisėta prieiga; neteisėta perimtis; poveikis duomenims; poveikis sistemai) daryti,

b) kompiuterio slaptažodžio, prieigos kodo arba panašių 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 minėtos veikos (įtaisų, slaptažodžių, kodų gaminimas, pardavimas, įsigijimas naudoti, įvežimas, platinimas ir kitoks galimybės naudotis suteikimas arba turėjimas) neužtraukia baudžiamosios atsakomybės, jei jos yra teisėtos, t.y. skirtos tik sankcionuotam kompiuterinės sistemos tikrinimui arba jos apsaugai.

Nusikaltimų kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui grupę Jungtinių Tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalgoje sudaro **neteisėtas prieigos prie kompiuterinių duomenų ir kompiuterinių duomenų ir programų sunaikinimas arba modifikavimas (kompiuterinis sabotažas).** Teigiama, jog **neteisėtu prieigu prie kompiuterinių duomenų** gali būti siekiama įvairių tikslų. Šiai grupei priskiriami hakerių veiksmai, demonstruojantys gebėjimą apeiti apsaugos sistemas, pasinaudojant jų trūkumais (pvz., pasinaudojus sistemoje vartojamais bendrais

slaptažodžiais, perėmus slaptažodĮ "Trojos arklio" pagalba ir apsimetus teisėtu vartotoju, naudojant specialias slaptažodžių Įveikimo programas ir pan.). Svarbu paminėti neteisėtą prieigą prie ypatingos kategorijos duomenų, laikomų valstybės, tarnybos, banko ar komercine paslaptimi, kuri daugelyje valstybių yra kriminalizuota. Neteisėta prieiga gali padaryti žalą duomenims, sutrikdyti kompiuterinės sistemos darbą. **Kompiuterinių duomenų ir programų sunaikinimas arba modifikavimas (kompiuterinis sabotažas)** – tai kompiuterinių programų, duomenų, kompiuterinės Įrangos sugadinimas, sunaikinimas arba teisėtų vartotojų ir sistemos administratorių veiklos apribojimas, trukdant jiems dirbti su sistemos ištekliais, taip pat programų, skirtų sugadinti arba sunaikinti kitas kompiuterines programas bei duomenis (kompiuterinių virusų, „loginių bombų“, „kirmėlių“ ir kt.), kūrimas, platinimas bei naudojimas. Duomenys gali būti sunaikinami ar sistemos darbas sutrikdomas panaudojant prieiga internetu, taip pat panaudojant elektromagnetines bangas, radioaktyvų spinduliavimą ir kt. Kompiuterinio sabotažo motyvai gali būti skirtingi: komerciniai (konkurencinė kova), kariniai, politiniai, chuliganiški, keršto ir kt. Šios kategorijos nusikalstamos veikos apima ir tiesioginĮ ir slaptą neteisėtą priėjimą prie kompiuterinės sistemos.

Kompiuteriniai nusikaltimai (nusikaltimai panaudojant kompiuterines technologijas)

Kompiuterinės klastotės *(forgery)* – tai tyčinis ir neteisėtas kompiuterių duomenų suklastojimas, t.y. duomenų Įvedimas, pakeitimas, sunaikinimas arba galimybės naudotis jais panaikinimas, siekiant, kad pakeisti, neautentiški duomenys būtų laikomi autentiškais, ar jais būtų naudojamasi teisėtiems tikslams, (nepriklausomai nuo to, ar šie duomenys yra tiesiogiai skaitomi ir suprantami), esant ketinimui apgauti ar panašiam nesąžiningam ketinimui.

Jungtinių Tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalgoje ši nusikaltimų grupė Įvardinta kaip **klastojimas naudojant kompiuterĮ**, t.y. kompiuterių duomenų pakeitimas, sugadinimas arba sunaikinimas dėl Įvairių tikslų, tačiau nesiekiant tiesioginės turtinės naudos, o tai ir skiria šiuos nusikaltimus nuo sukčiavimo panaudojant kompiuterĮ. Šiai grupei nusikaltimų priskiriami tradiciniai dokumentų klastojimo nusikaltimai, vykdomi naudojant kompiuterinę Įrangą (ypač naujos kartos lazerinius spausdintuus ir kopijuoklius), taip pat gali būti priskiriama nesąžininga konkurencija, mokesčių slėpimas, kai apskaita yra kompiuterizuota, ir kt.

Kompiuterinis sukčiavimas *(fraud)* – tai tyčiniai ir neteisėti veiksmai, sąlygojantys kito asmens nuosavybės praradimą, Įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis, paveikiant kompiuterinės sistemos darbą, siekiant gauti neteisėtos ekonominės naudos sau arba kitam asmeniui.

Jungtinių Tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalgoje kompiuterinis sukčiavimas Įvardijamas kaip **manipuliavimas naudojant kompiuterĮ**, t.y.

kompiuterinių duomenų Įvedimo ir išvedimo manipuliacijos, kuriomis sunaikinami arba sugadinami duomenys, padaromi nuostoliai, siekiant turtinės naudos sau.

Duomenų Įvedimo manipuliacijų metu Į kompiuterinę sistemą gali būti Įvesti neteisingi duomenys, tokius veiksmus sąlyginai paprasta atlikti vykdant kompiuterinių sistemų duomenų apdorojimo funkcijas, nes tam nereikia ypatingų kompiuterinių žinių, tačiau gana sunku aptikti. Programų manipuliacijų metu Į kompiuterinę sistemą gali būti Įvestos naujos programos arba pakeistos kompiuterinėje sistemoje esančios programos (pvz., taikomas „Trojos arklio“ metodas), tokios manipuliacijos yra sudėtingos ir sunkiai aptinkamos, reikalauja specialių kompiuterinių žinių.

Duomenų išvedimo manipuliacijų metu iš kompiuterinės sistemos gali būti Įvairiais būdais išvesti duomenys, falsifikuojant komandas (pvz., grynųjų pinigų automato apgavimas, naudojant vogtas bankų kortelės ar specialius Įrenginius, „Salami“ metodas, kai kartojamos kompiuterinės procedūros, siekiant pervesti pinigus iš vienos sąskaitos Į kitą).

Nusikaltimai, susiję su vaikų pornografija – tai turinio nusikaltimai, tiksliau tyčinis ir neteisėtas pornografinio turinio produkcijos, kurioje atvaizduotas vaikas:

1) gaminimas, turint tikslą platinti per kompiuterinę sistemą;

2) siūlymas arba pateikimas per kompiuterinę sistemą;

3) platinimas arba perdavimas per kompiuterinę sistemą;

4) Įsigijimas per kompiuterinę sistemą sau arba kitam asmeniui;

5) laikymas kompiuterinėje sistemoje arba kokioje nors kompiuterinių duomenų laikmenoje.

Konvencijoje sąvoka „pornografinio turinio produkcija, kurioje atvaizduotas vaikas“ reiškia pornografinę medžiagą, vizualiai vaizduojančią:

a) aiškiai seksualų nepilnamečio elgesĮ;

b) aiškiai seksualų asmens, atrodančio kaip nepilnametis, elgesĮ;

c) tikroviškus nepilnamečio aiškiai seksualaus elgesio vaizdus.

Konvencijoje sąvoka „vaikas“ reiškia nepilnametis asmuo iki 18 metų, tačiau šalys gali nustatyti žemesnę amžiaus ribą – iki 16 metų.

Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais, – tai šios veikos:

1) autorių teisių pažeidimai, nustatyti šalies teisės aktuose, laikantis Įsipareigojimų, kuriuos ji prisiėmė pagal Berno konvencijos dėl literatūros ir meno kūrinių apsaugos Paryžiaus aktą, priimtą 1971 m. liepos 24 d., SutartĮ dėl intelektinės nuosavybės teisių prekyboje aspektų ir WIPO autorių teisių sutartĮ, išskyrus moralines teises, suteikiamas tokių konvencijų, kai tokie veiksmai

atliekami sąmoningai, komerciniais tikslais ir naudojantis kompiuterių sistema.

2) gretutinių teisių pažeidimai, nustatyti šalies teisės aktuose, laikantis Įsipareigojimų, kuriuos ji prisiėmė pagal Romoje sudarytą Tarptautinę konvenciją dėl atlikėjų, fonogramų gamintojų ir transliuojančiųjų organizacijų apsaugos (Romos konvencija), SutartĮ dėl intelektinės nuosavybės teisių prekyboje aspektų ir WIPO atlikimų ir fonogramų sutartĮ, išskyrus moralines teises, suteikiamas tokių konvencijų, kai tokie veiksmai atliekami sąmoningai, komerciniais tikslais ir naudojantis kompiuterių sistema.

Jungtinių Tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalgoje nurodytas **neteisėtas kompiuterinių programų platinimas,** t.y. programinės Įrangos, kuria turi teisę naudotis tik ją sukūręs arba Įsigijęs juridinis ar fizinis asmuo, pasisavinimas ir platinimas, darantis turtinę žalą teisėtiems savininkams (pvz., programinės Įrangos piratinis platinimas).

3. NUSIKALSTAMŲ VEIKŲ, SUSIJUSIŲ SU KOMPIUTERINĖMIS TECHNOLOGIJOMIS BEI INFORMACIJOS SAUGA, TEISINIS REGLAMENTAVIMAS

3.1. KOMPIUTERINIŲ NUSIKALTIMŲ TEISINIS REGLAMENTAVIMAS EUROPOS SĄJUNGOS VALSTYBĖSE

Kompiuterinių nusikaltimų teisinĮ reglamentavimą tarptautiniu mastu vykdo šios organizacijos:

1. Europos Taryba;
2. Europos ekonominio bendradarbiavimo ir plėtros organizacija (OECD);
3. Jungtinių Tautų Organizacija;
4. Pasaulio prekybos organizacija;
5. kitos organizacijos.

Europos Tarybos Kompiuterinių nusikaltimų ekspertų komitetas parengė ir Europos Taryba išleido šias rekomendacijas, skirtas teisinėms kompiuterinių nusikaltimų problemoms spręsti: rekomendaciją R(85)S, rekomendaciją R(89)9 ir rekomendaciją R(95)13.

1994 m. Jungtinės Tautos išleido Vadovą, skirtą su kompiuteriais susijusių nusikaltimų kontrolei ir prevencijai, kuriame nagrinėjami kompiuterinių nusikaltimų apibrėžimo, jų teisinio reglamentavimo, prevencijos, tarptautinis bendradarbiavimo klausimai.

Tačiau bene svarbiausias tarptautinis teisės aktas buvo 2001 m. lapkričio 23 d. Budapešte priimta Europos Tarybos Konvencija dėl elektroninių nusikaltimų[23]. Svarbu paminėti, kad Budapešto Konvencija yra vienintelė sutartis, tarptautiniu mastu reglamentuojanti su kompiuteriniais nusikaltimais susijusius teisinius klausimus. Vis dėlto nors Konvencija yra privaloma ją pasirašiusioms ir ratifikavusioms valstybėms, o jos pateiktą nusikaltimų klasifikaciją galima laikyti universaliausia, ji sukėlė nemažai diskusijų bei prieštaringų atsiliepimų: vienų mokslininkų nuomone šio dokumento priėmimas – žymus postūmis kovojant su moderniais nusikaltimais, kurių Įvykdymo objektas ar priemonės yra kompiuterinės technologijos, kitų, daugiausia informacinių technologijų specialistų, vertinimu, Konvencija tėra formalus susitarimas, kurio pagrindinis trūkumas – teisinių ir technologinių aspektų kolizija. Pagrindinė Konvencijos paskirtis – harmonizuoti Europos valstybių teisinę bazę, reglamentuojančią kompiuterinius nusikaltimus.

Beje, 2003 m. birželio 23 d. Konvenciją pasirašė 33 šalys, tačiau ją ratifikavo tik trys šalys – Albanija, Estija ir Kroatija, o tam, kad Konvencija Įsigaliotų, ją ratifikuoti privalėjo ne mažiau kaip penkios šalys ir mažiausiai trys iš jų – Europos Tarybos narės. Tik 2004 m. kovo 18 d. Konvenciją ratifikavo penktoji šalis – Lietuva (Lietuvos Respublikos 2004 m. sausio 22 d. Įstatymu

[23] Konvencija dėl elektroninių nusikaltimų // Valstybės 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, jų teisinės normos, susijusios su kompiuteriniais nusikaltimais, išlieka pakankamai skirtingos[24]. Vienos valstybės atliko kai kuriuos baudžiamųjų Įstatymų pakeitimus, kitos išleido specialius Įstatymus, skirtus kovai su kompiuteriniu nusikalstamumu. Kai kuriose šalyse, pavyzdžiui, Ispanijoje, nėra specialių normų, skirtų 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 Įvykdytus kompiuterinius nusikaltimus. Austrijoje iki 2002 m. Baudžiamojo kodekso pataisų nė viena iš veikų, susijusių su kompiuterinėmis 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 vienose valstybėse kompiuterinius nusikaltimus reglamentuoja specialios teisės normos, o kitose – tik bendrosios, dalis valstybių taiko tik administracinę atsakomybę arba apskritai nelaiko tokių veikų nei nusikaltimu, nei administraciniu pažeidimu (apibendrinti duomenys pateikiami 2 priede).

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

Belgija. 2000 m. lapkritĮ Belgijos Parlamentas Į BaudžiamąjĮ kodeksą Įtraukė pakeitimus, skirtus kovai su kompiuteriniais nusikaltimais, kurie Įsigaliojo nuo 2001 m. vasario 13 d. Belgijos Baudžiamojo kodekso 550^1 straipsnis numato atsakomybę už hakerių (kompiuterinių Įsilaužėlių) veiksmus. Pirma šio straipsnio dalis numato atsakomybę už tyčinę neteisinę prieigą prie kompiuterinių sistemų arba tyčinĮ tarpininkavimą suteikiant neteisėtą prieigą (sankcija – bauda arba areštas nuo 3 mėnesių iki 1 metų). Antrojoje straipsnio dalyje numatoma atsakomybė už neteisėtą prieigą prie kompiuterinių sistemų, Įvykdytą asmens, turinčio Įgaliojimus ir teises šiai prieigai, tačiau pasinaudojusio šia teise viršijant suteiktus Įgaliojimus ir turint piktavališkų kėslų ar su tikslu Įvykdyti kenksmingus veiksmus (sankcija - bauda arba laisvės atėmimas nuo 6 mėnesių iki 2 metų). Pirmosios minėto straipsnio dalys akcentuoja kompiuterinių sistemų apsaugą, o trečiojoje dalyje kalbama apie pačių duomenų, saugomų kompiuterinėse sistemose, vientisumą, neliečiamumą ir saugumą. Ji numato baudžiamąją atsakomybę už neteisėtą prieigą prie duomenų, kurie yra saugomi kompiuteryje ar kompiuterinėse sistemose, apdorojami ar perduodami kompiuterinėmis sistemomis,

[24] 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 neteisėtą šių duomenų panaudojimą. Atsakomybė numatoma tiek už tyčinius, tiek už neatsargius veiksmus, jei jie sukėlė žalą. Už šių veikų Įvykdymą baudžiama laisvės atėmimu nuo 1 iki 3 metų, pasikėsinimas Įvykdyti minėtus nusikaltimus taip pat yra baudžiamas. Už nusikaltimų, numatytų minėtame straipsnyje, organizavimą, taip pat už skatinimą juos Įvykdyti, numatoma bausmė – bauda arba laisvės atėmimas nuo 6 mėnesių iki 5 metų.

Belgijos Baudžiamojo kodekso 314 straipsnis numato baudžiamąją atsakomybę už neteisėtą duomenų perėmimą ryšių tinkluose (sankcija – nuo 1 iki 3 metų laisvės atėmimo); 523, 528, 559 straipsniai numato atsakomybė už kenkėjiškų programų sukūrimą ir kompiuterinĮ sabotažą, Įrangos sugadinimą, nuostolių nuosavybei padarymą. Neteisėtas kompiuterinės informacijos pakeitimas nusikalstamais tikslais gali būti baudžiamas priklausomai nuo jo pobūdžio pagal Belgijos Baudžiamojo kodekso 134 straipsnĮ (klastojimas), 461 straipsnĮ (vagystė), 496 straipsnĮ (sukčiavimas).

Didžioji Britanija. Ši valstybė priklauso bendrosios teisės sistemai, tad baudžiamieji Įstatymai nėra kodifikuoti. Kompiuteriniams nusikaltimams reglamentuoti skirtas 1990 m. Aktas dėl kompiuterių panaudojimo neteisėtiems tikslams. Šio Akto pirmasis straipsnis numato atsakomybę už neteisėtą prieigą prie kompiuterinių duomenų ir nustatyto, kad asmuo Įvykdo nusikaltimą, jei jis naudoja kompiuterĮ bet kurios funkcijos vykdymui, siekdamas užtikrinti prieigą prie bet kurios programos ar duomenų, saugomų bet kuriame kompiuteryje, jei tokia prieiga žinomai yra neteisėta. Anglijos baudžiamoji teisė nenumato skirtingų bausmių už prieigą prie kompiuterių, apsaugotų specialiomis priemonėmis, ir neapsaugotų. Be to, nusikaltimu yra pripažĮstama prieiga prie kompiuterio, kurio pagalba duomenys arba programos pakeičiami arba sunaikinami, kopijuojami ar perkeliami Į kitą vietą, nei jie buvo saugomi, arba naudojami bet kuriuo būdu. Už šio nusikaltimo Įvykdymą numatyta bausmė - bauda arba laisvės atėmimas iki 6 mėnesių.

Antrasis Akto straipsnis numato atsakomybę už nelegalią prieigą siekiant Įvykdyti kitą nusikaltimą (kompiuterio panaudojimas vagystei, sukčiavimui). Tai gali būti nusikaltimas, numatytas šiame Akte, ar kitas nusikaltimas, kurĮ asmuo ketina Įvykdyti arba palengvinti jo vykdymą sau ar kitam asmeniui. Bausmė, priklausomai nuo Įvykdytos veikos sunkumo, yra skirtinga – bauda arba laisvės atėmimas iki 6 mėnesių, sunkių nusikaltimų atvejais – iki 5 metų.

Trečiasis Akto straipsnis numato atsakomybę už neteisėtą duomenų pakeitimą. Tyčiniai neteisėti veiksmai, sąlygojantys bet kurio kompiuterio duomenų turinio pokyčius, laikomi nusikaltimu, asmuo žinojo ar turėjo žinoti, kad neturi teisės vykdyti duomenų keitimo (sankcijos už tokią veiką yra analogiškos, nurodytoms 2 straipsnyje).

Baudžiamosios atsakomybės normos dėl neteisėto informacijos rinkimo, neteisėtos prieigos prie informacijos, neteisėto perėmimo taip pat yra nustatytos Akte dėl tyrimų reguliavimo. Šis aktas numato, kad tyčinis be nustatyto leidimo vykdomas bet kokio pobūdžio ryšio viešaisiais

telekomunikaciniais tinklais perėmimas yra laikomas nusikaltimu. Už šio nusikaltimo Įvykdymą numatyta bausmė - bauda arba laisvės atėmimas iki 2 metų.

Ispanija. Ispanijos Baudžiamojo kodekso 197 straipsnis numato baudžiamąją atsakomybę už slaptų duomenų atskleidimą ir platinimą be savininko sutikimo, taip pat ir duomenų iš elektroninio pašto arba saugomų duomenų bazėse. Nusikaltimu taip pat yra laikoma informacijos, perduodamos telekomunikaciniais tinklais ar sistemomis, perėmimas arba Įrašymo ar pasiklausymo Įrangos naudojimas. Už tokių veikų Įvykdymą numatyta sankcija - bauda arba laisvės atėmimas nuo 1 iki 4 metų. Jeigu šie duomenys buvo viešai išplatinti, pademonstruoti arba pateko tretiesiems asmenims, numatytas laisvės atėmimas nuo 2 iki 5 metų. 197 straipsnyje yra kelios dalys, patikslinančios bausmę, atsižvelgiant Į Įvykdyto nusikaltimo sunkumą, maksimali bausmė numatoma tuo atveju, jeigu duomenys yra susiję su nukentėjusiojo ideologija, religija, sveikata, rase, seksualine orientacija (lietuviškas atitikmuo - ypatingieji asmens duomenys pagal Asmens duomenų teisinės apsaugos Įstatymą). 198 ir 199 straipsniai yra susiję su 197 straipsniu ir skirti atvejams, kai nusikaltimo subjektas yra asmuo, Įgaliotas dirbti su duomenimis, o taip pat kai nusikaltimas yra Įvykdomas pareigūno, viršijant tarnybinius Įgaliojimus. Už šias veikas baudžiama laisvės atėmimu iki 10 metų. 263 straipsnis numato atsakomybę už telekomunikacijų panaudojimą be savininko sutikimo, jei taip buvo padaryta žala (sankcija - laisvės atėmimas nuo 3 mėnesių iki 1 metų). 264 straipsnio 2 dalis numato atsakomybę asmenims, kurie kokiu nors būdu sugadino, padarė netinkamais naudotis ar kitaip padarė žalą svetimiems elektroniniams duomenims, programoms ar dokumentams, esantiems tinkle, informaciniuose Įrenginiuose ar sistemose. Už tokio pobūdžio nusikaltimą numatyta bausmė - bauda arba laisvės atėmimas nuo 1 iki 3 metų. 278 straipsnis numato baudžiamąją atsakomybę už duomenų, rašytinių ar elektroninių dokumentų, informacinių Įrenginių ar kitų objektų, kurie priskiriami komercinėms paslaptims, gavimą bet kokiu būdu.

Prancūzija. Prancūzijos Baudžiamajame kodekse yra du – 186^1 ir 323 straipsniai, susiję su kompiuteriniais nusikaltimais. 186^1 straipsnis nustato baudžiamąją atsakomybę už neteisėtą duomenų perėmimą elektroninių ryšių (telekomunikacinėse) sistemose. Už šio nusikaltimo padarymą numatoma bausmė - bauda arba laisvės atėmimas iki 1 metų, o jei nusikaltimo subjektas yra pareigūnas, tai laisvės atėmimo bausmė gali būti padidinta iki 5 metų. 323 straipsnio pirma dalis numato baudžiamąją atsakomybę už neteisėtą prieigą prie automatizuotos duomenų apdorojimo sistemos ar tokios sistemos dalies, jei tokios prieigos metu sunaikinti ar pakeisti duomenys, saugomi sistemoje, arba pažeistas ar pakeistas sistemos funkcionalumas. Atsakomybė pagal minėtą straipsnĮ gali būti pritaikyta ir už kenkėjiškų programų sukūrimą, pasikėsinimą Įsilaužti Į sistemą, neteisėtą prieigą prie duomenų, neteisėtą prieigą prie ryšio sistemų. Už šių nusikalstamų veikų padarymą yra numatoma bausmė - bauda ar laisvės atėmimas iki 2 metų. 323 straipsnio antroji dalis

nustato atsakomybę už duomenų pakeitimą ar bet kokĮ kitą Įsiskverbimą Į veikiančią automatizuotą duomenų apdorojimo sistemą. Trečioji šio straipsnio dalis nustato atsakomybę už duomenų pakeitimą sistemose su klastojimo arba sukčiavimo tikslu. Už nurodytus nusikaltimus numatytos bausmės - bauda arba laisvės atėmimas iki 3 metų.

Vokietija. Vokietijos Baudžiamajame kodekse yra pakankamai daug straipsnių, kurie gali būti taikomi ir kompiuteriniams nusikaltimams, tačiau pagrindiniai yra du – 202 ir 303 straipsniai. 202 straipsnio a punktas numato baudžiamąją atsakomybę asmeniui už neteisėtą duomenų, apsaugotų specialiomis priemonėmis nuo neteisėtos prieigos, paėmimą, siekiant asmeninės naudos ar naudos trečiajam asmeniui. 202 straipsnis nustato atsakomybę už neteisėtą prieigą prie duomenų, laikomų elektroninėse ar magnetinėse laikmenose, ar kitose panašiose laikmenose, t.y. tokie duomenys apibrėžiami kaip kompiuteriniai. Už šią veiką taikoma bausmė - bauda arba laisvės atėmimas iki 3 metų. 303 straipsnio a punktas nustato atsakomybę už duomenų pakeitimą, duomenų ištrynimą, sunaikinimą, padarymą netinkamais naudoti ar pasikėsinimą atlikti išvardintus veiksmus. Šis straipsnis taikomas tik tiems duomenims, kurie nurodyti 202 straipsnyje. Bausmė - bauda arba laisvės atėmimas iki 2 metų. 303 straipsnio b punktas apima tokius nusikaltimus kaip DNS atakos (kompiuterinis sabotažas) ir kenkėjiškų programų sukūrimas. Straipsnyje apibrėžta, kad kompiuterinis sabotažas – tai Įsikišimas Į duomenų apdorojimo procesą, kuris yra svarbus Įmonei, valstybės institucijoms, ar verslui. Įsikišimas gali būti Įvykdytas būdais, nurodytais 303 straipsnio a punkte arba sunaikinant, pažeidžiant, padarant netinkamais naudoti, pakeičiant kompiuterinę sistemą ar Įsikišant Į duomenų perdavimo sistemą. Nurodytos veikos baudžiamos bauda arba laisvės atėmimu iki 5 metų. Baudžiama ir už pasikėsinimą Įvykdyti minėtus nusikaltimus.

Estija. Estijos elektroninių ryšių sektorius yra vienas labiausiai išvystytų Centrinėje ir Rytų Europoje, tačiau greita informacinės visuomenės plėtra buvo glaudžiai susijusi ir su kompiuterinių nusikaltimų plitimu. Šiuo metu pagrindinės kompiuterinių nusikaltimų rūšys, kriminalizuotos Estijoje, yra kompiuterinis sukčiavimas (fišingas, kardingas), neteisėtas kompiuterių, kompiuterinių sistemų ar kompiuterių tinklų panaudojimas), kenkėjiškų programų (kompiuterinių virusų, kirminų, Trojos arklių ir kitų) panaudojimas Įvairiems nusikalstamiems tikslams, pedofilijos turinio platinimas internete. Estai ėmėsi pertvarkyti savo teisės aktų bazę jau 2000 m. Nuo 2000 m. Įsigaliojo trys svarbūs Įstatymai elektroninių ryšių srityje: Asmens duomenų apsaugos aktas, Informacinės visuomenės paslaugų aktas ir Telekomunikacijų aktas, nustatantys atsakomybę už „spamą“ ir reguliuojantys komercinę komunikaciją internete. Informacinės visuomenės paslaugų aktas nustatė tam tikras ribas informacinės visuomenės paslaugų tiekėjams ir atsakomybę už šio akto nuostatų pažeidimus. Juo vadovaujamasi, kai būtina kovoti su neteisėtu viešu turinio paskelbimu Internete, nustatant reikalavimus automatizuotoms paslaugoms ir duomenų

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 veikų, susijusių su kompiuteriais ar jų tinklais, rūšis: ryšio perėmimas, savavališkas prisijungimas prie kompiuterinių sistemų, neteisėtas kompiuterinių programų Įsigijimas; programinės Įrangos 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 Į tai, kad naujasis Latvijos Baudžiamojo proceso kodeksas, kuris buvo patvirtintas 2005 m. balandžio 21 d. ir Įsigaliojo nuo 2005 m. spalio 1 d., nustatė specialius procesinius veiksmus, susijusius su kompiuterinių nusikaltimų tyrimu.

Lenkija. Galiojančiame 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 Įsigaliojo keletas šio kodekso pataisų, susijusių su kompiuteriniais nusikaltimais. 2004 m. gegužės 18 d. baudžiamųjų Įstatymų pataisos buvo priimtos siekiant suderinti Lenkijos Baudžiamojo kodekso ir Baudžiamojo proceso kodekso nuostatas su Europos Konvencija dėl elektroninių nusikaltimų.

Lenkijos Įstatyme dėl elektroniniu būdu teikiamų paslaugų (2002 m. liepos 18 d.) Įtvirtintos nuostatos, draudžiančios perteklinės informacijos siuntimą, nepageidaujamos komercinio pobūdžio informacijos platinimą („spamą“).

Apibendrinant Europos valstybių, pasirašiusių Konvenciją dėl elektroninių nusikaltimų, baudžiamosios teisės harmonizavimo patirtĮ, galima teigti, kad nacionaliniai Įstatymai turi daug skirtumų tiek teisinės technikos, tiek turinio prasme. Vis dėlto daugelyje valstybių veikos, 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. KOMPIUTERINIŲ NUSIKALTIMŲ TEISINIS REGLAMENTAVIMAS LIETUVOJE

Kaip jau buvo minėta, Lietuvos Respublikos baudžiamajame kodekse terminas „kompiuterinis nusikaltimas“ nėra apibrėžtas, taigi jis oficialiai nėra įteisintas *de jure*, tačiau kalbant apie veikas, susijusias su kompiuterinėmis technologijomis bei elektronine erdve, vartojamas *de facto*. Lietuvoje nėra specialaus įstatymo, reglamentuojančių kompiuterinius nusikaltimus, tačiau kai kurių įstatymų normos gali būti taikomos kompiuteriniams nusikaltimams ar pažeidimams. Svarbu tai, kad naujajame Lietuvos Respublikos baudžiamajame kodekse veikoms, susijusioms su kompiuterinėmis 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 (198^1 straipsnis);

5) neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti (198^2 straipsnis).

Reikia pastebėti, kad Lietuvos Respublikos vidaus reikalų ministerijos Nusikalstamų veikų žinybinio registro, kurį tvarko Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos Statistikos skyrius, duomenimis, įsigaliojus 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, ištirta 20 veikų (žr. 4 priedas 1 lentelė). Galima daryti prielaidą, jog tai lemia kelios objektyvios aplinkybės: kompiuterinės technologijos dažniausiai panaudojamos siekiant įvykdyti kitas nusikalstamas veikas (plg. 4 priedas 2 lentelė), be to, šios rūšies nusikaltimams būdingas ypač didelis latentiškumas (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 įstatymo kriminalizuotos šios veikos:

1) autorystės pasisavinimas (191 str.);

2) literatūros, mokslo, meno ar kitokio kūrinio neteisėtas atgaminimas, neteisėtų kopijų 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 sudėtys buvo reglamentuotos ir senajame Baudžiamajame kodekse. Atkreiptinas dėmesys Į tai, kad skirtingai nei senajame Baudžiamajame kodekse, aprašant minėtų nusikaltimų objektyviuosius požymius nepateikiama tiesioginė nuoroda Į kompiuterių programas, tačiau pagal Lietuvos Respublikos autorių teisių ir gretutinių teisių Įstatymą kompiuterinė programa yra laikoma kūriniu, todėl naujojo Baudžiamojo kodekso 191-194 straipsniai taikytini ir kompiuterinės programos 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 pornografinei produkcijai gaminti (atsakomybė 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, pateikiamas kaip vaikas, pagaminimą su tikslu platinti, ar jos Įsigijimą arba platinimą, o Baudžiamojo kodekso 309 straipsnio 3 dalyje numatoma, kad baudžiamas tas, kas viešai demonstravo ar rek1amavo pornografinio turinio dalykus arba Įgijo ar laikė pornografinio turinio dalykus.

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

1) neteisėtas susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimas (166 straipsnis);

2) neteisėtas informacijos apie privatų asmens gyvenimą rinkimas (167 straipsnis);

3) neteisėtas 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[25]: šnipinėjimas (119 straipsnis); neteisėtas disponavimas informacija, kuri yra valstybės paslaptis (124 straipsnis); valstybės paslapties atskleidimas (125 straipsnis); valstybės paslapties praradimas (126 straipsnis); šmeižimas (154 straipsnis); Įžeidimas (155 straipsnis); diskriminavimas dėl tautybės, rasės, lyties, kilmės, religijos ar kitos grupinės priklausomybės (169 straipsnis); kurstymas prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę (170 straipsnis); komercinis šnipinėjimas (210 straipsnis);

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

komercinės paslapties atskleidimas (211 straipsnis); melagingas pranešimas apie visuomenei gresiantĮ pavojų ar ištikusią nelaimę (285 straipsnis); grasinimas valstybės tarnautojui ar viešojo administravimo funkcijas atliekančiam asmeniui (287 straipsnis); valstybės tarnautojo ar viešojo administravimo funkcijas atliekančio asmens Įžeidimas (290 straipsnis); neteisėtas specialios technikos Įrengimas ar panaudojimas informacijai rinkti (295 straipsnis); tarnybos paslapties pagrobimas ar kitoks neteisėtas Įgijimas (296 straipsnis); tarnybos paslapties atskleidimas (297 straipsnis).

Išanalizavus Nusikalstamų veikų 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: šmeižimą (154 straipsnis); sukčiavimą (182 straipsnis); literatūros, mokslo, meno ar kitokio kūrinio neteisėtą atgaminimą, neteisėtų kopijų platinimą, gabenimą ar laikymą (192 straipsnis); netikrų 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 Baudžiamojo kodekso XXX skyriaus normas, reikia pastebėti, jog visų kompiuterinių nusikaltimų, išskyrus kompiuterinės informacijos pasisavinimo ir skleidimo (198 str.), **sudėtys yra materialios**, t.y. tokio pobūdžio nusikalstama veika turi būti sukeliama didelė žala (kuri gali būti tiek turtinė, tiek neturtinė).

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

Galiojantis Baudžiamasis kodeksas nustato, kad kompiuterinių nusikaltimų **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 padarė juridinio asmens darbuotojas ar Įgaliotas atstovas dėl jam vadovaujančio asmens nepakankamos priežiūros arba kontrolės. Be to, juridinio asmens baudžiamoji atsakomybė nepašalina fizinio asmens, kuris padarė, organizavo, kurstė arba padėjo padaryti nusikalstamą veiką, baudžiamosios atsakomybės.

Baudžiamojo kodekso apibrėžtų kompiuterinių nusikaltimų sudėties analizė rodo, jog **kaltės forma gali būti tiek tyčia, tiek neatsargumas**, bet galima teigti, jog didžioji dalis šių veikų bus padaromos tiesiogine tyčia, rečiau – netiesiogine, o galimybė tokias veikas padaryti dėl nusikalstamo pasitikėjimo ar nusikalstamo nerūpestingumo yra mažai tikėtina, Įvertinus kompiuterinių sistemų funkcionavimo ypatumus bei saugos priemones.

Įvertinus galiojančio Baudžiamojo kodekso XXX skyriaus normų sankcijas, pažymėtina, kad visi kompiuteriniai nusikaltimai **yra nesunkūs**, nes pagal Baudžiamojo kodekso 11 straipsnio trečiąją dalĮ nusikaltimai, už kuriuos Įstatymas numato bausmę, neviršijančią 3 metų laisvės atėmimo, laikomi nesunkiais.

Būtina pastebėti, kad veikos, nurodytos Baudžiamojo kodekso XXX skyriuje, dažnai Įvykdomos ne kaip atskiri nusikaltimai, bet kartu su kitais nusikaltimais ir inkriminuojamos papildomai. Tai sąlygota aplinkybės, jog kompiuterinė technika ir informacija dažniausiai panaudojama siekiant Įvykdyti kitas nusikalstamas veikas.

2004 m. kovo 18 d. Lietuva ratifikavo Konvenciją dėl elektroninių nusikaltimų (Lietuvos Respublikos 2004 m. sausio 22 d. Įstatymu Nr. IX-1974 (Žin., 2004, Nr.36), kuri Įsigaliojo nuo 2004 m. liepos 1 d. Išanalizavus Konvencijos rekomenduojamas kriminalizuoti neteisėtas veikas bei mūsų Baudžiamojo kodekso XXX skyriaus „Nusikaltimai informatikai“ kriminalizuotas veikas, galima daryti išvadą, jog šiuo metu kodekso normos iš esmės atitinka Konvencijos reikalavimus. 2004 m. sausio 29 d. Lietuvos Respublikos Seimas priėmė Baudžiamojo kodekso pataisas, kuriomis suderino Baudžiamojo kodekso 196 ir 197 straipsnius su Konvencijos nuostatomis, taip pat papildė Baudžiamojo kodekso XXX skyrių 198^1 straipsniu „Neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo“ ir 198^2 straipsniu „Neteisėtas disponavimas Įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti“. Tačiau galima būtų paminėti ir keletą Lietuvos Baudžiamojo kodekso ir Konvencijos neatitikimų: rengiant Baudžiamojo kodekso pataisas nebuvo atsižvelgta Į Konvencijos vartojamus terminus kompiuterinių nusikaltimų apibūdinimui, pvz., Lietuvos Baudžiamojo kodekso vartojamas kompiuterinės informacijos terminas neatitinka Konvencijos nustatyto termino *computer data*, reiškiančio kompiuterinius duomenis, be to, Konvencijoje neskiriamos kompiuterinių duomenų ir kompiuterinės programos sąvokos, kaip tai yra padaryta mūsų Baudžiamajame kodekse, nes kompiuterinės programos laikomos sudarytomis iš

kompiuterinių duomenų ir todėl iš esmės nesiskiria; Konvencijoje vartojama kompiuterinės sistemos sąvoka, reiškianti kietosios ir programinės įrangos visumą, skirtą tvarkyti duomenis (taip apibrėžiamas kompiuteris arba kompiuterių tinklas).

Šiuo metu teisės normų, taikytinų veikoms, susijusioms su kompiuterių panaudojimu, galima rasti atskiruose Lietuvos Respublikos Įstatymuose, Lietuvos Respublikos Vyriausybės nutarimuose ir kituose teisės aktuose (sąrašas ir komentaras pateikiami 3 priede). Už šių teisės aktų, daugiau ar mažiau susijusių su visuomeninių santykių saugaus kompiuterinės informacijos tvarkymo srityje reglamentavimu, nustatytų reikalavimų pažeidimus atsakomybė numatyta Lietuvos Respublikos baudžiamajame kodekse ir Lietuvos Respublikos administracinių teisės pažeidimų kodekse.

Kompiuterinių 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 normų, taikytinų tiriant kompiuterinius nusikaltimus, netikslumas ar trūkumas nurodomas kaip viena iš priežasčių, sąlygojančių kompiuterinių nusikaltimų tyrimo problemas. Ikiteisminio tyrimo pareigūnų teigimu, keblumų kyla praktiškai taikant Baudžiamojo proceso kodekso normas, kurios nepakankamai išsamiai reglamentuoja veiksmus, susijusius su kompiuterinių nusikaltimų tyrimo ypatumais. Taigi, galima teigti, jog būtų tikslinga Baudžiamojo proceso kodekso normas patikslinti, atsižvelgiant į Konvencijos dėl elektroninių nusikaltimų 2 skirsnio „Proceso teisė“ reikalavimus (laikomųjų kompiuterinių duomenų paieška ir poėmis, kompiuterinių duomenų surinkimas realiuoju laiku – srauto duomenų bei turinio duomenų perimtis).

Apibendrinant kompiuterinių 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 kodekso normos iš esmės atitinka Konvencijos dėl elektroninių nusikaltimų reikalavimus, tačiau, pagrindine problema, autorės manymu, lieka šios srities terminologijos teisinis neapibrėžtumas.

II. KOMPIUTERINIŲ NUSIKALTIMŲ APIBŪDINIMO KRIMINALISTINIAI ASPEKTAI

4. KOMPIUTERINIŲ NUSIKALTIMŲ KRIMINALISTINĖ CHARAKTERISTIKA

Kriminalistinė charakteristika yra dinamiška kategorija, kintanti priklausomai nuo kriminalinės praktikos. Kriminalistinei nusikaltimų charakteristikai svarbūs nusikalstamų veikų elementai keičiasi pakankamai sparčiai, nes tobulėja nusikaltimų padarymo būdai, kinta nusikalstamų veikų tikslai ir motyvai, kėsinimosi dalykas, priežastys ir sąlygos, palankios tam tikroms nusikaltimų rūšims, todėl ir pati kriminalistinė charakteristika nėra pastovi ir apibrėžta Įvairių nusikaltimų rūšių duomenų visuma, bet dinamiškas reiškinys, atspindintis būdingiausias nusikaltimų ypatybes tam tikru laikotarpiu.

Taigi, siekiant, kad kriminalistinė charakteristika atliktų savo praktinę taikomąją užduotĮ ir padėtų atskleisti nusikaltimus, ji privalo būti tiksli, išsami ir aktuali, t.y. šiuolaikiška, atspindinti naujausius kriminalinės praktikos pokyčius, apimti aktualius kriminalistinės nusikaltimų, Įvykdytų pastaruoju laikotarpiu, analizės rezultatus.

Daugelyje kriminalistikos mokslo darbų pabrėžiama, kad kompiuterinių nusikaltimų kriminalistinė charakteristika, palyginus su kitų nusikaltimų rūšių charakteristika, pasižymi savitomis ypatybėmis, kurias sąlygoja kompiuterinių nusikaltimų pagrindinių struktūrinių elementų specifika ir išskirtiniai, tik šiai nusikaltimų rūšiai būdingi bruožai. Atkreiptinas dėmesys Į šiuos kriminalistiniu požiūriu svarbius elementus:

- pažeidėjo asmenybė;
- nusikalstamo elgesio motyvai ir tikslai;
- tipiniai nusikaltimo rengimo, Įvykdymo ir nuslėpimo būdai;
- laikas, vieta ir pasikėsinimo aplinkybės.

Be to, kriminalistikos mokslo darbuose akcentuojamos ir kompiuterinės informacijos, kaip pasikėsinimo dalyko, išskirtinės kriminalistinės ypatybės:

1) kompiuterinė informacija palyginti paprastai ir greitai keičiama (kinta), kopijuojama, dauginama Įvairia technine Įranga, siunčiama Įvairiausiu atstumu, ribojamu tik elektroninių ryšių Įrangos veikimo plotu;

2) paimant kompiuterinę informaciją (atliekant poėmĮ), skirtingai nei materialų objektą (daiktą), 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.

Kompiuterinio nusikaltimo Įvykdymo aplinkybės apima Įvairius aplinkos, kurioje Įvykdyta nusikalstama veika, faktorius: fizinius, techninius, socialinius ir psichologinius. Tai gali

Įtakoti visus kitus kompiuterinių nusikaltimų kriminalistinės charakteristikos elementus bei lemti nusikaltėlio ir nukentėjusiojo elgesio ypatumus.

V.B.Vechovas metodiniame leidinyje „Nusikaltimų, vykdomų panaudojant elektroninės skaičiavimo technikos priemones, tyrimo ypatybės“ nurodo, kad kompiuterinių nusikaltimų rengimo, Įvykdymo ir nuslėpimo aplinkybių visumos kriminalistinį savitumą lemia dvejopi faktoriai – objektyvūs ir subjektyvūs[26]. Prie objektyvių faktorių galima būtų priskirti šias nukentėjusių fizinių ir juridinių asmenų veiklos sąlygas:

- veiklos sritis arba darbo pobūdis (ūkinė, gamybinė, komercinė, valdymo, informacinė, tarpininkavimo, finansinė, energetinė, paslaugų ir kita veikla);
- juridinio ar fizinio asmens nuosavybės forma, informacinių sistemų ir informacinių išteklių, kaip nuosavybės dalies, teisinis statusas;
- gamybinių ar valdymo procesų paskirtis ir organizacinė struktūra, naudojamų išteklių ir gaminamos produkcijos, taip pat ir intelektualios, pobūdis;
- apskaitos ir atsiskaitomybės sistemos pobūdis;
- žmoniškųjų išteklių (personalo) valdymas ir materialinis-techninis aprūpinimas;
- naudojamų kompiuterinių sistemų, telekomunikacijų Įrangos rūšys, jų techniniai duomenys ir konstrukciniai trūkumai;
- patalpų ir Įrangos pobūdis;
- produkcijos, kitų vertybių apskaitos ir realizavimo tvarka;
- visų grandžių apsaugos sistemų pobūdis (apsaugos priemonių egzistavimas, techninė būklė ir kt.).

Prie subjektyvių faktorių galima būtų priskirti šias nukentėjusių fizinių ir juridinių asmenų veiklos organizacinio, socialinio, psichologinio pobūdžio sąlygas:

- informacijos apdorojimo technologinių procesų, gamybos, diegimo, derinimo, remonto, techninio aptarnavimo, kompiuterinių sistemų eksploatavimo, taip pat vertybių apskaitos, saugojimo, skirstymo, panaudojimo tvarką reglamentuojančių taisyklių pažeidimas ir nesilaikymas;
- šių taisyklių netobulumas;
- informacijos apsaugos priemonių nebuvimas ar netobulumas;
- darbo su Įstatymų saugoma kompiuterine informacija (pvz., valstybės, tarnybos ar komercinėmis paslaptimis) taisyklių pažeidimas;
- nepagrĮstas kompiuterinių sistemų naudojimas konkrečiuose technologiniuose procesuose ir operacijose;

[26] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно вычислительной техники. Волгоград, 1998. Стр.17.

- nepatenkinamas gamybinių ar valdymo procesų organizavimas, dokumentų administravimo sistemos trūkumai, pvz., dokumentų neautomatizuotos („rankinės“) ir automatizuotos apskaitos egzistavimas tuo pačiu metu;
- netinkama psichologinė darbo aplinka (problemiški asmeniniai santykiai tarp vadovų ir pavaldinių, kitų darbuotojų, atsakomybės masto ir darbo užmokesčio neatitikimas).

Tiek objektyvūs, tiek subjektyvūs faktoriai gali stipriai Įtakoti konkretaus kompiuterinio nusikaltimo Įvykdymo aplinkybes.

4.1. KOMPIUTERINIŲ NUSIKALTIMŲ SUBJEKTO CHARAKTERISTIKA

Svarbi nusikaltimų, susijusių su kompiuterinės technikos panaudojimu, kriminalistinės charakteristikos dalis yra duomenys, apibūdinantys nusikaltimo subjektą.

Asmenys, darantys kompiuterinius nusikaltimus, pagal specializaciją skirstomi Į kelias grupes[27], nusikaltėlių žargonu vadinamas " hakeriais", "krekeriais", " frekeriais", „karderiais" *(angl.k. „hacker", „cracker", „phracker", „carder").* Hakeris – tai kompiuterio, informacinės sistemos ar tinklo vartotojas, kuris dažniausia savanaudiškais tikslais užsiima nesankcionuotos prieigos prie kompiuterinių sistemų ar Įstatymų saugomos kompiuterinės informacijos būdų paieška. Krekeris – kompiuterio, informacinės sistemos arba tinklo vartotojas, kuris specializuojasi Įstatymų saugomos kompiuterinės informacijos programinių ir techninių apsaugos priemonių „nulaužimo" srityje (modifikavimo, blokavimo, sunaikinimo). Karderiai – tai profesionalūs nusikaltėliai, užsiimantys neteisėta veikla elektroninių kortelių apyvartos bei elektroninių rekvizitų padirbimo ir klastojimo srityje. Frekerių specializacija – nusikaltimai elektroninių ryšių, telekomunikacijų srityje, panaudojant konfidencialią informaciją ir specialias technines priemones, skirtas srauto duomenų ir turinio perėmimui.

Įvairių šalių kriminalistų duomenimis, hakeriai ir kiti kompiuteriniai nusikaltėliai veikia tiek pavieniui, tiek jungdamiesi Į regionines grupes, be to, naudojasi internetu savo „profesinei" informacijai skleisti bei keistis patirtimi tarptautiniu mastu, jų elektroniniuose leidiniuose pateikiama Įvairių kompiuterinių nusikaltimų Įvykdymo metodika ir nuslėpimo būdai, kiti duomenys, padedantys jauniems pažeidėjams tobulėti. V.B.Vechovo pastebėta, jog Rusijoje šie asmenys leidžia savo elektronines masinės informacijos priemones (laikraščius, žurnalus, skelbimų lentas su skubiais pranešimais), rengia elektronines konferencijas, kiekviena grupė ("hakeriai", "krekeriai", "frekeriai", „karderiai") turi savo žargoninĮ žodyną, kuris yra nuolat papildomas ir platinamas elektroniniais leidiniais. Be to, nusikaltėliai glaudžiai bendradarbiauja su užsienio „kolegomis", naudodamiesi globaliais telekomunikaciniais tinklais.

Kompiuteriniai nusikaltėliai priklauso Įvairiems visuomenės sluoksniams – nuo moksleivių ir studentų mėgėjų iki profesionalių nusikaltėlių, teroristų grupuočių, pagal išsilavinimą šiuos asmenis galima suskirstyti Į diletantus ir profesionalus. Nusikaltėlių amžius svyruoja nuo 15 iki 45 metų, Europos ir JAV tyrėjų duomenis, nusikaltimo Įvykdymo metu 33 proc. nusikaltėlių amžius neviršijo 20 metų, 13 proc. – vyresni nei 40 metų ir 54 proc. – nuo 20-40 metų. Lietuvos Respublikos vidaus reikalų ministerijos Įtariamų, kaltinamų ir teistų asmenų žinybinio registro duomenimis, asmenų, kaltinamų nusikalstamos veikos, kurios pasikėsinimo dalykas - kompiuterinė informacija ir sistemos, o priemonė - kompiuterinė technika ar internetas, padarymu, amžius toks:

[27] В. Голубев. Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий // http://www.crime-research.org; prisijungimo laikas: 2006-07-10

iki 20 metų – beveik 22 proc., vyresni nei 40 metų – 14 proc., nuo 20 iki 40 metų – 64 proc. (žr. 4 priedo 9 lentelė); šių asmenų išsilavinimas: aukštasis – 22 proc., aukštesnysis arba profesinis – 23 proc., vidurinis, pagrindinis ar pradinis – 55 proc. (žr. 4 priedo 10 lentelė); užimtumas: valstybės tarnautojai – 9 proc., nevalstybinių Įstaigų ir Įmonių darbuotojai – 34 proc., moksleiviai ir studentai – 21 proc., nedirbantys ir nesimokantys – 36 proc. (žr. 4 priedo 11 lentelė). Palyginus pasaulio ir Lietuvos kompiuterinių nusikaltimų tendencijas bei Įvertinus šių nusikaltimų latentiškumą, galima daryti prielaidą, jog šiuo metu Lietuvoje išaiškinama daugiausia santykinai nesudėtingų kompiuterinių nusikaltimų, nes daugiau nei pusė juos padariusių asmenų teturi vidurinĮ ar žemesnĮ išsilavinimą, kai tuo tarpu kitose Europos valstybėse ir JAV didžioji dalis šių asmenų priskiriami „baltųjų apykaklių“, t.y. turinčių aukštąjĮ išsilavinimą tarnautojų ir darbuotojų, kategorijai.

Mokslo leidiniuose asmenys, darantys kompiuterinius nusikaltimus, skirstomi Įvairiais pagrindais, pvz., pagal jau minėtą specializaciją, taip pat pagal motyvaciją (skiriamos trys grupės: hakeriai, tipiniai nusikaltėliai ir vandalai), pagal organizacinę priklausomybė (skiriami asmenys, susiję su Įstaiga, Įmone 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 nuostolingiausius ekonominius nusikaltimus. Nuo pirmųjų dviejų grupių ji skiriasi tuo, kad turi aiškią nusikalstamą motyvaciją, o jų veikla pasižymi pakartotinumu ir organizuotumu.

Asmenų, darančių kompiuterinius nusikaltimus, veikos skirstomos Į vidaus ir išorės pasikėsinimus. Svarbu pastebėti, jog didžioji dalis kompiuterinių nusikaltimų juridinio asmens atžvilgiu Įvykdomi nusikaltėlio arba jo bendrininko, kurie yra tos Įstaigos, organizacijos ar Įmonės darbuotojai (vidaus pasikėsinimai sudaro apie 80 proc. visų nusikaltimų, 90 proc. ekonominių kompiuterinių nusikaltimų padaro Įstaigų ir Įmonių darbuotojai). Šie asmenys paprastai yra puikiai Įvaldę specialias žinias ir turi praktinės patirties kompiuterinių technologijų srityje. Dažniausiai šie asmenys dirba kompiuterių tinklų ar ryšio 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 informacinės sistemos, duomenų bazių ar telekomunikacinio tinklo.

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

sritis. Dažniausiai šie asmenys nebūna patekę teisėsaugos akiratin, anksčiau neĮvykdę jokių nusikaltimų.

Būtina pastebėti, kad vis dažniau kompiuteriniai nusikaltimai yra Įvykdomi organizuotų nusikaltėlių grupių, kurioms būdinga aiški motyvacija siekiant naudos, geras techninis aprūpinimas, mobilumas, tikslus vaidmenų pasidalinimas, gerai apgalvota nusikalstamos veiklos pėdsakų slėpimo sistema. Didžiausią pavojų kelia bei sunkiausiai išaiškinamos tos nusikalstamos grupuotės, kuriose dirba aukštos kvalifikacijos informatikos specialistai, ekonomistai, teisininkai, turintys specialių žinių ir patirties kompiuterinės informacijos apsaugos srityje. Didelė dalis nusikaltimų, Įvykdytų šių grupuočių, išlieka latentiniais. Įtariamų, kaltinamų ir teistų asmenų žinybinio registro duomenimis, beveik 30 proc. asmenų, kaltinamų nusikalstamų veikų, kurių pasikėsinimo dalykas - kompiuterinė informacija ir sistemos, o priemonė - kompiuterinė technika ar internetas, padarymu, Įvykdė veikas būdami bendrininkų ar organizuotoje grupėje (pastarosios nariais buvo apie 3 proc. asmenų) (žr. 4 priedo 12 lentelė).

Galima konstatuoti, jog kompiuterinių nusikaltimų Įvykdymo **motyvai ir tikslai** yra labai skirtingi:

- pasipelnymas (neteisėtas pinigų, vertybinių popierių, kredito, materialinių vertybių, prekių, paslaugų, privilegijų, lengvatų, kvotų, nekilnojamojo turto, energetinių ir kitų išteklių gavimas);
- mokesčių, rinkliavų mokėjimo vengimas;
- nusikalstamais būdais gautų pajamų legalizavimas;
- dokumentų, antspaudų, blankų, piniginių ženklų klastojimas ar gamyba savanaudiškais tikslais;
- konfidencialios ar Įslaptintos informacijos gavimas pasipelnymo ar politiniais tikslais;
- kerštas dėl asmeninio priešiškumo darbovietės administracijai ar kolegoms;
- šalies valiutos sistemos dezorganizavimas piktavališkais ar politiniais tikslais; padėties šalyje, atskiroje gyvenamoje vietovėje ar Įstaigoje destabilizavimas politiniais tikslais;
- pastangos nuslėpti kitą nusikaltimą;
- chuliganiškos paskatos;
- tyrinėjimo tikslai;
- asmeninių intelektualinių galimybių ir pranašumo demonstravimas.

Pagal statistinĮ populiarumą asmenų, darančių kompiuterinius nusikaltimus, motyvus

ir tikslus Interpolo ekspertų komisija skirsto taip[28]:

1) savanaudiški – didžioji dalis, 66 proc.;

2) politiniai (terorizmas, politinės akcijos) – 17 proc.;

3) tiriamieji – 7 proc.;

4) chuliganiški – 5 proc.;

5) kerštо – 4 proc.

Apibendrinant kompiuterinių nusikaltimų subjektų charakteristiką, galima pateikti šiuos bendruosius užsienio valstybių duomenis [29]: 1) amžius: 54 proc. – 20-40 metų; 33 proc. – jaunesni kaip 20 metų; 13 proc. – vyresni kaip 40 metų; 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. – nusikalstamų grupių nariai; 38 proc. – veikia be bendrininkų.

Lyginamieji užsienio valstybių ir Lietuvos kompiuterinių nusikaltimų subjektų duomenys:

Rodiklis		**Užsienio valstybių duomenys, proc.**	**Lietuvos duomenys, proc.**
1. Amžius:	20-40 metų –	54	64
	jaunesni kaip 20 metų –	33	22
	vyresni kaip 40 metų –	13	14
2. Išsilavinimas:	aukštasis –	40	22
	specialusis (aukštesnysis arba profesinis) –	40	23
	vidurinis (ir žemesnis) –	20	55
3. Organizuotumas:	nusikalstamų grupių nariai –	62	29
	veikia be bendrininkų –	38	71

Palyginus pasaulio ir Lietuvos kompiuterinių nusikaltimų tendencijas bei įvertinus šių nusikaltimų latentiškumą, galima daryti prielaidą, jog šiuo metu Lietuvoje išaiškinama daugiausia santykinai nesudėtingų kompiuterinių nusikaltimų, nes daugiau nei pusė juos padariusių asmenų teturi vidurinį ar žemesnį išsilavinimą, be to, mažiau nei trečdalis jų yra nusikalstamų grupių nariai, kai tuo tarpu kitose Europos valstybėse ir JAV didžioji dalis šių asmenų priskiriami „baltųjų apykaklių“, t.y. turinčių aukštąjį išsilavinimą tarnautojų ir darbuotojų, kategorijai, o nusikalstamų grupių nariai sudaro net šešiasdešimt procentų visų padariusių kompiuterinius nusikaltimus asmenų.

[28] Голубев В. Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий // http://www.crime-research.org; prisijungimo laikas: 2006-05-06.
[29] Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija.- Vinius, 2000. P.23.

4.2. KOMPIUTERINIŲ NUSIKALTIMŲ ĮVYKDYMO LAIKAS IR VIETA

Apibūdinant kompiuterinių nusikaltimų laiką ir vietą, būtina pastebėti šių aplinkybių išskirtinumą, kurĮ sąlygoja tai, jog kompiuteriniai nusikaltimai paprastai yra vykdomi nuotoliniu būdu, naudojant nutolusius terminalus, kuriuos sieja su atakos objektu elektroninio ryšio kanalai, tačiau pasitaiko ir tiesioginės prieigos atvejų. Taigi, pirma, faktinė neteisėtos veikos Įvykdymo vieta ir visuomenei pavojingų pasekmių atsiradimo vieta dažniausiai nesutampa; antra, veikos Įvykdymo ir pasekmių atsiradimo laikas taip pat gali skirtis, pati ataka gali trukti labai trumpai, nes vykdoma naudojant specialias technines ir programines priemonės, nors pasirengimo veikai stadija gali būti pakankamai ilga. Tiek planuojant tokio pobūdžio nusikaltimą, tiek jĮ Įvykdant būtinos Įvairių sričių specialiosios žinios (informacijos apdorojimo ir apsaugos, finansinių ir bankinių operacijų, techninės ir programinės Įrangos), taip pat paprastai reikalingas detalus nusikaltimo Įvykdymo planas bei kiti duomenys, padedantys nepalikti jokių pėdsakų.

Būtina pastebėti, kad kompiuteriniai nusikaltimai gali būti vietiniai, lokalūs arba tarptautiniai, transnacionaliniai, taigi tiriant šios kategorijos nusikaltimų bylas, nusikalstamo pasikėsinimo vieta gali būti:

1) Įstaiga, organizacija ar Įmonė, kuri naudoja kompiuterinę Įrangą kuriame nors iš technologinių ar administracinių procesų;

2) konkreti, apibrėžta teritorija ar sritis, iš kurios galima realizuoti prieigą;

3) neapibrėžta teritorija, jei kompiuterinės atakos objektas Įjungtas Į tarptautinĮ elektroninių ryšių tinklą (tai gali būti kita valstybė, kitas žemynas).

Tiriant kompiuterinių nusikaltimų bylas, veikos Įvykdymo laikas gana retai nustatomas labai tiksliai, tačiau būna atvejų, kai laiką būtina fiksuoti valandų ar minučių tikslumu, siekiant išsiaiškinti atskirus nusikalstamos veikos epizodus. Paprastai kompiuterinių nusikaltimų Įvykdymo laikas apskaičiuojamas tam tikrais tarpsniais, susijusiais su konkrečių fizinių ar juridinių asmenų veikla. Baudžiamąja teisine prasme, nusikalstamos veikos Įvykdymo laiku yra pripažĮstamas šios veikos vykdymo pabaigos laikas, nepriklausomai nuo pasekmių atsiradimo laiko.

4.3. KOMPIUTERINIŲ NUSIKALTIMŲ BŪDAI

Kriminalistikos metodikos darbuose paprastai pabrėžiama, kad svarbiausiu bet kurios rūšies nusikaltimo kriminalistinės charakteristikos elementu yra duomenų, charakterizuojančių jo Įvykdymo būdą, visuma. Baudžiamojoje teisėje nusikaltimo būdas yra objektyviosios nusikaltimo sudėties pusės požymis, kuris gali būti tik fakultatyvinis, jei jis nenurodytas konkrečioje nusikaltimo sudėtyje, arba būtinasis (Įrodinėtinas) požymis, jei yra nurodytas. Kriminalistikoje nusikaltimo Įvykdymo būdas suprantamas kaip nusikaltimo subjekto veiksmų visuma rengiant, vykdant bei slepiant nusikaltimą, t.y. pažeidėjo veiksmai iki nusikaltimo padarymo, nusikaltimo padarymo metu ir po nusikaltimo, suformuojantys tam tikrus pėdsakus.

Kompiuterinių nusikaltimų Įvykdymo būdų išmanymas palengvina kompiuterinių nusikaltimų tyrimą, nes kiekvienas būdas palieka atitinkamus pėdsakus, padeda apibūdinti nusikaltėlio asmenybę ir kryptingiau formuoti versijas, atsižvelgiant Į metodus ir jų taikymo sąlygas, būtinos tam technines priemones, šaltinius, iš kurių jos gautos ir kt.

Visi kompiuterinių nusikaltimų Įvykdymo ir nuslėpimo būdai turi savo individualius, tik jiems būdingus požymius, pagal kuriuos galima juos atpažinti ir suskirstyti Į atskiras apibendrinančias grupes. Pagrindinis klasifikuojantis požymis yra **metodas**, kurio pagalba nusikaltėlis vykdo tikslingą poveikĮ kompiuterinės technikos priemonėms ir kompiuterinei informacijai. JAV Nacionalinio kompiuterinio saugumo instituto duomenimis, pagrindiniai kompiuterinių nusikaltimų metodai, kuriais neteisėtai užvaldoma informacija, yra šie:

- pasiklausymo Įrangos panaudojimas;
- nuotolinis fotografavimas;
- elektroninio spinduliavimo perėmimas;
- akustinio spinduliavimo perėmimas ir spausdintuvo teksto atkūrimas;
- mistifikacija (prisidengimas teisėta sistemos užklausa);
- informacijos kaupiklių ir pramoninių atliekų (šiukšlių) pagrobimas ar surinkimas;
- informacijos nuskaitymas iš kitų vartotojų masyvų;
- informacijos kaupiklių kopijavimas, Įveikiant apsaugos priemones;
- apsimetimas registruotu vartotoju;
- programinių spąstų panaudojimas;
- neteisėtas prisijungimas prie Įrangos ar ryšio linijų;
- apsaugos sistemų sugadinimas.

V.B.Vechovas, laikydamasis kompiuterinio nusikaltimo traktavimo plačiąja prasme,

skiria šias apibendrintas metodų grupes[30]:

1. kompiuterinės technikos pagrobimas;
2. informacijos perėmimas;
3. nesankcionuota prieiga prie kompiuterinės sistemos ar kompiuterinės informacijos;
4. manipuliavimas duomenimis ar valdymo komandomis;
5. kompleksiniai metodai.

Pirmajai grupei priskiriami tradiciniai nusikaltimų Įvykdymo būdai, kuriais nusikaltėlis siekia pasisavinti svetimą turtą (t.y. bet kokią kompiuterinę techniką, Įrenginį) ir Įvykdo vagystę ar grobimą.

Antrajai kompiuterinių nusikaltimų Įvykdymo būdų grupei priskiriami tokie būdai, kuriais nusikaltėlis kompiuterinę informaciją gauna panaudodamas audiovizualinio ir elektromagnetinio informacijos perėmimo metodus, taikomus ir teisėsaugos pareigūnų operatyvinės paieškos metu. Šiai grupei priklauso:

1. Pasyvus (bekontaktinis) perėmimas, vykdomas nuotoliniu būdu perimant elektromagnetinĮ spinduliavimą, skleidžiamą veikiančios kompiuterinės Įrangos:

a) optinių (vaizdo) signalų, sklindančių matomų, infraraudonųjų ir ultravioletinių spindulių diapazone, perėmimas (vykdomas naudojant optines, optines elektronines, televizines, lazerines, foto ir kitas vaizdo informacijos perėmimo priemones);

b) akustinių (garso) signalų, sklindančių oro, vandens ar kietoje terpėje, perėmimas (vykdomas naudojant akustines, hidroakustines, viroakustines, lazerines ir seismines priemones);

c) elektromagnetinių signalų, sklindančių techniniais pagrindinių ir pagalbinių priemonių bei sistemų kanalais, kaip parazitinių informacinių laukų perėmimas: šalutinio elektromagnetinio spinduliavimo ir trukdžių, parazitinių aukšto dažnio signalų moduliacijų, parazitinių informacinių srovių ir Įtampų, sukuriamų dėl signalo elektroakustinio transformavimo radijo ir elektros ryšių, radijotransliaciniuose, apsaugos ir priešgaisrinės signalizacijos, televizijos, kompiuterinių sistemų tinkluose ir kt.

2. Aktyvus (kontaktinis) perėmimas, vykdomas tiesiogiai prisijungus prie kompiuterinės sistemos arba prie duomenų perdavimo sistemos, panaudojant Įvairias operatyvines technines ir specialiai pagamintas (pritaikytas) priemones, kai kuriais atvejais panaudojant slaptus kanalus. Šiuo atveju nusikaltėlis gali tikslingai paveikti visą kompiuterinę sistemą, jos sudėtines dalis, prieigos sankcionavimo sistemą, duomenų perdavimo kanalus ir pačią kompiuterinę informaciją.

---

[30] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники.- Волгоград, 1998. Стр.21.

Trečiajai grupei priskiriami kompiuterinių nusikaltimų Įvykdymo būdai, Įgalinantys gauti neteisėtą prieigą prie kompiuterinės sistemos, pavyzdžiui, pasinaudojant „legendos“ metodu („elektrikas“, „santechnikas“, „telefonų meistras“ ir kt.), taip pat nesankcionuoto prisijungimo prie kompiuterinės informacijos perdavimo sistemos, perimant abonento kreipimosi Į tinklą valdymą, metodu ir pan.

Ketvirtajai grupei priskiriami kompiuterinių nusikaltimų Įvykdymo būdai, susiję su Įeinančių ir išeinančių duomenų bei kompiuterinės technikos valdymo komandų manipuliavimo metodų panaudojimu. Šie metodai naudojami labai dažnai ir gerai žinomi ekonominių nusikaltimų tyrimo tarnybų pareigūnams, pavyzdžiui, buhalterinės apskaitos Įeinančių ir išeinančių duomenų pakeitimas automatizuoto dokumentų apdorojimo proceso metu arba tyčinis programos pakeitimas, kuris sąlygoja nesankcionuotą informacijos sunaikinimą, blokavimą, modifikavimą arba kopijavimą, taip pat kompiuterių, jų sistemos ar tinklo darbo sutrikdymas (naudojami populiarieji būdai „Trojos arklys“, „Saliami“, „Aitvaras“, „Laiko bomba“ ar „Loginė bomba“, „Liukas“, kompiuteriniai virusai ir pan.).

Penktajai grupei priklauso kompleksiniai kompiuterinių nusikaltimų Įvykdymo būdai, kai nusikaltėlis panaudoja kelis skirtingų grupių būdus, iš kurių vienas visada būna naudojamas kaip pagrindinis, o kiti vykdo pagalbines funkcijas, pavyzdžiui naudojami nusikaltimo pėdsakams nuslėpti.

J.M.Baturinas skiria tris pagrindines kompiuterinių nusikaltimų Įvykdymo būdų grupes: perėmimo, neteisėtos prieigos ir manipuliacijų [31]. Reikia pastebėti, jog daugelio Rusijos ir kitų Europos šalių specialistų nuomonė dėl tokio kompiuterinių nusikaltimų Įvykdymo būdų klasifikavimo iš esmės sutampa, tačiau nurodoma ir ketvirtoji – kompleksinių metodų grupė. Įvertinus kompiuterinių nusikaltimų Įvykdymo būdų ypatumus, autorės manymu, ši jų klasifikacija pagal metodus yra optimaliausia:

1. perėmimo metodai;
2. neteisėtos prieigos metodai;
3. manipuliacijų metodai;
4. kompleksiniai metodai.

1. Perėmimo metodai:

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

[31] Батурин Ю.М. Проблемы компьютерного права.- Москва, 1991. Стр.22.

2) elektromagnetinis perėmimas – įvykdomas per įrangos šalutinį spinduliavimą (vaizduoklio, spausdintuvo, ryšio sistemų), be to, pakankamai dideliu atstumu nuo spinduliuojančio objekto.

Netiesioginio (nuotolinio) perėmimo metodams priskirtini ir audio perėmimas (informacijos nuskaitymas per vibroakustinį kanalą) bei video perėmimą (informacijos gavimas panaudojant videooptinę įrangą).

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

2. Neteisėtos prieigos metodai

Šiai grupei priskiriami nusikaltėlių veiksmai, siekiant neteisėtai 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 neteisėtas patekimas į 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 tęsimas vartotojo vardu.

“Įsilaužimas” *(hacking)* – šis metodas paprastai naudojamas įsiskverbimui į svetimas informacines sistemas, naudojantis specialia programine įranga, parenkant identifikuojančius teisėtų vartotojų požymius (paprastai slaptažodžius ir vardus).

“Lėtas parinkimas (lėta atranka)” *(browsing)* – tai prisijungimas prie kompiuterio vieną kartą aptikus silpnąsias apsaugos sistemos vietas ar trūkumus 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.

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

“Maskaradas (apsišaukėlis)” *(masquerading)* – tai įsiskverbimas į kompiuterinę sistemą, apsimetant teisėtu vartotoju, sužinojus jo kodą ar slaptažodį, jei nėra galimybių papildomai identifikuoti asmenį.

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

[32] Мелик Э. Компьютерные преступления. Информационно-аналитический обзор // http://www.melik.narod.ru; prisijungimo laikas: 2006-06-08.

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

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

"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. Manipuliacijų metodai

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

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

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

Modeliavimas – tai programinės įrangos naudojimas modeliuojant, kaip elgsis įrenginys arba sistema. Šis metodas naudojamas analizuojant procesus, į kuriuos nusikaltėliai planuoja įsiterpti, ir planuojant nusikaltimo įvykdymo metodus.

„Trojos arklys" – tai būdas, kurio metu į programą slaptai įrašomos tokios komandos, kurios padeda įvykdyti kitas, programos savininko nenumatytas, funkcijas, tačiau tuo pat metu išsaugomas ir pirminis programos funkcionalumas. Tai vizualiai užmaskuotas būdas, nes „Trojos arklio" programėlė įrašoma šalia kitos programos arba įvedama į jos vidų ir tik tuomet pagrindinė programa atlieka vienokio arba kitokio pobūdžio pakeitimus. Literatūroje minimos dvi „Trojos arklio" atmainos: 1) „Trojos kirminas" – tai programinis modulis, kai į programos darbo algoritmą, be pagrindinių funkcijų, įvedama veiksmų algoritmo funkcija, kuri atlieka automatišką „Trojos arklio" atsinaujinimą, o tinkle tokios programos save automatiškai kopijuoja į kitus kompiuterius; 2) „Trojos matrioška" – tai ypač sunkiai aptinkamas programinis modulis, kuris sukuria „Trojos arklį" 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 kitų programų (užkrėsti jas) ir jas paleidžiant vykdyti įvairius neplanuotus, nepageidaujamus veiksmus: trinti duomenis ir informaciją, gadinti failus ir katalogus, perpildyti kompiuterio atmintį, sutrikdyti jo darbą. Dažniausiai užkrečiamos *.com, *.exe, *.bat, *.sys, *.do*, *.xl* tipo bylos. Virusai, kurie skaičiuojami tūkstančiais, skirstomi į kelias grupes: standartiniai *COM-EXE-TSR* virusai, Stels *(Stealth)* virusai, polimorfiniai *(polymorphic)* virusai, „kompiuteriniai kirminai“ *(worm)*, makrovirusai ir kt.

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

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

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

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

4. Kompleksiniai metodai

Šiai grupei priskiriami nusikaltėlių veiksmai, kuriais siekiama neteisėtai prieiti prie kompiuterio, jų tinklo ir saugomų išteklių, perimti informaciją bei manipuliuojama duomenimis arba kompiuterio komandomis, t.y. nusikalstamiems tikslams pasiekti kompleksiškai naudojami keli skirtingų grupių būdai. Optimaliausias konkrečiomis aplinkybėmis nusikaltimo būdas pasirenkamas ir naudojamas kaip pagrindinis, o kiti naudojami pagalbinėms funkcijoms vykdyti, paprastai nusikaltimui maskuoti, pėdsakams nuslėpti.

Apibendrinant galima konstatuoti, kad praktiškai neįmanoma pateikti visų kompiuterinių nusikaltimų įvykdymo būdų išsamaus sąrašo, nes jų turinys gali būti sudarytas iš įvairiausių veiksmų derinių, priklausančių nuo pažeidėjo išradingumo, kvalifikacijos ir intelekto. Dažniausiai minimi šie veiksmai: kenkėjiškų kompiuterinių programų ar kaupiklių su tokiomis programomis naudojimas arba platinimas; kompiuterinės informacijos perėmimas; neteisėta prieiga prie kompiuterinės informacijos; manipuliacija duomenimis ar valdančiomis programomis; kompiuterinės technikos, ryšių įrangos, kompiuterinės informacijos apsaugos, konfidencialios kompiuterinės informacijos apdorojimo, saugojimo ir perdavimo priemonių eksploatavimo taisyklių

pažeidimas; kompiuterinės informacijos blokavimas, modifikavimas, kopijavimas, sunaikinimas, panaudojant specialiai sukurtas, pritaikytas, užprogramuotas technines priemones ir kt. Tačiau, nepaisant kompiuterinių nusikaltimų Įvykdymo būdų Įvairovės, juos galima sugrupuoti pagal metodus Į keturias grupes: 1) perėmimo; 2) neteisėtos prieigos; 3) manipuliacijų; 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, Įvykdymo būdus, nes nusikalstamos veikos statistinėje kortelėje (10 kortelė) tokio pobūdžio veikos pagal padarymo būdą skirstomos tik Į dvi apibendrintas grupes: „panaudojant kompiuterinę Įrangą“ (20 proc.) ir „pasinaudojant netikra mokėjimo kortele“ (80 proc.) (žr. 4 priedo 4 lentelė), be to, atlikus minėto registro duomenų analizę, paaiškėjo, jog tyrėjai, pildydami statistines korteles, fabuloje taip pat nenurodo tikslių nusikalstamų veikų padarymo būdų ar metodų.

Siekiant gauti praktinių duomenų apie kompiuterinių nusikaltimų Įvykdymo 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 kompiuterinių nusikaltimų Įvykdymo būdai: 1) tiesioginis perėmimas, priklausantis perėmimo metodų grupei; 2) Įsilaužimas (hacking), priklausantis neteisėtos prieigos metodų grupei; 3) „Trojos arklys“ ir kompiuteriniai virusai, priklausantys manipuliacijų metodų grupei.

4.4. KOMPIUTERINIŲ NUSIKALTIMŲ PRIETAISAI IR PRIEMONĖS

Universaliausia ir plačiausiai naudojama kompiuterinių nusikaltimų vykdymo priemonė, žinoma, yra asmeninis kompiuteris, kuriame įdiegta speciali programinė įranga ir atitinkami išoriniai įrenginiai. Tačiau rengiant, vykdant ir nuslepiant tokio pobūdžio nusikalstamas veikas, naudojami įvairiausi prietaisai bei priemonės, kurie kriminalistikos metodiniuose leidiniuose paprastai suskirstomi į dvi apibendrintas grupes: bendruosius techninius ir specialiuosius kompiuterinius.

1. Bendrieji techniniai prietaisai ir priemonės

Bendrieji techniniai prietaisai ir priemonės naudojami kompiuterio, kompiuterių tinklo ar informacinės sistemos veiklai sutrikdyti ir informacijai gauti, pakeisti, sunaikinti ar blokuoti. Šie prietaisai ir priemonės gali būti standartiniai, legaliai įsigyti ir pritaikomi kompiuteriniams nusikaltimams vykdyti arba savadarbiai, specialiai modifikuoti, užprogramuoti.

Bendrųjų techninių prietaisų ir priemonių grupei priskiriami:

Įvairūs montavimo įrankiai, elektros montavimo instrumentai ir medžiagos;

Įvairios magnetinės medžiagos ir techninės priemonės, sukuriančios kryptinį magnetinį lauką;

elektromagnetinio spinduliavimo registravimo įrenginiai;

garso ir vaizdo įrašymo įranga;

pasiklausymo įranga;

kontroliniai matavimo prietaisai ir įrenginiai;

ryšių sistemų priemonės ir jų komponentai.

2. Specialieji kompiuteriniai prietaisai ir priemonės

2.1. Techninė įranga – tai patys kompiuteriai ir kita kompiuterinė technika (taip pat ir įranga, kuri nėra kompiuterinė bendrąją prasme, pvz., perprogramuojama mikroschema PIC), išoriniai įrenginiai.

2.2. Programinė įranga – tai ir standartinė, laisvai platinama įranga (kurios poveikio rezultatai yra lengvai prognozuojami bei analizuojami) ir specialios programinės priemonės (kurių poveikį tirti žymiai sudėtingiau) – komandų arba mnemokodų sistema, valdanti informacinius procesus, kurios pagalba vykdomos įvairios manipuliacijos su kompiuterine informacija.

Specialiųjų kompiuterinių prietaisų ir priemonių grupei priskiriama:

Įvairios elektroninės skaičiavimo technikos rūšys (asmeniniai kompiuteriai, kompiuterių tinklo ar telekomunikacinio tinklo darbo ir tarnybinės stotys (serveriai), judriojo

(mobilaus) ryšio Įrenginiai, turintys duomenų perdavimo internetu funkciją, bankomatai, kasos aparatai, turintys fiskalinės atminties bloką, elektroninės užrašų knygutės ir kt.);

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

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

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

kenkėjiškos kompiuterinės programos (kompiuteriniai virusai, „Trojos arklys“ ir kitos), kompiuterinės informacijos apsaugos sistemų Įveikimo programos (apsaugos kodų Įveikimo (nulaužimo) programa, prieigos kodų generatorius, kriptografinės apsaugos dešifravimo Įranga ir kt.).

Lietuvos Respublikos vidaus reikalų ministerijos Nusikalstamų veikų žinybiniame registre nėra kaupiami detalūs duomenys apie nusikalstamų veikų, 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 Į tris apibendrintas grupes: kompiuterinė technika (74), internetas (75), netikra mokėjimo kortelė (76), nedetalizuojant, kokie tiksliai kompiuteriniai prietaisai ir priemonės buvo panaudoti konkrečiai nusikalstamai veikai Įvykdyti 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 nusikalstamų veikų, kurių padarymo priemonė – internetas, ir 584 nusikalstamos veikos, kurių padarymo priemonė – netikra mokėjimo kortelė.

III. KOMPIUTERINIŲ NUSIKALTIMŲ TYRIMO METODIKOS YPATUMAI

5. KOMPIUTERINIŲ NUSIKALTIMŲ TYRIMO VEIKSMAI

5.1. ĮRODINĖTINOS APLINKYBĖS

Tiriant kompiuterinĮ nusikaltimą, tyrėjui būtina išsiaiškinti, kokios aplinkybės Įrodinėtinos šiuo konkrečiu atveju, nes kaip tik tai leis tinkamai suformuluoti tyrimo užduotis. Žinoma, kad patraukti baudžiamojon atsakomybėn asmenĮ galima tik tuomet, kai nustatoma, jog konkreti jo veika atitinka baudžiamojo kodekso straipsnio nustatytą abstrakčią nusikaltimo sudėtĮ, tačiau kompiuterinio nusikaltimo atveju tyrėjui būtinos ne tik baudžiamosios teisės materialinės ir procesinės žinios, kriminalistikos žinios, bet ir specialios informacinių technologijų žinios.

Daugelyje kriminalistikos metodikos darbų pateikiamas toks apibendrintas Įrodinėtinų aplinkybių sąrašas: nusikaltimo sudėties elementai; kvalifikuojančios aplinkybės, sunkinančios ir lengvinančios atsakomybę aplinkybės bei šalinančios baudžiamąją atsakomybę aplinkybės. V.B.Vechovas bei kiti mokslininkai, apibendrindami nusikaltimų, susijusių su kompiuterinių technologijų panaudojimu, tyrimo praktiką, siūlo detalizuoti Įrodinėtinų aplinkybių sąrašą, atsižvelgiant Į šios rūšies nusikaltimų specifiką[33].

Įvertinus kompiuterinių nusikaltimų ypatybes, galima nurodyti šias pagrindines aplinkybes, kurios turėtų būti nustatytos ir Įrodytos kompiuterinių nusikaltimų bylose:

1. nusikaltimo Įvykdymo faktas ir tiesioginė kompiuterinės informacijos bei jos apdorojimo priemonių saugumo pažeidimo priežastis (t.y., ar veika yra nusikaltimas, ar kitos rūšies teisės pažeidimas, ar nelaimingas atsitikimas – nenugalimos jėgos aplinkybių (*forse majore*) pasekmė, pvz., oro sąlygų, gamtos katastrofų, vidinių techninių gedimų ar sutrikimų);

2. nusikalstamo pasikėsinimo objektas ir dalykas (tai turi lemiamą reikšmę tyrėjui pasirenkant vienokią ar kitokią nusikaltimo tyrimo metodiką); kompiuterinės informacijos kategorija (vieša, bendro naudojimo ar nevieša, Įslaptinta);

3. nusikaltimo Įvykdymo būdas (ar nusikaltimas Įvykdytas tiesioginiu, ar nuotoliniu būdu; jei nuotoliniu būdu,- ar naudojant vietinĮ (lokalų) kompiuterių tinklą ar internetą, ar kitus telekomunikacinius kanalus, ir kt.);

4. nusikaltimo Įvykdymo vieta (konkreti tos Įmonės, Įstaigos, organizacijos, kito objekto, teritorijos dalies vieta, kur Įvykdytas nusikaltimas);

5. nukentėjęs asmuo (fizinis ar juridinis asmuo); objekto, kuriame Įvykdytas nusikaltimas, pavadinimas, paskirtis, darbo režimas;

6. nusikaltimo Įvykdymo priemonės (bendrosios techninės Įrangos ar kompiuterinės

[33] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно вычислительной техники. Волгоград, 1998. Стр.24.

techninės ir programinės Įrangos tipas, rūšis, modelis, funkcinė paskirtis, techninė būklė ir kitos charakteristikos; konkretaus terminalo ar tinklo srities registracijos, abonentinis numeris, kodas, šifras, darbo dažnis);

7. kompiuterių tinklo ar informacinės sistemos darbo režimas (darbo su kompiuterine informacija, jos apdorojimo ir apsaugos priemonėmis tvarka);

8. nusikaltimo Įvykdymo laikas (laikotarpis).

9. žalos dydis ir jos sudėtis.

10. tarnybinės funkcijos, veiksmai ir technologinio proceso operacijos, su kuriais susijęs nusikaltimas;

11. asmenų, atsakingų ir tiesiogiai susijusių su gamybos technologija, informacijos apdorojimu, naudojimu ar administraciniu valdymu, sąrašas;

12. nusikaltimo subjektas (Įtariamojo asmenybės charakteristika, ar turi praktinių gebėjimų ir specialių žinių, kokios srities ir kokio lygio žinios būtinos nusikaltimui Įvykdyti); jei nusikaltimą Įvykdo grupė asmenų, jos sudėtis ir kiekvieno nario vaidmuo;

13. nusikaltimo motyvai ir tikslai (naudos siekimas, kerštas, chuliganiškos paskatos, asmeninių intelekto galimybių demonstravimas, kito nusikaltimo nuslėpimas ir kt.);

14. priežastinio ryšio buvimas tarp veikos ir atsiradusių pasekmių (būtina Įrodyti, kad konkretaus Įtariamo asmens veiksmai, kurie jam inkriminuojami, buvo atsiradusių pasekmių priežastimi);

15. priežastys ir sąlygos, paskatinusios Įvykdyti ir nuslėpti nusikaltimą (norminių teisės aktų, instrukcijų, taisyklių, darbo tvarkos reglamentavimo trūkumai ir pažeidimai, Įvykdyti trečiųjų asmenų, kurių būtent ir dėl kokių priežasčių, ar šie asmenys neturi būti patraukti baudžiamojon atsakomybėn už pažeidimus, kurie sudarė sąlygas Įvykdyti tiriamą nusikaltimą);

16. kam buvo žinomi nusikaltėlių ketinimai;

17. kas dalyvavo nuslepiant nusikaltimą ar jo pėdsakus.

5.2. TIPINĖS TYRIMO SITUACIJOS IR KRIMINALISTINĖS TYRIMO UŽDUOTYS

Kompiuteriniams nusikaltimams būdingas ypač didelis latentiškumas (manoma, jog jis gali siekti iki 90 proc.). Asmenys, rengiantys kompiuterinį nusikaltimą, paprastai labai tiksliai ir detaliai planuoja savo veiksmus, iš anksto numato pėdsakų slėpimo būdus, panaudoja įvairias nusikalstamos veikos maskavimo priemones, pasitelkdami subjektyvius ir objektyvius faktorius, (pavyzdžiui, įprastus kompiuterių darbo sutrikimus, ryšių, maitinimo įrangos gedimus, trumpuosius jungimus kabelių sistemose ir kt.), todėl ypač sudėtinga aptikti tokius nusikaltimus pasirengimo stadijoje bei rasti įvykdytų nusikaltimų pėdsakus. Be to, nukentėjęs nuo kompiuterinio nusikaltimo asmuo dažnai nėra labai suinteresuotas nusikaltėlio sulaikymu, o pats nusikaltėlis, jei būna sulaikomas, linkęs reklamuoti savo pasiekimus. Tai lemia šios priežastys: kompiuterinių nusikaltimų aukos dažniausiai mano, jog šių nusikaltimų padaryta žala yra mažesnė, nei nuostoliai, kuriuos gali sukelti jų atskleidimas (pvz., kredito įstaigų reputacijos praradimas), o patys kompiuteriniai nusikaltėliai, atskleidus jų nusikaltimus, tampa įžymūs tiek nusikalstamo, tiek legalaus verslo sferose (pasaulio praktikoje žinomas ne vienas atvejis, kai kompiuteriniams įsilaužėliams pasiūlydavo darbą informacinių technologijų saugos sistemų įmonės).

Taigi, kompiuterinius nusikaltimus tiriantys pareigūnai susiduria su įvairiomis kliūtimis: pirma, ypač kruopščiai parengtais intelektualiais nusikaltimais, antra, netipišku nukentėjusiųjų ir nusikaltėlių elgesiu. Vadinasi, aptikti šių nusikaltimų pėdsakus sudėtinga, o nusikaltimų tyrimo sėkmė 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 įranga padeda rasti nusikaltimo pėdsakus kompiuteryje ir jų tinkle bei nustatyti nusikaltėlio veiksmų seką.

Pirminių tyrimo, operatyvinių veiksmų visuma, jų atlikimo nuoseklumas priklauso nuo konkrečios tyrimo situacijos. Tyrimo situaciją sąlygoja tyrėjo turima pradinė kriminalistiniu požiūriu svarbi informacija. Ikiteisminis 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 masinės informacijos priemonėse, taip pat ir Internete. Paprastai prieš pradedant tyrimą yra atliekamas pirminis medžiagos, gautos teisėsaugos institucijų, patikrinimas, tyrėjas gali iš anksto susipažinti su surinkta medžiaga, kartu su operatyviniu darbuotoju pasirinkti taktiniu požiūriu tinkamiausius tyrimo metodus, nustatyti pirminių tyrimo veiksmų, organizacinių ir kitų priemonių pobūdį ir vykdymo nuoseklumą. Kompiuterinių nusikaltimų tyrimo sėkmę dažnai lemia tyrėjo veiksmų operatyvumas ir glaudus bendradarbiavimas su kompiuterinių technologijų srities specialistu.

Vykdant pirminį medžiagos patikrinimą, tyrėjas turi gauti kuo tikslesnius duomenis apie pasikėsinimo objektą, jo buvimo vietą ir fizinės apsaugos sąlygas, veiklos pobūdį, gamybos, valdymo, dokumentų administravimo procesų technologinius ypatumus, apskaitos ir atskaitingumo tvarką, naudojamos kompiuterinės technikos charakteristikas, informacijos apsaugos organizavimo principus. Be to, būtina žinoti sąrašą ir tarnybines pareigas tų asmenų, kurie turi tiesioginę ar netiesioginę prieigą prie kompiuterinės informacijos, jos apdorojimo priemonių, tapusių nusikalstamo pasikėsinimo objektu.

Galima paminėti šiuos tipinius pasirengimo įvykdyti kompiuterinį nusikaltimą, jo įvykdymo ar nuslėpimo požymius: suklastotų ar neatitinkančių duomenų aptikimas kompiuteryje, jų tinkle ar informacinėje sistemoje, dažni įrangos darbo sutrikimai, nesankcionuotas failų sistemos struktūros, kompiuterio programinės ar techninės įrangos, sistemos ar tinklo konfigūracijos pakeitimas, vartotojų nusiskundimai dėl sutrikusios prieigos prie kompiuterio, tinklo ar kompiuterinės informacijos, nereglamentuotos prieigos prie kompiuterio, tinklo ar atskirų vartotojų kompiuterinės informacijos užfiksavimas, darbo su kompiuterine informacija taisyklių pažeidimas, padidėjęs kai kurių darbuotojų ar kitų asmenų dėmesys saugomai kompiuterinei informacijai, įtartinas konkretaus vartotojo kreipimasis į tam tikros kategorijos duomenis ar kompiuterinę informaciją, atskirų duomenų kopijavimo atvejai be rimtų priežasčių, išorinių asmeninių informacijos kaupiklių naudojimas įvairiais motyvais darbo vietoje, konfidencialios informacijos atskleidimo atvejai arba slapto jos gavimo priemonių aptikimas, nustatytų darbo su kompiuteriu, tinklu ar kompiuterine informacija taisyklių pažeidimai.

Siekiant tiksliai išsiaiškinti nukentėjusiojo (fizinio ar juridinio asmens) veiklos ypatumus, tyrėjui reikia išanalizuoti žinybinius norminius teisės aktus, susipažinti su informaciniais dokumentais. Svarbu pabrėžti, kad pradedant kompiuterinio nusikaltimo tyrimą, būtina pasitelkti specialistus, turinčius profesionalių žinių ir patirties kompiuterinės informacijos apdorojimo bei apsaugos srityje.

Kriminalistikos mokslo darbuose skiriamos kelios tipinės kompiuterinių nusikaltimų tyrimo situacijos. Atsižvelgiant į duomenų apie įvykdytą nusikaltimą gavimo šaltinį, skiriami šie atvejai: nukentėjęs asmuo savarankiškai aptinka kompiuterinį nusikaltimą, numano, kas yra kaltininkas, ir praneša tai teisėsaugos įstaigai; nukentėjęs asmuo savarankiškai aptinka kompiuterinį nusikaltimą, tačiau nežino kaltininko ir praneša tai teisėsaugos įstaigai; įvykdyto kompiuterinio nusikaltimo duomenys paaiškėja iš kitų šaltinių (dažniausiai teisėsaugos pareigūnams tiriant kitą nusikaltimą).

Tiriant ekonominius nusikaltimus, įvykdytus panaudojant kompiuterinę įrangą, (sukčiavimą, turtinės žalos padarymą apgaule arba piktnaudžiaujant pasitikėjimu) skiriamos šios

tipinės tyrimo situacijos[34]: įtariamasis sulaikytas nusikaltimo vietoje su įkalčiais; įtariamojo asmenybė nenustatyta, tačiau žinomas jo nusikaltimo padarymo būdas ir vieta (panaudojus atokius nusikaltimo padarymo būdus); žinomi tik nusikaltimo padariniai.

Apibendrinant kriminalistikos teorijos bei praktikos darbuose nurodomas kompiuterinių nusikaltimų tipines tyrimo situacijas ir atsižvelgiant į turimų duomenų apie nusikaltimą ir įtariamąjį išsamumą, galima išskirti tris pagrindines situacijas:

1) nėra duomenų apie nusikaltimo įvykdymo būdą ir įtariamojo asmenybę, žinomos tik pasekmės, nukentėjusysis;

2) yra duomenų apie nusikaltimo įvykdymo būdą, bet nėra duomenų apie įtariamojo asmenybę;

3) yra duomenų apie nusikaltimo įvykdymo būdą, įtariamojo asmenybę ir kitas aplinkybes;

4) įtariamasis sulaikytas nusikaltimo vietoje su įkalčiais.

Atsižvelgiant į šių situacijų pobūdį, parenkami ir atliekami atitinkami tyrimo veiksmai: įvykio vietos ir kompiuterinės įrangos apžiūra; dokumentų, kompiuterinės įrangos ar kompiuterinės informacijos laikmenų poėmis arba krata siekiant juos surasti; asmens sulaikymas; įtariamojo apklausa; kompiuterinės ir kitos įrangos ekspertizė bei kiti veiksmai.

Pirmojoje ir antrojoje situacijoje, kai nėra duomenų apie įtariamąjį, paprastai imamasi šių operatyvinės paieškos, organizacinių ir kitų priemonių bei atliekami šie tyrimo veiksmai:

1) nukentėjusiojo apklausa;

2) įvykio vietos apžiūra, dalyvaujant pakviestiems specialistams;

3) operatyvinių paieškos priemonių organizavimas, siekiant nustatyti nusikaltimo įvykdymo priežastis, įtariamuosius, aptikti nusikaltimo pėdsakus, daiktinius įrodymus;

4) kompiuterinės ir kitos įrangos, kompiuterinės informacijos, jos laikmenų, dokumentų apžiūra, pirminis tyrimas ir poėmis, dalyvaujant pakviestiems specialistams;

5) liudytojų apklausa;

6) įtariamų asmenų, vykdančių konkrečias funkcijas, informacijos apdorojimo procesus, susijusius su nusikaltimu, ar atsakingų už informacijos apsaugą, apklausa;

7) įtariamųjų darbo vietos ir gyvenamosios vietos krata;

8) ekspertizių skyrimas (kompiuterinės techninės ir programinės įrangos, kompiuterinės spausdinimo įrangos, radiotechninės, techninės, buhalterinės ir kitų).

Trečiojoje situacijoje, kai yra duomenų apie nusikaltimo įvykdymo ir nuslėpimo būdus, įtariamojo asmenybę ir kitas aplinkybes, tyrėjas, atlikęs pirminę gautos medžiagos analizę,

[34] Burda R. Kompiuterinės įrangos panaudojimas ekonominiams nusikaltimams (kai kurie kriminalistinės charakteristikos ir tyrimo metodikos ypatumai) // Jurisprudencija, 1999. T.12(4). P.71.

(Įvertinant jos išsamumą, baudžiamojo proceso normų vykdymą ir perdavimo ikiteisminio tyrimo Įstaigoms tvarką), imasi šių veiksmų:

1) operatyvinių paieškos priemonių ir Įtariamojo sulaikymo su Įkalčiais organizavimas;

2) sulaikytojo krata;

3) sulaikyto asmens apklausa;

4) sulaikytojo darbo vietos ir gyvenamosios vietos krata;

5) Įvykio vietos apžiūra, dalyvaujant pakviestiems specialistams;

6) liudytojų apklausa, ryšių tarp sulaikytojo ir asmenų, susijusių su Įvykdytu nusikaltimu, nustatymas;

7) nukentėjusiojo apklausa;

8) Įtariamųjų apklausa;

9) kompiuterinės ir kitos Įrangos, kompiuterinės informacijos, jos laikmenų, dokumentų apžiūra, pirminis tyrimas ir poėmis, dalyvaujant pakviestiems specialistams;

10) dokumentų, patvirtinančių Įtariamojo tapatybę ir specialių žinių turėjimą, taip pat dokumentų (visų formų ir laikmenų), charakterizuojančių tas gamybines ar informacijos apdorojimo operacijas, kurių metu buvo Įvykdyti pažeidimai ir nusikalstami veiksmai, poėmis ir apžiūra;

11) asmenų, paminėtų tyrėjams perduotuose dokumentuose kaip padariusių pažeidimus ar atsakingų už konkrečią darbo sritĮ pagal nustatytų pažeidimų faktus, apklausa;

12) asmenų, susijusių su atitinkamomis gamybinėmis ar informacijos apdorojimo operacijomis ar Įtariamų ryšiais su nusikaltėliu, apklausa;

13) ekspertizių skyrimas (kompiuterinės techninės ir programinės Įrangos, kompiuterinės spausdinimo Įrangos, radiotechninės, techninės, buhalterinės ir kitų).

Ketvirtojoje tyrimo situacijoje, kai Įtariamasis sulaikytas nusikaltimo vietoje su Įkalčiais, atliekami šie tyrimo veiksmai:

1) sulaikytojo krata;

2) sulaikyto asmens apklausa;

3) sulaikytojo darbo vietos ir gyvenamosios vietos krata;

4) Įvykio vietos apžiūra, dalyvaujant pakviestiems specialistams;

5) kiti veiksmai, kaip ir trečiojoje situacijoje.

Nurodytų tyrimo, operatyvinių ir organizacinių veiksmų bei priemonių nuoseklumas gali būti keičiamas, atsižvelgiant Į situacijos pasikeitimus. Visose tyrimo situacijose rekomenduojama atlikti žinybinių norminių teisės aktų, informacinių dokumentų, kompiuterinės Įrangos eksploatavimo taisyklių ir darbo su kompiuterine informacija tvarkos analizę, organizuoti konsultacijas su atitinkamų sričių specialistais; išreikalauti dominančio laikotarpio kontrolinių

patikrinimų, inventorizacijų ir revizijų medžiagą (informacijos apdorojimo taisyklių laikymosi, neviešos ar Įslaptintos informacijos apsaugos, elektroninių dokumentų apyvartos, vertybių apskaitos ir kt.) ir atlikti jos analizę; gauti būtiną informaciją iš kontroliuojančių, inspektuojančių ir licencijuojančių Įstaigų (mokesčių inspekcijos ir kt.).

Kompiuterinių nusikaltimų tyrimo užduotis yra surinkti ir užfiksuoti šiuos duomenis:

a) baudžiamojo Įstatymo numatytos veikos požymius;

b) šia veika padarytos žalos pobūdĮ ir dydĮ;

c) priežastinĮ ryšĮ tarp veikos ir jos pasekmių, nustatant kaltininko veiksmų pobūdĮ, nusikaltimo padarymo būdą;

d) kaltininko tyčią.

Apibendrinant tai, kas išdėstyta, galima konstatuoti, kad tipinėse kompiuterinių nusikaltimų tyrimo situacijose pagrindiniai pirminiai tyrimo veiksmai yra šie: Įvykio vietos apžiūra, kompiuterinės Įrangos apžiūra (paties kompiuterio ir kitų Įrenginių), liudytojų apklausa, nukentėjusiojo apklausa, dokumentų poėmis (pirmiausia, elektroninių dokumentų, fiksuojančių svarbius tyrimui duomenis – Įtariamojo prisijungimo prie sistemos laiką ir būdą (tai vadinamieji „log failai“).

Jei Įtariamasis nesulaikytas, greta minėtų pirminių tyrimo veiksmų, būtina organizuoti jo paiešką, taip pat, pasitelkus nukentėjusĮ asmenĮ ir specialistus, nustatyti nusikaltimo padarymo būdo 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. ATSKIRŲ TYRIMO VEIKSMŲ ATLIKIMO YPATUMAI

Įvertinus kompiuterinių nusikaltimų specifines ypatybes (latentiškumą, kėsinimosi objekto nematerialumą, sąlyginį slėpimo paprastumą), reikia pabrėžti apžiūros, kratos ir poėmio svarbą sėkmingam šių nusikaltimų tyrimui.

Kriminalistikos teorijos darbuose apžiūra apibrėžiama kaip procesinis tyrimo veiksmas, kurio metu Įstatymo nustatyta tvarka tyrėjas savo jutiminiais organais ir nesudėtingais instrumentiniais metodais observuoja, analizuoja, fiksuoja ir atlieka kitus veiksmus su objektais, susijusiais su tiriamu Įvykiu[35]. Pagrindinis apžiūros tikslas – rasti, užfiksuoti, surinkti ir paimti informaciją, jos laikmenas ir kaupiklius apie nusikalstamos veikos požymių turintį Įvykį

Krata – tai toks procesinis prievartos tyrimo veiksmas, kurio metu prievarta apieškomos patalpos, vietovės ir kiti objektai, taip pat asmenys, turint tikslą rasti ir paimti nusikalstamos veikos Įrankius, nusikalstamu būdu Įgytus daiktus bei vertybes, nusikalstamos veikos pėdsakus, dokumentus ir kitus daiktus, turinčius reikšmės bylos tyrimui[36].

Vertingi Įrodymai gali būti aptikti krečiant Įtariamųjų darbo, mokslo ir gyvenamąsias vietas, tarnybines patalpas, taip pat pačius Įtariamuosius. Rengiantis atlikti kratą, būtina atidžiai išnagrinėti bylos aplinkybes ir surinkti orientacinę medžiagą apie kratos objektą, jos vykdymo vietą ir krečiamą asmenį. Kompiuterinių nusikaltimų bylose ieškoma ne tik įvairių kompiuterinių priemonių, kaupiklių, laikmenų ir juose esančios kompiuterinės informacijos, bet ir dokumentų, ryšio priemonių, kitų techninių priemonių ir prietaisų (taip pat ir savadarbių), buitinių elektrotechninių įrenginių ir prietaisų, medžiagų ir kt. Ypatingas dėmesys skirtinas daiktams, kuriuose yra kodai, prieigos slaptažodžiai, identifikaciniai numeriai, elektroniniai konkrečių kompiuterinių sistemų ir tinklų vartotojų adresai, Įsijungimo ir darbo sistemose ar tinkluose algoritmai, būtina atkreipti dėmesį į užrašus, telefonų knygutes, žinynus, katalogus (popierinius ir elektroninius, įrašytus į telefonų aparatų ir kitų elektroninių įrenginių atmintį). Paprastai kompiuterinių nusikaltimų bylose svarbu rasti mokslinius bei informacinius leidinius, metodinę medžiagą apie informacines technologijas, kompiuterinės informacijos apdorojimą, apsaugą, perdavimą ir gavimą (tiek teisėtą, tiek neteisėtą), garso ir vaizdo kasetes, spausdintą kompiuterinę informaciją, taip pat ir Įtariamojo išsilavinimą liudijančius dokumentus.

Poėmis – tai toks procesinis prievartos tyrimo veiksmas, kuris atliekamas tuomet, kai reikia paimti daiktus bei dokumentus, turinčius reikšmės bylai, kai žinoma jų buvimo vieta, t.y., kur ir pas ką jie yra[37]. Tiriant kompiuterinių nusikaltimų bylas, poėmio objektai dažniausiai yra šie: asmeniniai kompiuteriai; informacijos kaupikliai ir laikmenos; įvairūs dokumentai (popieriniai ir

[35] Burda R., Krikščiūnas R., Latauskienė E.ir kt. Kriminalistikos taktika ir metodika.- Vilnius, 2004. P.23.
[36] Ten pat. P.55.
[37] Ten pat. P.55.

elektroniniai), aprašantys ar reglamentuojantys įvairias operacijas, technologinius procesus, susijusius su kompiuterinės informacijos apdorojimu, kaupimu, sukūrimu, perdavimu ir apsauga, kompiuterių, jų tinklų ir informacinių sistemų funkcionavimu; specialios techninės priemonės, skirtos slaptam informacijos gavimui, modifikavimui ar sunaikinimui ir kt. Be to, atliekamas parašo pavyzdžių, dokumentų ir blankų fragmentų, informacijos kaupiklių ruošinių, programų išeities kodų, juodraščių ir kitų pavyzdžių poėmis lyginamajam tyrimui atlikti.

Visi kompiuterinių nusikaltimų bylų tyrimo veiksmai turi būti atliekami griežtai laikantis baudžiamojo proceso normų, nes nuo to priklausys gautų duomenų įrodomoji vertė bylos teisminio nagrinėjimo metu, be to, svarbu laikytis šių reikalavimų:

tyrimo veiksmai turi būti iš anksto parengti ir detaliai suplanuoti;

tyrimo veiksmams tinkamai atlikti turi būti iš anksto paruošta reikalinga įranga ir medžiagos;

atliekant tyrimo veiksmus, turi dalyvauti specialistai, tiksliai žinantys savo užduotis, teises ir pareigas; kviestiniai privalo turėti minimalių specialiųjų kompiuterinės informacijos apdorojimo srities žinių (asmeninio kompiuterio vartotojo lygiu), tyrėjas ir specialistai – būtinų žinių apie darbą su kompiuterine technine ir programine įranga (svarbiausia - kompiuterinės informacijos išsaugojimas, jos nepakeičiant).

Atliekant apžiūrą, kratą ar poėmį, svarbu aptikti bei tinkamai surinkti tiek tradicinius, tiek netradicinius pėdsakus, kurie paprastai skirstomi į dvi grupes[38]:

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

2. intelektinius pėdsakus, kuriuos galima suskirstyti į tris grupes:

2.1. kompiuterinių 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, vaizdelių, spausdintuvo ar kitos įrangos tarpusavio suderinamumo pakitimai ir pan.;

2.3. neįprastas kompiuterio darbas: sulėtėjęs operacinės sistemos, pelytės valdymo darbas, netikėtų simbolių atsiradimas, įprastų komandų nestandartinis įvykdymas ir pan.

Konkretaus kompiuterinio nusikaltimo pėdsakai gali būti labai įvairūs, jie priklauso nuo kompiuterinės techninės ir programinės įrangos panaudojimo būdų bei nusikaltimo pobūdžio.

Atsižvelgiant į tai, jog tiriant kompiuterinius nusikaltimus nepakanka profesinių

[38] Burda R. Kompiuterinės įrangos 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 specialistą atliekant bet kurį tyrimo veiksmą.

Vykdant kompiuterinės techninės bei programinės įrangos apžiūrą, kratą ar poėmį, svarbu elgtis ypač atidžiai, atsižvelgti į kompiuterinės informacijos saugojimo, pėdsakų slėpimo priemonių ir būdų ypatybes, numatyti kaltininko priešiškų veiksmų bei kitų faktorių poveikio informacijai galimybes.

Pasiruošiant įvykio vietos apžiūrai ar kratai būtina laikytis šių taisyklių[39]**:**

a) niekam neleisti liesti kompiuterinės įrangos;

b) neišjunginėti patalpose elektros;

c) jei pastate elektra atjungta, būtina ištraukti iš kištukinių lizdų kompiuterinę įrangą, kol ji vėl bus įjungta;

d) tyrėjas neturi liesti kompiuterio klaviatūros, jungiklių, jei nežino šių veiksmų padarinių;

e) jei patalpose kartu su kompiuterine įranga yra lengvai užsidegančių medžiagų, sprogmenų ir pan., iki darbo su kompiuteriais pradžios būtina šias medžiagas izoliuoti;

f) jei pavojingų medžiagų neįmanoma atskirti nuo kompiuterinės įrangos, būtina evakuoti žmones.

Prieš pradedant įvykio vietos apžiūrą ar kratą, būtina imtis visų įmanomų apsaugos priemonių:

a) nustatyti visų patalpoje esančių žmonių asmenybes; tai ypač svarbu siekiant rasti kompiuterinės įrangos specialistus, kuriems tikrinama įmonė (įstaiga) nėra pagrindinė darbovietė;

b) atlikti visų patalpoje esančių žmonių kratą; ieškant darbą su kompiuteriu liečiančių užrašų, neleisti jiems pasinaudoti nuotolinio valdymo įrenginiais, kuriais gali būti paveikti kompiuteriai;

c) neleisti kratomiesiems pažeisti ar sunaikinti kompiuterinės įrangos, kitų įrenginių, diskelių, diskų ir pan.;

d) išsiaiškinti, ar yra kompiuterinės įrangos apsaugos sistema;

e) nustatyti, ar yra informacijos sunaikinimo programa, kuria būtų galima nesankcionuotai pasinaudoti;

f) nustatyti, kokia tyrėjui nežinoma techninė įranga yra patalpoje.

Įvertinus kompiuterinių nusikaltimų būdingus bruožus, būtina pabrėžti, jog atliekant tyrimo veiksmus svarbios šios aplinkybės:

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

[39] Burda R. Kompiuterinės įrangos panaudojimas ekonominiams nusikaltimams (kai kurie kriminalistinės charakteristikos ir tyrimo metodikos ypatumai) / /Jurisprudencija, 1999. T.12(4). P.72.

Įvairūs fiziniai veiksniai – smūgiai, sukrėtimai, aukšta temperatūra, staigūs temperatūros svyravimai, drėgmė ir kt.;

2) jei informacija saugoma magnetiniuose diskuose, stiprus elektromagnetinis laukas gali visiškai suardyti jos loginę struktūrą nuotoliniu būdu, be akivaizdaus, t.y. matomo, fizinio kontakto su ja;

3) bet koks neatsargus elgesys su kompiuterine Įranga gali pažeisti ar sunaikinti informaciją;

4) informacija gali būti užšifruota taikant atitinkamus algoritmus, kuriems vienintelis raktas gali būti ne tik slaptažodis, bet ir tam tikras priėjimo būdas, žinomas tik savininkui;

5) duomenys, svarbūs nusikaltimo atskleidimui ir tyrimui, gali būti saugomi laikmenose, esančiose ne kaltininko, bet kitų vartotojų kompiuterinėje Įrangoje.

Atsižvelgiant Į nurodytas aplinkybes, tyrėjui, atliekančiam konkrečius kompiuterinio nusikaltimo tyrimo veiksmus, būtina:

a) atliekant apžiūrą, kratą ar poėmĮ, turėti ir naudoti elektromagnetinių laukų nustatymo ir matavimo prietaisus;

b) griežtai laikytis saugaus darbo reikalavimų bei būti ypatingai atidžiu fiksuojant, transportuojant ir saugant kompiuterinę techniką bei informacijos laikmenas kaip daiktinius Įrodymus;

c) savarankiškai, be specialisto pagalbos, neatlikti su kompiuterine technika jokių veiksmų, kurių rezultatų negalima iš anksto tiksliai numatyti;

d) neleisti jokiems asmenims, esantiems tyrimo veiksmo vykdymo vietoje, liesti kompiuterinę Įrangą, informacijos laikmenas, Įjungti ir išjungti kompiuterius ar kitus elektroninius Įrenginius;

e) numatyti galimus veiksmus, kurių konkrečioje situacijoje gali imtis Įtariamieji, siekdami sunaikinti informaciją (Įrodymus), ir užkirsti jiems kelią.

Atkreiptinas dėmesys Į tai, jog siekiant išsaugoti kompiuterinius duomenis, reikia atidžiai Įvertinti konkrečias tyrimo aplinkybes ir pasirinkti tinkamus darbo su kompiuterine Įranga metodus. Kartais kriminalistikos rekomendacijose nurodoma, jog būtina nedelsiant išjungti kompiuterĮ iš elektros maitinimo šaltinio, jei yra pagrindo manyti, kad svarbi bylai informacija gali būti pažeista ar sunaikinta, tačiau dažnai būtent toks kompiuterio išjungimas gali lemti informacijos praradimą. Tarkime, jei kaltininkas saugo darbo rezultatus ar priemones šifruotame PGP diske, prie kurio prieiti galima tik ĮvedusslaptažodĮ, staigus ir netikėtas kaltininkui tyrimo veiksmas leistų aptikti Įrodymus, o kompiuterio išjungimas ir keliasdešimt sekundžių, sugaištų diskui uždaryti, padarys informaciją visiškai neprieinama.

Toliau bus detaliau išnagrinėti pagrindiniai kompiuterinių nusikaltimų tyrimo

veiksmai, kuriuos paprastai nurodo dauguma kriminalistikos darbų autorių (pvz., E.Melik, V.B.Vechovas, J.M.Baturinas ir kiti):

1) Įvykio vietos apžiūra;
2) kompiuterinės technikos apžiūra ir poėmis;
3) kompiuterinės informacijos laikmenų apžiūra, nusikalstamo poveikio jai pėdsakų paieška ir poėmis;
4) specialiųjų žinių panaudojimas ir ekspertizės skyrimas.

5.3.1. ĮVYKIO VIETOS APŽIŪRA

Kriminalistikos mokslo darbuose Įvykio vietos apžiūra apibrėžiama kaip neatidėliotinas procesinis tyrimo veiksmas, kurio metu tiesiogiai ištiriama, suvokiama organioleptiniais ir techniniais būdais ir užfiksuojama Įvykio, turinčio nusikalstamos veikos požymių, vieta, jos aplinka, randami, Įtvirtinami, preliminariai ištiriami ir paimami nusikaltimui ištirti reikalingi objektai bei jų lokalinės struktūros[40]. Bendras Įvykio vietos apžiūros uždavinys – susipažinti su Įvykio vietos situacija, aplinka, rasti ir užfiksuoti su tiriamuoju Įvykiu susijusius pėdsakus, o tiriant kompiuterinių nusikaltimų bylas, Įvykio vietos apžiūros pagrindinis tikslas – konkrečios kompiuterinės Įrangos, kuri yra nusikalstamo pasikėsinimo dalykas arba priemonė ir turi nusikalstamos veikos pėdsakų, nustatymas. Kriminalistikos teoriniuose ir praktiniuose darbuose atliekant šĮ tyrimo veiksmą siūloma naudoti ekscentrinĮ taktinĮ būdą („nuo centro – iki periferijos“), kur „centru“ (Įvykio vietos apžiūros išeities tašku) laikoma konkreti kompiuterinė Įranga (arba kompiuterinės informacijos kaupiklis, laikmena). Įvertinus konkrečią tyrimo situaciją, Į operatyvinę tyrimo grupę rekomenduojama Įtraukti šiuos asmenis: tyrėją, kurio specializacija – kompiuteriniai nusikaltimai (grupės vadovas); kriminalistą, išmanantĮ šios kategorijos nusikaltimų tyrimo ypatumus; kompiuterinių technologijų specialistą; telekomunikacinių tinklų technologijų specialistą (nuotolinės prieigos atvejams); operatyvinius darbuotojus; apylinkės ĮgaliotinĮ; apsaugos pareigūną (jei Įvykio vieta ar joje esanti kompiuterinė sistema yra saugomas objektas); kinologą.

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

Vykdant Įvykio vietos apžiūrą, rekomenduojama fotografuoti ir filmuoti, užfiksuojant tyrėjo ir specialistų veiksmų nuoseklumą, taip pat gautus rezultatus. Jei apžiūros metu naudojamos kompiuterinės priemonės ir specialūs techniniai Įrenginiai, tai pažymima protokole, nurodant jų individualius požymius (tipą, pavadinimą, gamyklinĮ numerĮ ir kt.).

Atsižvelgiant Į tai, kad kompiuterinė informacija (nusikaltimo ir nusikaltėlio pėdsakai) gali būti sunaikinta ne tik naudojant valdymo Įrenginius (klaviatūrą, pelę), bet ir vienkartiniu trumpalaikiu kompiuterinės Įrangos Įjungimu ar išjungimu arba ryšio linijos tarp Įrenginių nutraukimu, apžiūros pradžioje būtina nustatyti, kurie kompiuteriniai Įrenginiai ar kiti elektrotechniniai Įrenginiai ar prietaisai yra Įjungti ar išjungti, ir išlaikyti juos tos pačios būsenos iki specialistas baigs jų apžiūrą, tai pat turi būti apsaugoti visi maitinimo Įrangos Įjungimo Įtaisai, esantys Įvykio vietoje.

---

[40] Burda R., Krikščiūnas R., Latauskienė E.ir kt. Kriminalistikos taktika ir metodika.- Vilnius, 2004. P.26.

Įvykio vietos apžiūros protokole turi būti aprašyti šie faktiniai duomenys[41]:

objekto, kuriame įvykdytas nusikaltimas, pavadinimas ir paskirtis;

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

objekto apsaugos sistemos ypatumai, kompiuterinės įrangos ir kompiuterinės informacijos apsaugos būklė, rūšis, išdėstymas, pagrindinės techninės charakteristikos;

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

kompiuterinės įrangos technologinės jungtys su kita įranga, taip pat ir esančia už apžiūros teritorijos ribų (nustatoma tiriant ryšio kabelius ir laidus, vedančius nuo apžiūrimos kompiuterinės įrangos, tokiu būdu apžiūros teritorija gali išsiplėsti);

kompiuterinės įrangos išdėstymas ventiliacinių ir kitų angų statybinėse konstrukcijose, durų ir langų angų, vaizdo stebėjimo techninių priemonių atžvilgiu, darbo vietų atžvilgiu;

kitų techninių elektros, elektroninių įrenginių, prietaisų, priemonių, esančių toje pačioje patalpoje kartu su kompiuterine įranga (telefonų, kitų ryšių priemonių, biuro organizacinės technikos, garso ir vaizdo magnetofonų, autoatsakiklių, elektroninių rašomųjų mašinėlių, 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, sąlygojančios nesankcionuotus vartotojo veiksmus ar turinčios įtakos galutiniams technologinio proceso rezultatams ir jų laikmenos; slapto kompiuterinės informacijos ir magnetinių kaupiklių gavimo, sunaikinimo ar blokavimo techninės priemonės; specifiniai nusikaltėlio ir nusikaltimo pėdsakai. Kriminalistikos darbuose paprastai nurodomi šie tipiniai kompiuterinių nusikaltimų pėdsakai, aptinkami apžiūros metu:

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

įsilaužimo įrankių, apsaugos ar signalinių įrenginių sugadinimo, sunaikinimo ar modifikavimo pėdsakai;

jungiamųjų laidų ir izoliacinių medžiagų likučiai, lydmetalio, kanifolijos ar fliuso lašai, jungiamųjų laidų spaudimo, lydymo, dūrimo, pjovimo ar klijavimo prie jų pašalinių daiktų ar

[41] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно вычислительной техники. Волгоград, 1998. Стр.32.

Įtaisų pėdsakai;

specialios registravimo, stebėjimo, testavimo Įrangos duomenys (darbo su kompiuterine informacija elektroninio registravimo žurnalo duomenys, vaizdo ir garso Įrašymo priemonių duomenys ir pan.).

Apžiūros metu gali būti rasti šie dokumentai, jų laikmenos ir kaupikliai, svarbūs kompiuterinių nusikaltimų tyrimui:

informaciniai, apskaitos dokumentai, susiję su kompiuterinės Įrangos darbu ir kompiuterinės informacijos naudojimu (techninis pasas arba jĮ pakeičiantis dokumentas; operatoriaus žurnalas arba technologinių operacijų, prieigos prie kompiuterinės sistemos ir prie konfidencialios informacijos automatinio fiksavimo protokolas; kompiuterinių kaupiklių, užsakymų (užduočių ar užklausų), programų, Įrašytų kaupikliuose, apskaitos žurnalai; broko sunaikinimo apskaitos žurnalai; konfidencialios informacijos ir kaupiklių su ja trynimo aktai);

dokumentai, susiję su prieigos teisėtumu (elektroniniai prieigos raktai, slaptažodžiai, asmeniniai identifikavimo numeriai (PIN kodai), elektroninis parašas ir kitos sankcionuoto vartotojo identifikavimo ir autentifikavimo priemonės);

registravimo ir buhalteriniai dokumentai (licencijos ir licencinės sutartys; kompiuterinės techninės ir programinės Įrangos, informacijos apsaugos priemonių, informacijos apsikeitimo protokolų ir elektroninių dokumentų formatų atitikimo nustatytiems reikalavimams sertifikatai; sutartys (susitarimai) dėl kompiuterinės Įrangos naudojimo ir prieigos prie kompiuterinės informacijos su atitinkamų dokumentų komplektu; atsiskaitymo ir kiti buhalteriniai dokumentai, atspindintys vartotojo atsiskaitymus už jam suteiktas paslaugas, parduotas prekes ar Įvykdytus kreditinius atsiskaitymus);

kontroliniai apskaitos dokumentai (kompiuterinės techninės ir programinės Įrangos, apsaugos sistemų Įdiegimo, konfigūravimo, derinimo, remonto ir techninio aptarnavimo darbų registravimo žurnalas; gedimų ir sutrikimų registravimo žurnalas; apsaugos signalizacijos darbo trikdžių ir suveikimo atvejų registravimo žurnalas; informacijos saugumo režimo kontrolinių patikrinimų, revizijų, tarnybinių ar kitų patikrinimų aktai; suvestinės ataskaitos ir kontroliniai atskirų darbo sričių, operacijų ar laiko intervalų duomenys);

dokumentai, reglamentuojantys darbuotojų veiksmus (pareigybių aprašymai, pareiginės instrukcijos, darbo su kompiuterinėmis sistemomis, programine Įranga, apsaugos priemonėmis, operatoriaus darbo nestandartinėmis (avarinėmis) situacijomis instrukcijos ir kt.).

Paskesnė minėtų dokumentų apžiūra leidžia nustatyti kompiuterinio nusikaltimo Įvykdymo būdą, nusikaltėlio panaudotas priemones ir medžiagas, disponavimą specialiomis žiniomis ir Įgūdžiais, iškelti versijas dėl priežastinių ryšių.

5.3.2. KOMPIUTERINĖS TECHNIKOS PRIEMONIŲ APŽIŪRA IR POĖMIS

Kompiuterinės technikos priemonių apžiūra – tai neatidėliotinas procesinis tyrimo veiksmas, kurio metu siekiama rasti ir užfiksuoti su tiriamuoju Įvykiu susijusius pėdsakus, leisiančius nustatyti, kas, kokiu tikslu ir kokiomis aplinkybėmis Įvykdė nusikaltimą, išsiaiškinti Įvykio detales ir nusikaltimo Įvykdymo mechanizmą bei nustatyti kompiuterinės Įrangos techninę būklę. Visuose kriminalistikos teoriniuose ir praktiniuose darbuose pabrėžiama, jog vykdyti kompiuterinės technikos priemonių apžiūrą būtina dalyvaujant informacinių technologijų specialistui.

Pradėjus apžiūrą, pirmiausia reikia išsiaiškinti kompiuterinės Įrangos paskirtĮ, nustatyti, Įjungta ji ar ne, patikrinti jos darbingumą ir tai, ar jos atmintinėje yra kompiuterinė informacija, nustatyti, ar Įranga prijungta prie ryšio linijų ar kitų techninių Įrenginių. Po to būtina pradėti materialių pėdsakų ant jos korpuso, atskirų detalių ir laidinių sujungimų, valdymo priemonių (klaviatūros, pelės) paiešką.

Atsižvelgiant Į kompiuterinės informacijos būdingas ypatybes, kriminalistikos rekomendacijose nurodoma, kad vykdant kompiuterinės technikos apžiūrą neleistina naudoti šių priemonių:

1) magnetinių medžiagų ir instrumentų (magnetinių miltelių, šepetėlių ir kt.);

2) techninės Įrangos, sukuriančios elektromagnetinĮ lauką ar trukdžius (elektrostatinių ieškiklių (EPI-2), elektromagneto), metalo ieškiklių, galingų apšvietimo prietaisų, ultravioletinius ir infraraudonuosius spindulius skleidžiančių prietaisų ir kt.;

3) rūgštinių ar šarminių medžiagų ir šildymo prietaisų, kad išvengti kompiuterinės technikos ir informacijos, nusikaltėlio ir nusikaltimo pėdsakų sunaikinimo ar pažeidimo.

Minėtas medžiagas ir prietaisus galima naudoti tik laikantis ypatingų atsargumo priemonių, ne mažiau kaip 1 metro atstumu nuo kompiuterinės Įrangos ir jos jungiamųjų laidų.

Po kompiuterinės technikos apžiūros dažniausiai atliekamas jos poėmis ir tolesnis ekspertinis tyrimas. Kadangi kompiuterinės technikos poėmis vykdomas siekiant, kad vėliau ją ištirtų informacinių technologijų specialistas ar ekspertas, labai svarbu tinkamai atlikti poėmio veiksmus – nustatyta tvarka demontuoti kompiuterĮ ir kitus Įrenginius jų aptikimo vietoje bei supakuoti juos taip, kad laboratorijoje ar kitoje specialioje tyrimo vietoje būtų galima sėkmingai sujungti tiksliai atkuriant pirminĮ modelĮ.

Atkreiptinas dėmesys Į tai, kad kompiuterinės technikos apžiūros bei poėmio veiksmų metodika gali būti dvejopa ir priklauso nuo kompiuterio būsenos tyrimo veiksmo atlikimo momentu, t.y. svarbiausia, ar kompiuteris aptinkamas neveikiantis (išjungtas) ar veikiantis (Įjungtas).

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

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

1) tiksliai nurodyti kompiuterio ir kitų išorinių įrenginių radimo vietą protokole bei pridedamoje schemoje;

2) tiksliai ir detaliai aprašyti kompiuterio ir kitų išorinių įrenginių sujungimo tvarką, akcentuojant konkrečias jungiamųjų laidų ir kabelių ypatybes (specifikacijas, sujungimo grandžių kiekį, spalvą ir kt.);

3) nufotografuoti arba padaryti vaizdo įrašą visų įrenginių sujungimo vietų prieš juos atjungiant;

4) išjungti kompiuterį iš elektros maitinimo šaltinio ir laikantis darbų saugos reikalavimų atjungti išorinius įrenginius;

5) atskirai supakuoti laikmenas (disketes, magnetines juostas) į pakuotes, nekaupiančias statinio elektros krūvio;

6) atskirai supakuoti kiekvieną įrenginį, jungiamuosius laidus ir kabelius;

7) ypatingai atidžiai ir atsargiai supakuoti bei gabenti pagrindinį informacijos kaupiklį – kietąjį diską (vinčesterį).

Antruoju atveju, kai kompiuteris veikia, tyrimo veiksmų eiga informacijos išsaugojimo požiūriu žymiai sudėtingesnė. Šiuo atveju tyrėjas, neturėdamas pakankamų informacinių technologijų srities specialiųjų žinių, negali operatyviai užfiksuoti įkalčių. Tokiomis aplinkybėmis pagrindinė tyrėjo užduotis – išsaugoti ir perduoti specialistui ar ekspertui kompiuterinę techniką ir joje esančią informaciją nepakitusią, taigi tyrėjas privalo paisyti anksčiau išvardintų bendro pobūdžio rekomendacijų ir papildomai atlikti šiuos veiksmus:

1) nustatyti, kokia programa ar programos tyrimo veiksmo atlikimo momentu vykdomos veikiančiame kompiuteryje;

2) detaliai aprašyti vaizdą displėjaus ekrane, jei būtina padaryti jo nuotraukas ar vaizdo įrašą;

3) išsaugoti operatyvinėje atmintyje esančią informaciją atskiroje laikmenoje;

4) tinkamai sustabdyti programų vykdymą;

5) nustatyti, ar kompiuteris turi išorinių įrenginių, skirtų nuotolinei prieigai prie sistemos, pvz., modemą, ir užfiksuoti protokole jų būklę, po to nutraukti prieigos per šiuos įrenginius galimybę;

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, konfigūracija, spalva ir gamyklinis numeris (serijinis, inventorinis arba gaminio apskaitos numeris);

– jungiamųjų ir maitinimo laidų tipas (paskirtis), spalva ir kiti individualūs požymiai;

– būsena apžiūros metu (Įjungta ar išjungta);

– techninė būklė – išorinis vaizdas, korpuso būklė, komplektacija (blokai, mazgai, detalės, sujungimai tarp jų, darbingumas), naudojamo informacijos kaupiklio tipas;

– maitinimo šaltinio tipas, jo techninės charakteristikos ir būklė (darbinė Įtampa, srovės dažnis, darbinė apkrova, ar yra saugiklis, stabilizatorius, tinklo filtras, prijungtos prie jo Įrangos kiekis, kištukinių lizdų skaičius ir kt.);

– ar yra kompiuterinės Įrangos Įžeminimas, jo techninė būklė;

– techninės galimybės prie kompiuterinės Įrangos prijungti išorinius Įrenginius, kompiuterinės Įrangos prijungimo prie išorinių Įrenginių ar prie ryšio linijų charakteristika;

– kompiuterinės Įrangos pažeidimai, standarte nenumatyti konstrukciniai pakeitimai kompiuterinės Įrangos architektūroje, jos atskirose detalėse (dalyse, blokuose), ypač tie, kurie galėjo atsirasti dėl nusikalstamos veikos; nusikalstamos veikos pėdsakai (kompiuterinės Įrangos korpuso pažeidimo, patekimo Į korpuso vidų, nesankcionuoto techninės Įrangos prijungimo prie kompiuterinės sistemos, pirštų ir kt. pėdsakai);

– kompiuterinės Įrangos išdėstymas erdvėje išorinių Į r enginių ir kitos elektrotechninės Įrangos atžvilgiu; tiksli kompiuterinės Įrangos sujungimų su kita technine Įranga tvarka;

– apdorojamos informacijos kategorija (vieša, bendro naudojimo ar nevieša, Įslaptinta);

– aptiktų informacijos laikmenų (diskelių, kompaktinių diskų (CD, DVD), USB raktų) duomenys (tipas, markė, užrašai ant lipduko ir pan.);

– kompiuterinės Įrangos ir joje apdorojamos informacijos apsaugos sistemos priemonių ypatybės (jei yra apsaugos sistema, nurodyti slaptažodžius, kitus algoritmus, Įėjimo ir išėjimo Į kompiuterio programas būdus) ir kt.

Siekiant užtikrinti kompiuterinės Įrangos ir joje esančios informacijos saugumą, būtina apžiūrėti ir, jei Įmanoma, paimti visą kratomojoje Įmonėje ar Įstaigoje esančią kompiuterinę Įrangą. Ant paimamų kompiuterių maitinimo lizdų, jungiklių reikia užklijuoti tyrėjo užpildytus i r pasirašytus lapelius, informacijos laikmenas (diskelius ir kompaktinius diskus) būtina paimti kartu su pakuote arba dėžute, kurioje saugomos, atskiri diskeliai Įpakuojami Į aliuminio foliją ir užantspauduojami pagal bendrąsias taisykles. Jei kompiuterinės Įrangos paimti neĮmanoma, atlikus apžiūrą, būtina kompiuterinę Įrangą išjungti ir užantspauduoti, patalpoje atjungti elektrą, užantspauduoti elektros skydelĮ ir užtikrinti jos fizinę apsaugą.

5.3.3. KOMPIUTERINĖS INFORMACIJOS LAIKMENŲ APŽIŪRA, NUSIKALSTAMO POVEIKIO JAI PĖDSAKŲ PAIEŠKA IR POĖMIS

Kriminalistikos metodikos darbuose skiriami du kompiuterinės informacijos bei nusikalstamo poveikio jai pėdsakų paieškos atvejai:

1) informacijos bei nusikalstamo poveikio jai pėdsakų paieška kompiuterinėse laikmenose ir kitoje kompiuterinėje Įrangoje (kitaip tariant, skaitmeninės formos);

2) informacijos bei nusikalstamo poveikio jai pėdsakų paieška ne kompiuterinėje Įrangoje (neskaitmeninės formos).

Kompiuterinė informacija gali būti kaupiama Įvairiose laikmenose – magnetinėse, optinėse, magnetooptinėse ir kitokiose atmintinėse – kietajame diske, lanksčiuose diskuose, kompaktiniuose diskuose, rezervinių kopijų Įrenginių laikmenose, taip pat operatyvinėje atmintinėje, jei vykdomos programos (tačiau šią informaciją ypač 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 Įvairaus pobūdžio duomenys, paprastai skiriamos šios duomenų grupės:

- vartotojų identifikaciniai duomenys, slaptažodžiai, kodai, prisijungimo vardai;
- techniniai duomenys;
- Įrenginių schemos ir grafiniai vaizdai;
- dokumentų tyrinys;
- kenkėjiškos programos, virusai, jų kodai bei kūrimo priemonės ir kt.

Pabrėžtina tai, jog informacijos paiešką būtina atlikti visoje failų sistemoje, nepaisant vardų bei prievardžių (plėtinių), Įskaitant paslėptuosius failus ir jų struktūras. Ypač atidžiai reikia ištirti vadinamuosius „log failus“ (programų veiklos registrus, kuriuose gali būti užfiksuota svarbi Įvairių veiksmų atlikimo informacija, laikas ir data).

Siekiant užfiksuoti nusikaltėlio bendravimo su kitais asmenimis duomenis, būtina ištirti elektroninio pašto programų bazes, „online“ bendravimo programų pranešimų bazes (ICQ, Odigo ir kt.), laikinąją programos naršyklės atmintinę (spartinančiąją atmintinę – „kešą“).

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 kompiuterinės informacijos paiešką, galima aptikti ir šias rūšis svarbių dokumentų ne kompiuterinėje Įrangoje:

- popierinius dokumentus, su Įvykdyto nusikaltimo pėdsakais, pvz., prieigos

slaptažodžius ir kodus, telefoninių pokalbių išklotines, sąskaitas, užrašus ir kt.;

– popierinius dokumentus, likusius išoriniuose Įrenginiuose, pvz, spausdintuvuose ar kopijuokliuose, dėl nusikaltėlio neapdairumo;

– techninės ir programinės Įrangos dokumentus;

– darbo su kompiuteriu dokumentus ar norminius teisės aktus, reglamentuojančius darbo su konkrečia kompiuterine Įranga, informacine sistema ar tinklu, tvarką, Įrodančius, kad Įtariamasis ją žinojo ir sąmoningai pažeidė;

– Įtariamojo ar kaltinamojo asmeninius dokumentus.

Kriminalistikos metodikos darbuose rekomenduojama kompiuterinės informacijos laikmenų (dažniausiai lanksčiųjų diskų, kompaktinių diskų, kietojo disko ir kt.) apžiūrą atlikti naudojant taktinĮ būdą „nuo bendro prie atskiro“, dalyvaujant informacinių technologijų specialistui. Pradėjus apžiūrą, pirmiausia reikia aprašyti individualius laikmenos požymius (nurodoma tipas, rūšis, paskirtis, spalva, dydis, išvaizda, pavadinimas, gamyklinis ir individualus numeris, ar yra lipdukas ir užrašai ant jo, ar yra fizinių korpuso pažeidimo žymių ir pėdsakų ant jo, apsaugos nuo kompiuterinės informacijos trynimo ir Įrašymo elemento būsena), po to yra atliekama laikmenoje esančios kompiuterinės informacijos apžiūra.

Prieš pradedant apžiūrą, tyrimo veiksmo protokole reikia nurodyti:

1) apžiūrai naudojamos kompiuterinės technikos duomenis ir pagrindinius jos programinės Įrangos rekvizitus (tipas, rūšis, pavadinimas, gamyklinis arba registracijos numeris, versijos numeris, juridinis adresas ir (arba) programinio produkto autorius);

2) programos, kurios pagalba buvo testuojama kompiuterinė sistema ir jos programinė Įranga, siekiant nustatyti ar joje nėra kenkėjiškos programinės ar techninės Įrangos, rekvizitus.

Analizuojant laikmenoje esančią kompiuterinę informaciją, būtina nustatyti duomenis, turinčius ryšĮ su tiriamu Įvykiu. Didelės apimties informacijos apžiūros procesui spartinti galima naudoti automatizuotos paieškos pagal reikšminĮ žodĮ funkciją, kuri yra standartiniame kompiuterių programinės Įrangos pakete. Apžiūros procesas papildomai turi būti fiksuojamas fotografuojant ar filmuojant. Aptikus nusikaltimo pėdsakus, būtina išspausdinti visą arba dalĮ kompiuterinės informacijos ir pridėti ją prie tyrimo veiksmų protokolo, nurodant naudoto spausdinimo Įrenginio individualius požymius (tipą, rūšĮ, pavadinimą, numerĮ).

Apžiūros protokole taip pat nurodomi šie duomenys:

– laikmenos apsaugos nuo nesankcionuoto panaudojimo individualūs požymiai (holograma, brūkšninis kodas, šrifto iškilumas, perforacija, fluorescavimas, asmeninio parašo ar savininko nuotraukos laminavimas, jų dydis, spalva, išvaizda ir kt.);

– laikmenos ir jos apsaugos klastojimo ar kitokio neteisėto poveikio požymiai;

– vidinė laikmenos specifikacija (serijinis numeris, kodas, talpa);

– laikmenos talpos užimtos ir laisvos dalies dydis;

– sugadintų zonų, sektorių, klasterių, cilindrų kiekis ir numeriai;

– Įrašytų programų, failų, katalogų skaičius (jų išdėstymo laikmenoje struktūra, pavadinimai, vardai ir(arba) prievardžiai (plėtiniai), dydis (apimtis), taip pat ir tas, kurĮ užima jų pavadinimai, sukūrimo (arba paskutinio pakeitimo) data ir laikas, specialios žymės (pvz., sisteminis, archyvinis, paslėptas, tik skaitymui arba rašymui ir kt.);

– paslėptų arba ištrintų failų (programų), jei tokių buvo, rekvizitai (pavadinimas, dydis, sukūrimo ar sunaikinimo data ir laikas).

5.3.4. SPECIALIŲJŲ ŽINIŲ PANAUDOJIMAS IR EKSPERTIZĖS SKYRIMAS

Lietuvoje informacinių technologijų ekspertizės, tyrimus atlieka ir specialistų išvadas teikia Lietuvos teismo ekspertizės centro Kompiuterinių tyrimų skyrius, Lietuvos policijos Kriminalistinių tyrimų centro Kriminalistinių tyrimų valdybos Informacinių technologijų tyrimo skyrius, Valstybės saugumo departamento specializuotas padalinys. Lietuvos teismo ekspertizės centro, kuriame informacinių technologijų ekspertizės (tyrimai) atliekamos nuo 1995 m., duomenimis[42], būtent šios ekspertizės tampa vienos iš paklausiausių, pastaraisiais metais ženkliai išaugo metinis skiriamų tyrimų skaičius (plg., 2002 m. – 57 tyrimai, 2005 m. – 120 tyrimų).

Specialiųjų žinių panaudojimo ir ekspertinių tyrimų klausimai bei problemos buvo nagrinėjami Baltijos valstybių teisėsaugos pareigūnams skirtame tarptautiniame Baltijos regiono seminare „Kompiuterinių nusikaltimų ikiteisminis tyrimas ir teisminis nagrinėjimas“, 2003 m. vykusiame Tartu (Estijoje). Šiame seminare buvo aptarti tiek bendrieji teoriniai, tiek specialieji technologiniai klausimai, pvz., specialių programų, skirtų kompiuterinių sistemų ekspertizei (ESCAP, CART), darbo aspektai.

Atsižvelgiant Į kompiuterinių nusikaltimų ypatybes bei Įvertinus kompiuterinės programinės ir techninės Įrangos kaip kriminalistinio objekto sudėtingumą, būtina pastebėti, jog šios rūšies nusikaltimų bylų sėkmingam tyrimui ypač didelę reikšmę turi tinkamas specialiųjų žinių panaudojimas. Atkreiptinas dėmesys Į tai, kad paprastai tyrėjas neturi pakankamų specialiųjų informatikos srities žinių ir techninių Įgūdžių, būtinų saugiam informacijos poėmiui, be to, tyrėjo prielaidos apie tai, kad viename ar kitame kompiuteryje arba kompiuterinėje laikmenoje gali būti saugoma svarbi tiriamai bylai informacija, dažniausiai yra paremtos tikimybe, tyrėjas neturi Įrodančių duomenų, geriausiu atveju disponuoja tik operatyvine informacija. Kriminalistikos mokslo darbuose daroma išvada, kad kompiuterinė Įranga yra gana sudėtingas kriminalistinis objektas, kurĮ tiriant būtina panaudoti specialias žinias“[43]. Galima konstatuoti, jog specialistų dalyvavimas vykdant kompiuterinių nusikaltimų bylų ikiteisminĮ tyrimą būtinas, nes specialiųjų žinių panaudojimas labai svarbus vykdant kratas, apžiūras, poėmius ir kitus tyrimo veiksmus. A.N.Jakovlevo[44] ir kitų mokslininkų teigimu, specialiosios žinios turėtų būti panaudojamos rengiantis atlikti tyrimo veiksmus, vykdant nusikaltimo vietos ir kompiuterinės technikos apžiūrą, kratą ar poėmĮ, tardymo metu, akistatos metu, tiriamojo eksperimento metu.

V.B.Vechovo darbuose pabrėžiama, kad specialistų dalyvavimas turi būti privalomas

---

[42] Informacinių technologijų tyrimų galimybės // http://www.ltec.lt/naujienos.php?item=56; prisijungimo laikas 2006-10-01.

[43] Burda R.. Kompiuterinės Įrangos panaudojimas ekonominiams nusikaltimams (kai kurie kriminalistinės charakteristikos ir tyrimo metodikos ypatumai) //Jurisprudencija, 1999. T.12(4). P.73.

[44] Яковлев А. Н. Использование специальных познаний при расследовании компьютерных» преступлений // Конфидент.- С.Петербург, 2000. №.

tiriant kompiuterinius nusikaltimus ir rekomenduojama, atsižvelgiant Į bylos ypatybes, kaip nešališkus ekspertus pasitelkti programuotojus, informacinių ir telekomunikacinių sistemų analitikus, kompiuterinių tinklų operatorius, ryšių priemonių ir telekomunikacinės Įrangos inžinierius, informacinių sistemų saugos specialistus, kompiuterinės technikos aptarnavimo specialistus, kompiuterizuotos finansinės apskaitos ir bankų operacijų specialistus[45]. Tokie specialistai turėtų būti kviečiami iš mokslo, švietimo ir kitų Įstaigų ar Įmonių, kurios užsiima informacinių ir telekomunikacinių technologijų tyrimu, saugos užtikrinimu, kompiuterinės Įrangos eksploatacija bei priežiūra. Patariama nesinaudoti nukentėjusio juridinio asmens specialistų paslaugomis, nes šie asmenys gali būti suinteresuoti nuslėpti Įstaigos informacinės sistemos eksploatavimo ir saugumo spragas, be to, yra didelė tikimybė, kad nusikaltimas galėjo būti Įvykdytas vieno iš jų.

Apibendrinant kompiuterinių nusikaltimų tyrimo praktiką, pastebėtina, kad specialiųjų žinių panaudojimas ir ekspertizės atlikimas gali lemti nusikalstamos veikos kvalifikavimą ir būti svarbiu, o kai kuriais atvejais vieninteliu duomenų, rodančių nusikaltimo požymius, gavimo būdu, todėl atliekant šios rūšies nusikaltimų ikiteisminį tyrimą rekomenduojama specialistus Įtraukti kuo anksčiau. Specialistai ir ekspertai gali padėti tyrėjui išspręsti šiuos klausimus: kokia yra tiriamos kompiuterinės Įrangos sudėtis ir sąranka (konfigūracija), ar galima šios Įrangos pagalba atlikti veiksmus, inkriminuojamus Įtariamajam (kaltinamajam); kokie informaciniai resursai yra šioje Įrangoje; kokiu būdu gali būti Įvykdyta nesankcionuota prieiga prie tiriamos Įrangos ar kompiuterinės sistemos; ar kompiuterinę informaciją buvo bandoma sunaikinti, pakeisti, kopijuoti; ar rastos laikmenos (failai, bylos) yra informacijos, esančios konkrečioje kompiuterinėje Įrangoje, kopijos; ar išspausdinti popieriuje tekstai yra programos ar atliktų programos pakeitimų išeities kodai ir kokia yra šios programos paskirtis arba koks yra atliktų pakeitimų rezultatas; ar laikmenos, programos yra užkrėstos virusais ir jeigu taip, tai kokiais būtent; ar pateiktas kodas nėra virusinis; ar Įtariamojo (kaltinamojo) veiksmais buvo pažeistos nustatytos darbo su informacine sistema, kompiuteriu taisyklės, informacinių resursų naudojimo tvarka; ar darbo taisyklių pažeidimas turėjo priežastinį ryšį su informacijos sunaikinimu, pakeitimu, kopijavimu ir kt.

Daugelyje kriminalistikos mokslo darbų pabrėžiama ekspertizių svarba kompiuterinių nusikaltimų tyrimui ir nurodoma, kad tiriant tokius nusikaltimus paprastai skiriamos šios ekspertizės: kompiuterinės Įrangos; programinės Įrangos; kompiuterinės spausdinimo Įrangos; kompiuterinių laikmenų.

Lietuvos teismo ekspertizės centro duomenimis ekspertams dažniausiai pateikiami informacinių technologijų tyrimo objektai yra šie: nešiojamieji asmeniniai kompiuteriai,

[45] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно вычислительной техники.- Волгоград, 1998; Компьютерные преступления. Способы совершения, методики расследования.- Москва, 1996.

kompiuterių sisteminiai blokai, delninukai, spausdintuvai, skeneriai, mobiliojo ryšio telefono aparatai, mokėjimo kortelės, Įvairios informacijos laikmenos, lyginamieji (dokumentų, banknotų ar kiti) pavyzdžiai[46].

Kompiuterinės Įrangos ekspertizės skyrimo problemos aptartos V.Kligio ir V.Jankausko straipsnyje „Informacinių technologijų ekspertizė LTEC: dabartis ir perspektyva“[47], leidinyje „Teismo ekspertizių skyrimo klausimai“[48], kompiuterinės spausdinimo Įrangos ekspertizės ypatybes nagrinėjo A.Deringas, Z.Rinkevičienė ir L.Sakalauskas straipsnyje „Kompiuteriniais spausdintuvais išspausdintų dokumentų kriminalistinis tyrimas“[49].

Iki nutarimo dėl ekspertizės skyrimo priėmimo rekomenduotina pasikonsultuoti su specialistu dėl jos tikslų, klausimų formulavimo, pateikiamos medžiagos pobūdžio. Kompiuterinių 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 (sudėtingų formatų – programavimo kalbų forma, elektroninių lentelių, duomenų bazių 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 (dokumentų, failų, programų) sukūrimo, pakeitimo, sunaikinimo, kopijavimo datos ir laiko nustatymas;

4. kompiuterinės informacijos (dokumentų, failų, programų), esančių laikmenoje, parengimo vietos ir būdo, autorystės nustatymas;

5. užkoduotos kompiuterinės informacijos iššifravimas, slaptažodžių parinkimas ir apsaugos sistemos Įveikimas;

6. kompiuterinės sistemos ir informacijos tyrimas, siekiant nustatyti, ar yra programinių ar techninių modulių ir modifikacijų, sąlygojančių nesankcionuotą informacijos sunaikinimą, blokavimą, pakeitimą arba kopijavimą, kompiuterių, jų sistemos ar tinklo darbo sutrikdymą;

7. galimų informacijos nutekėjimo kanalų iš kompiuterių, jų sistemos ar tinklo, taip pat patalpų nustatymas;

8. galimų nesankcionuotos prieigos prie Įstatymų saugomos kompiuterinės

[46] Informacinių technologijų tyrimų galimybės // http://www.ltec.lt/naujienos.php?item=56; prisijungimo laikas 2006-10-01.
[47] Kligys V., Jankauskas V. Informacinių technologijų ekspertizė LTEC: dabartis ir perspektyva // Vilnius: M. Romerio universitetas, 2005;
[48] Teismo ekspertizių skyrimo klausimai. Informacinis laiškas.- Vilnius, 1996. P.4.
[49] Deringas A., Rinkevičienė Z., Sakalauskas L. Kompiuteriniais spausdintuvais išspausdintų dokumentų kriminalistinis tyrimas // Kriminalinė justicija: Lietuvos teisės akademijos mokslo darbai.- Vilnius, 1997. T.7-8.

informacijos ir jos laikmenų būdų nustatymas;

9. kompiuterių, jų sistemos ar tinklo techninės būklės, nusidėvėjimo, taip pat individualių kompiuterinės sistemos pritaikymo konkrečiam vartotojui požymių nustatymas;

10. atskirų asmenų, minimų byloje, profesinės kvalifikacijos informatikos ar programavimo srityje nustatymas, konkrečios kompiuterinės sistemos vartotojo žinių ir įgūdžių lygmens nustatymas;

11. konkrečių asmenų, pažeidusių kompiuterių, jų sistemos ar tinklo eksploatavimo taisykles, nustatymas;

12. priežasčių ir aplinkybių, paskatinusių įvykdyti kompiuterinį nusikaltimą, nustatymas;

13. kompiuterinės įrangos, išorinių įrenginių, magnetinių laikmenų, programinių produktų vertės nustatymas;

14. techninio pobūdžio dokumentų vertimas ir kt.

Kompiuterinės techninės ir programinės ekspertizės gali būti identifikacinės arba neidentifikacinės, be to, tiriant kompiuterinių nusikaltimų bylas, dažnai skiriamos šios kriminalistinės ekspertizės: daktiloskopinės, odorologinės, trasologinės, grafologinės, fonoskopinės, autorystės nustatymo, radiotechninės, dokumentų ekspertizės, polimerinių medžiagų ir gaminių iš jų ekspertizės.

Apibendrinant galima konstatuoti, kad specialiųjų žinių panaudojimas ir ekspertizės turi ypač didelę reikšmę kompiuterinių nusikaltimų sėkmingam tyrimui, tačiau pastebėtina ir tai, jog plintant nusikaltimams elektroninėje erdvėje, teisėsaugos institucijoms būtina kaupti žinias apie informacinių sistemų veikimo bei saugumo užtikrinimo principus, procedūras, darbo su kompiuterine informacija metodus bei kelti pačių teisėsaugos pareigūnų specialiąją kvalifikaciją ir kurti specialius padalinius kovai su kompiuteriniu nusikalstamumu, nes vienkartinis informatikos specialistų ar ekspertų įtraukimas tiriant bylas nėra pakankamai efektyvus ir negali užtikrinti moksliškai pagrįstos šios rūšies nusikaltimų tyrimo metodikos suformavimo. Atsižvelgiant į vyraujančias nusikalstamumo tendencijas bei pasaulinę praktiką, 2001 m. Lietuvos kriminalinės policijos biuro Nusikaltimų tyrimo vyriausiojoje valdyboje buvo įsteigtas specializuotas Nusikaltimų elektroninėje erdvėje tyrimo skyrius, kurio misija[50] – užtikrinti Konvencijos dėl elektroninių nusikaltimų reikalavimų įgyvendinimą, užkardyti, tirti ir atskleisti rengiamus, daromus ar padarytus nusikaltimus elektroninėje erdvėje – pasauliniame interneto tinkle bei korporatyvinėse informacinėse sistemose – intranete, taip siekiant užtikrinti Lietuvos visuomenės ir informacinių technologijų saugumą šioje sferoje.

[50] Aplinkybės, dėl kurių buvo įkurtas Nusikaltimų elektroninėje erdvėje tyrimo skyrius – NEETS (angl. CYBERPOLICE) // http://www.cyberpolice.lt/index_.asp?DL=L&TopicID=2; prisijungimo laikas 2006-10-14.

6. PAGRINDINĖS KOMPIUTERINIŲ NUSIKALTIMŲ TYRIMO KLAIDOS

Šiuo metu Lietuvoje dar nėra parengtos kompiuterinių nusikaltimų tyrimo metodikos, pagrĮstos susistemintomis teorinėmis žiniomis ir patikrintos praktikoje. Tikėtina, jog tai sąlygoja teisės teoretikų ir praktikų nuomonių dėl kompiuterinių nusikaltimų ir jų tyrimo metodų, kurie gana stipriai skiriasi nuo tradicinių nusikaltimų, Įvairovė bei vieningos pozicijos stygius. Galima pagrĮstai teigti, kad šios kategorijos baudžiamųjų bylų tyrimo klaidas dažniausiai lemia nepakankamas ikiteisminio tyrimo tyrėjų pasiruošimas tiek teoriniu, tiek praktiniu požiūriu bei Įkalčių, susijusių su kompiuteriniais nusikaltimais, specifika, nes šie Įkalčiai gali būti lengvai pakeisti ir prarasti Įrodomąją galią kompiuterinės technikos poėmio metu bei atliekant tolesnĮ tyrimą.

Siekiant išvengti esminių kompiuterinių nusikaltimų tyrimo klaidų, pirmiausia, kaip jau buvo minėta, rekomenduojam visus tyrimo veiksmus vykdyti dalyvaujant informacinių technologijų specialistui, o kompiuterinės technikos tyrimą atlikti kriminalistinės laboratorijos sąlygomis, 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 kompiuterinių nusikaltimų tyrimo veiksmus, pvz., kompiuterinės technikos poėmĮ, dažnai labai svarbus netikėtumo efektas ir operatyvumas, leidžiantys aptikti Įkalčius ir išsaugoti būtiną Įrodomąją informaciją. Atsižvelgiant Į šias aplinkybes, būtent ikiteisminio tyrimo tyrėjo kompetentingumas, teorinės žinios ir praktiniai Įgūdžiai lemia kompiuterinio nusikaltimo tyrimo sėkmę, o jo klaidomis gali pasinaudoti kaltinamojo gynėjas bylos teisminio nagrinėjimo metu.

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

1) bendrosios klaidos, kurios yra padaromos teisėsaugos institucijų pareigūnų, atliekančių kompiuterinių nusikaltimų tyrimo veiksmus, ir

2) techninės klaidos, susijusios su informacijos apsaugos priemonėmis, Įdiegtomis kompiuteriuose jų tiesioginių vartotojų.

V.A.Golubevas ir kiti kriminalistikos bei informacinių technologijų saugos specialistai, apibendrindami praktinės teisėsaugos institucijų veiklos rezultatus, pabrėžia, jog dažniausiai pasitaiko šios pagrindines kompiuterinių nusikaltimų tyrimo klaidos[51]:

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

[51] Голубев В.А. Некоторые вопросы расследования компьютерных преступлений // Сборник научных трудов международной конференции „Информационные технологии и безопасность“.– Киев, 2003. Выпуск 3. Стр.28 – 36.

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 tyrėjų klaidų yra leidimas dirbti su tiriamuoju (apžiūrimu, konfiskuotu) kompiuteriu jo savininkui arba vartotojui, prašant jų Įjungti ar išjungti kompiuterĮ, parodyti kompiuteryje saugomą informaciją ar kitokios pagalbos. Suinteresuotas asmuo, juo labiau išmanantis informacinių technologijų veiklos principus geriau nei tyrėjas, gali nepastebimai ištrinti, pakeisti ar užšifruoti informaciją ir sunaikinti Įkalčius, pasinaudodamas menkiausia galimybe dirbti kompiuteriu tiesiog tyrimo veiksmo metu. Įvertinus šią grėsmę, tyrėjui 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 kompiuterinių nusikaltimų tyrimo klaida – netinkamai atliekami veiksmai su tiriamuoju kompiuteriu ar informacijos laikmenomis – gali sudaryti galimybę kaltinamojo gynėjui teisminio bylos nagrinėjimo metu paneigti teismui pateiktos programinės Įrangos autentiškumą, t.y. jos atitikimą tai Įrangai (jos būsenai), kuri buvo kompiuteryje poėmio metu. Siekiant išvengti šios problemos, būtina vykdant bet kokią operaciją su kompiuteriu, užfiksuoti jo būseną tyrimo veiksmo vykdymo metu, kitaip tariant, teisėsaugos pareigūnui rekomenduojama užantspauduoti kompiuterĮ tokios būsenos, kokios jis rastas, neišjungiant jo ar neĮjungiant, Įmonės, Įstaigos ar organizacijos atstovo, savininko ar kviestinių akivaizdoje, arba, jei priimamas sprendimas apžiūrėti kompiuterĮ vietoje, būtina padaryti kopiją visų kietųjų ar lanksčiųjų diskų, kurie bus paimami kaip Įkalčiai.

Kriminalistikos metodikos darbuose pabrėžiama, kad kompiuteris pirmiausia yra specialisto tyrimo objektas, todėl iki jis bus perduotas specialistui ar ekspertui, tyrėjams rekomenduojama susilaikyti nuo bet kokių veiksmų su kompiuteriu arba griežtai laikytis būtinų saugos priemonių (sukurti rezervinę kopiją, naudoti apsaugą nuo pakeitimų). Jeigu tiriamajame kompiuteryje yra Įdiegta apsaugos sistema (prieigos kodas, slaptažodis ar kt.), tai netinkamas jo Įjungimas gali sąlygoti informacijos, esančios kietajame diske, sunaikinimą, todėl neleidžiama aktyvuoti tokio kompiuterio naudojant jo paties operacinę sistemą. Nusikaltėliai dažnai modifikuoja operacinę sistemą, Įdiegdami programas, skirtas kietajame ar kituose diskuose saugomai informacijai sunaikinti (pavyzdžiui, komanda DIR, naudojama disko katalogo parodymui, gali būti pakeista taip, kad ją Įvykdžius bus suformatuotas kietasis diskas), be to, tokios kenkėjiškos programos gali sunaikinti tiek duomenis, tiek pačios save, todėl vėliau, bylos teisminio nagrinėjimo metu, sunku Įrodyti, ar tiriamajame kompiuteryje tokio pobūdžio programos buvo Įdiegtos tyčia, ar tai neatsargaus kompiuterinių Įkalčių tyrimo, nekompetentingo tyrėjų elgesio pasekmės.

Dažnai, kai tiriamasis kompiuteris yra apkrėstas virusais, teisminio bylos nagrinėjimo metu kaltinamojo gynėjui sudaroma galimybė atmesti įkalčius, apkaltinus tyrėjus nekompetentingumu, dėl neatsargumo ar tyčia užkrėtus kompiuterį virusais, nes įrodyti, kad virusas buvo kompiuteryje iki apžiūros momento neįmanoma, jei tyrėjai kompiuterio tinkamai nepatikrino ir to procesiškai neužfiksavo, o panašaus pobūdžio kaltinimas verčia suabejoti visu eksperto darbu ir jo išvadų teisingumu. Siekiant išvengti trečiosios klaidos, kai tiriamasis kompiuteris nepatikrinamas dėl virusų ar programinių užsklandų, pasekmių, būtina tyrimo veiksmo metu pasitelkti specialistą, kuris patikrintų visas informacijos laikmenas (kietuosius, lanksčiuosius diskus ir kitas laikmenas) specialių programinių priemonių pagalba, pakraudamas tiriamąjį kompiuterį naudojant ne jo operacinę sistemą, bet iš specialiai paruošto kietojo ar kito disko.

Apibendrindami praktinės teisėsaugos institucijų veiklos rezultatus, įvairių šalių specialistai (pvz., Ukrainos specialistai tarptautinėje konferencijoje „Informacinės technologijos ir saugumas“[52], JAV specialistai anksčiau minėtame tarptautiniame Baltijos regiono seminare „Kompiuterinių nusikaltimų ikiteisminis tyrimas ir teisminis nagrinėjimas“), pateikia tokias pagrindines rekomendacijas, skirtas ikiteisminio tyrimo pareigūnams, tiriantiems kompiuterinius nusikaltimus, leisiančias išvengti esminių šių nusikaltimų tyrimo klaidų bei rasti ir tinkamai užfiksuoti kompiuterinius įkalčius: vykdant bet kurį tyrimo veiksmą (ypač kompiuterinės įrangos ir informacijos poėmį), tikslinga nuo pat pradžių pasitelkti informacinių technologijų specialistą; iki tyrimo veiksmų pradžios svarbu turėti apibrėžtą pirminę informaciją apie tyrimo objektą (kompiuterio, jo operacinės sistemos, išorinių įrenginių, ryšio priemonių tipą, modelį ir kitus duomenis); vykdant kompiuterio ar kompiuterinės sistemos poėmį, būtina tinkamai sužymėti ir nufotografuoti jų elementus bei jungtis; atliekant tyrimo veiksmą pirmiausia būtina padaryti rezervinę kompiuterinės informacijos kopiją; svarbu surasti ir padaryti laikinų bylų (failų) kopijas; būtina patikrinti Swap File; esant galimybei, reikia surasti ir sulyginti tekstinių dokumentų kopijas. Atliekant kompiuterinių nusikaltimų tyrimo veiksmus, tyrėjas turėtų 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 kompiuterinių nusikaltimų tyrimo veiksmų metu būtina griežtai laikytis baudžiamojo proceso normų ir visus elektroninius įkalčius, esančius kompiuteryje, kompiuterių tinkle ar informacinėje sistemoje, surinkti teisėtais būdais, kad jie galėtų būti pripažinti įrodymais teisme. Tuo tarpu užsienio valstybių patirtis rodo, kad labai dažnai, kaltinamojo gynėjų pastangomis, elektroniniai įrodymai teisme nėra pripažįstami dėl ikiteisminio tyrimo pareigūnų klaidų. Todėl labai svarbu vykdant kompiuterio ar kompiuterinės sistemos poėmį tinkamai sužymėti

[52] Голубев В.А. Некоторые вопросы расследования компьютерных преступлений // Сборник научных трудов международной конференции „Информационные технологии и безопасность“.– Киев, 2003. Выпуск 3. Стр.28 – 36.

ir nufotografuoti jų elementus bei jungtis, nes kompiuterio ar jų sistemos būklės tikslus užfiksavimas ir dokumentavimas atliekant pirminio tyrimo veiksmus leidžia teisingai sumontuoti įrangą, pajungti visus jos elementus ir tiksliai atkurti jos būklę laboratorijos sąlygomis. Fotografuojant reikia užfiksuoti priekinės ir užpakalinės kompiuterio dalies bei išorinių įrenginių vaizdus stambiu planu.

Vykdant tyrimo veiksmą, būtina padaryti rezervinę kompiuterinės informacijos kopiją, tačiau daryti informacijos (disko, bylų, failų) kopijas naudojantis tik standartinėmis rezervinio kopijavimo programomis nepakanka, nes daiktiniai įrodymai gali egzistuoti sunaikintų ar paslėptų bylų pavidalu, o duomenis susietus su šiomis bylomis (failais), galima išsaugoti tik pasinaudojus specialia programine įranga (paprastai naudojamos tokios programos kaip SafeBack, o lankstiems diskams kopijuoti pakanka naudoti DOS programą Diskcopy). Laikmenos, į kurias numatoma kopijuoti informaciją, turi būti iš anksto paruoštos (jos turi būti tuščios, be jokios kitos informacijos) ir saugomos specialiose apsauginėse pakuotėse.

Atkreiptinas dėmesys į tai, kad daugelis tekstinių redaktorių ir duomenų bazių valdymo programų kaip šalutinį normalaus programinės įrangos veikimo rezultatą sukuria laikinus failus, kurie dažniausiai yra pačios programos sunaikinami darbo seanso pabaigoje, tačiau duomenys, esantys šiuose failuose, gali būti labai naudingi bylai (pvz., galima atkurti failą, jei išeities failas buvo užkoduotas arba sukurtas tekstinis failas buvo išspausdintas, bet nebuvo išsaugotas diske). Naudingų duomenų galima rasti ir Microsoft Windows operacinės sistemos įrankiuose, susijusiuose su kompiuterinės informacijos analize, t.y. Swap File, kuris dirba kaip disko atmintinė, didžiulė duomenų bazė su daugybe skirtingų laikinų informacijos fragmentų, tarp kurių gali būti aptinkamas net ir visas dokumento tekstas. Tyrėjas turi atkreipti dėmesį ir į įvairiose laikmenose, kietajame diske aptiktas tekstinio dokumento kopijas, kurias būtina sulyginti naudojant paprastą tekstinį redaktorių, nes nežymiai besiskiriančios vieno dokumento kopijos gali atskleisti svarbios bylai informacijos ir turėti įrodomąją vertę.

Apibendrinant tai, kas išdėstyta, galima konstatuoti, kad ikiteisminio tyrimo pareigūnų ir pasitelktų specialistų bendras profesionalus darbas vykdant kompiuterinio nusikaltimo pirminio tyrimo veiksmus leidžia išvengti esminių šios rūšies nusikaltimų tyrimo klaidų, kurios galėtų sąlygoti kompiuterinės informacijos praradimą ar sugadinimą, bei rasti ir tinkamai užfiksuoti kompiuterinius įkalčius, turinčius įrodomąją vertę teisminio bylos nagrinėjimo metu.

IŠVADOS

1. Apibendrinus Lietuvos ir kitų valstybių patirtĮ bandant apibrėžti kompiuterinių 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 kėsinamasi Į visuomeninius santykius kompiuterinės informacijos apdorojimo procese ir kompiuterinės informacijos saugumą kaip nusikaltimo objektą.

Galima konstatuoti, jog iškelta hipotezė**,** jog kompiuteriniai nusikaltimai, atsižvelgiant Į jų pagrindinių struktūrinių elementų, technologijos savitumą (pasikėsinimo dalyko skaitmeninę formą, automatizaciją, duomenų perdavimo tinklų panaudojimą), yra atskira nusikaltimų rūšis, kuri ženkliai skiriasi nuo tradicinių nusikaltimų bei nėra tapati nusikaltimų elektroninėje erdvėje sąvokai, o kompiuterinių nusikaltimų išskirtinės savybės sąlygoja ir šių nusikaltimų tyrimo ypatumus, pasitvirtino.

KompiuterinĮ nusikaltimą galima būtų apibrėžti kaip baudžiamojo Įstatymo numatytą visuomenei pavojinga veiką, darančią 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 kitokĮ veiksmą arba veiksmų rinkinĮ. Lietuvos Respublikos baudžiamajame kodekse terminas „kompiuterinis nusikaltimas“ nėra apibrėžtas, taigi jis oficialiai nėra Įteisintas *de jure*, tačiau kalbant apie veikas, susijusias su kompiuterinėmis technologijomis bei elektronine erdve, dažniausiai vartojamas *de facto*. Nusikaltimų elektroninėje erdvėje sąvoka yra platesnė, apimanti ir kompiuterinius nusikaltimus, ir kitas nusikalstamas veikas, susijusias ne tik su kompiuterinių, bet ir su telekomunikacinių technologijų panaudojimu.

2. Išanalizavus Europos Sąjungos ir kitų valstybių baudžiamosios politikos patirtĮ, darytina išvada, jog naudojami du visuomenei pavojingų veikų, darančių žalą visuomeniniams santykiams kompiuterinės informacijos tvarkymo srityje, teisinio reglamentavimo būdai: 1) baudžiamuosiuose Įstatymuose numatomos atskiros specialios normos (skyriai, dalys), kurios prireikus papildomos naujomis sudėtimis, arba 2) taikomos tradicinės baudžiamųjų Įstatymų normos (reglamentuojančios nusikaltimus nuosavybei, asmens privataus gyvenimo neliečiamumui, intelektinei nuosavybei, dorovei ir kt.). Pirmojo būdo privalumas tas, jog veikos yra tiksliai apibrėžiamos, o trūkumas tas, jog rizikuojama atsilikti nuo kompiuterinių technologijų tobulėjimo; antrojo būdo privalumas tas, jog nereikia keisti baudžiamųjų Įstatymų, tačiau trūkumas tas, jog gali būti baudžiamos veikos, kurios nėra tokios pavojingos visuomenei, kad būtų kriminalizuotos, ir kartu kyla pavojus palikti nebaudžiamomis pavojingas visuomenei veikas, kurias sunku kvalifikuoti

pagal tradicines baudžiamųjų Įstatymų 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 Įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti. Būtina pastebėti, kad veikos, nurodytos šiame skyriuje, dažnai Įvykdomos ne kaip atskiri nusikaltimai, bet kartu su kitais nusikaltimais ir inkriminuojamos papildomai. Tai sąlygota aplinkybės, jog inforamcinės technologijos neretai panaudojamos siekiant Įvykdyti kitas nusikalstamas veikas.

Įvertinus 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 didele 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 Įstatymai 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 kitų nusikaltimų rūšių charakteristika, pasižymi savitomis ypatybėmis, kurias sąlygoja kompiuterinių nusikaltimų pagrindinių struktūrinių elementų specifika ir išskirtiniai, tik šiai nusikaltimų rūšiai būdingi bruožai.

Siekiant sėkmingai ištirti kompiuterinius nusikaltimus, būtina Įvertinti kompiuterinės informacijos, kaip pasikėsinimo dalyko, išskirtines kriminalistines ypatybes: kompiuterinė informacija palyginti paprastai ir greitai keičiama (kinta), kopijuojama, dauginama Įvairia technine Įranga, siunčiama Įvairiausiu atstumu, ribojamu tik elektroninių ryšių Įrangos veikimo plotu; paimant kompiuterinę informaciją (atliekant poėmĮ), skirtingai nei materialų objektą (daiktą), 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 valstybių ir Lietuvos duomenis: 1) *amžius*: 54 proc. (Liet. 64 proc.) – 20-40 metų; 33 proc. (Liet. 22 proc.) – jaunesni kaip 20 metų; 13 proc. (Liet. 14 proc.) – vyresni kaip 40 metų; 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.) – nusikalstamų grupių nariai; 38 proc. (Liet. 71 proc.) – veikia be bendrininkų; 4) intelektas: 21 proc. – aukštesnis nei vidutinis; 2 proc. – žemesnis nei vidutinis; 5) profesija: 52 proc. nusikaltėlių profesija susijusi su informacinėmis technologijomis; 6) motyvai ir tikslai: 1) savanaudiški – didžioji dalis, 66 proc.; politiniai (terorizmas, politinės akcijos) – 17 proc.; tiriamieji – 7 proc.; chuliganiški – 5 proc.; keršto – 4 proc.

Palyginus pasaulio ir Lietuvos kompiuterinių nusikaltimų tendencijas bei įvertinus šių nusikaltimų latentiškumą, galima daryti prielaidą, jog šiuo metu Lietuvoje išaiškinama daugiausia santykinai nesudėtingų kompiuterinių nusikaltimų, nes daugiau nei pusė juos padariusių asmenų teturi vidurinį ar žemesnį išsilavinimą, be to, mažiau nei trečdalis jų yra nusikalstamų grupių nariai, kai tuo tarpu kitose Europos valstybėse ir JAV didžioji dalis šių asmenų priskiriami „baltųjų apykaklių“, t.y. turinčių aukštąjį išsilavinimą tarnautojų ir darbuotojų, kategorijai, o nusikalstamų grupių nariai sudaro net šešiasdešimt procentų visų padariusių kompiuterinius nusikaltimus asmenų.

Atkreiptinas dėmesys į tai, kad kitaip nei senasis Baudžiamasis kodeksas, galiojantis Baudžiamasis kodeksas detaliai neaprašo kompiuterinių nusikaltimų padarymo būdų, nes teisiškai netikslinga ir praktiškai neracionalu apibrėžti visus būdus, kuriais galima paveikti kompiuterinę informaciją, ypač įvertinus jų dinamiką. Kompiuterinių nusikaltimų įvykdymo būdų turinys gali būti sudarytas iš įvairiausių veiksmų derinių, priklausančių nuo pažeidėjo išradingumo, kvalifikacijos ir intelekto. Tačiau, nepaisant kompiuterinių nusikaltimų įvykdymo būdų įvairovės, juos galima sugrupuoti pagal metodus į keturias grupes: 1) perėmimo; 2) neteisėtos prieigos; 3) manipuliacijų; 4) kompleksinius.

4. Teisės teoretikų ir praktikų nuomonių dėl kompiuterinių nusikaltimų ir jų tyrimo metodų, kurie gana stipriai skiriasi nuo tradicinių nusikaltimų, įvairovė bei vieningos pozicijos stygius lemia tai, kad iki šiol Lietuvoje dar nėra parengtos kompiuterinių nusikaltimų tyrimo metodikos, pagrįstos susistemintomis teorinėmis žiniomis ir patikrintos praktikoje.

Kompiuterinių nusikaltimų tyrimo užduotis yra surinkti ir užfiksuoti šiuos duomenis: baudžiamojo įstatymo numatytos veikos požymius; šia veika padarytos žalos pobūdį ir dydį; priežastinį ryšį tarp veikos ir jos pasekmių, nustatant kaltininko veiksmų pobūdį, nusikaltimo padarymo būdą, kaltininko tyčią. Tipinėse kompiuterinių nusikaltimų tyrimo situacijose pagrindiniai pirminiai tyrimo veiksmai yra šie: įvykio vietos apžiūra; kompiuterinės įrangos apžiūra (paties kompiuterio ir kitų įrenginių), kompiuterinės informacijos laikmenų apžiūra (fiksuojant svarbius tyrimui duomenis – įtariamojo prisijungimo prie sistemos laiką ir būdą (vadinamuosius

„log failus“), nusikalstamo poveikio jai pėdsakų paieška ir poėmis, liudytojų apklausa, nukentėjusiojo apklausa. Jei įtariamasis nesulaikytas, greta minėtų pirminių tyrimo veiksmų, būtina organizuoti jo paiešką, taip pat, pasitelkus nukentėjusį asmenį ir specialistus, nustatyti nusikaltimo padarymo būdo 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 įvykio vietos apžiūrą atlikti naudojant ekscentrinį taktinį būdą („nuo centro – iki periferijos“), kur „centru“ (įvykio vietos apžiūros išeities tašku) laikoma konkreti kompiuterinė įranga (arba kompiuterinės informacijos kaupiklis, laikmena), o kompiuterinės informacijos laikmenų (dažniausiai kietojo disko, lanksčiųjų diskų, kompaktinių diskų ir kt.) apžiūrą atlikti naudojant taktinį būdą „nuo bendro prie atskiro“.

Atsižvelgiant į tai, jog tiriant kompiuterinius nusikaltimus nepakanka profesinių teisinių žinių, visuose kriminalistikos metodikos darbuose tyrėjui patariama pasitelkti informacinių technologijų specialistą atliekant bet kurį tyrimo veiksmą. Vykdant kompiuterinės techninės bei programinės įrangos apžiūrą, kratą ar poėmį, svarbu elgtis ypač atidžiai, atsižvelgti į kompiuterinės informacijos saugojimo, pėdsakų slėpimo priemonių ir būdų ypatybes, numatyti kaltininko priešiškų veiksmų bei kitų faktorių poveikio informacijai galimybes.

Apibendrinus kriminalistikos bei informacinių technologijų saugos specialistų pasiūlymus ir išanalizavus praktinės teisėsaugos institucijų veiklos rezultatus, darytina išvada, jog dažniausiai pasitaiko šios esminės kompiuterinių nusikaltimų 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 dėl virusų ar programinių užsklandų. *Pagrindinės rekomendacijos*, skirtos ikiteisminio tyrimo pareigūnams, tiriantiems kompiuterinius nusikaltimus, padėsiančios išvengti esminių šių nusikaltimų tyrimo klaidų bei rasti ir tinkamai užfiksuoti įkalčius:

1) iki tyrimo veiksmų pradžios, jei įmanoma, reikėtų turėti apibrėžtą pirminę informaciją apie tyrimo objektą (kompiuterio, jo operacinės sistemos, išorinių įrenginių, ryšio priemonių tipą, modelį ir kitus duomenis);

2) atliekant tyrimo veiksmus, būtina ne tik žinoti saugaus darbo su kompiuterine informacija taisykles, bet ir išmanyti apsaugos priemones (programines bei technines), kurias naudoja nusikaltėliai, siekdami sunaikinti ar pakeisti kompiuterinę informaciją;

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

4) vykdant bet kurį tyrimo veiksmą (ypač kompiuterinės įrangos ir informacijos

poėmĮ), reikėtų nuo pat pradžių pasitelkti informacinių technologijų specialistą, nes kompiuteris pirmiausia yra specialisto tyrimo objektas, todėl iki jis bus perduotas specialistui ar ekspertui, tyrėjams rekomenduojama susilaikyti nuo bet kokių veiksmų su kompiuteriu arba griežtai laikytis būtinų saugos priemonių;

5) vykdant bet kokią operaciją su kompiuteriu, būtina užfiksuoti jo būseną tyrimo veiksmo vykdymo metu, kitaip tariant, tyrėjui rekomenduojama užantspauduoti kompiuterĮ tokios būsenos, kokios jis rastas, neišjungiant jo ar neĮjungiant;

6) jei esant būtinybei priimamas sprendimas apžiūrėti kompiuterĮ vietoje, pirmiausia reikia padaryti rezervinę kopiją visų kietųjų, lanksčiųjų, kompaktinių diskų ir kitų laikmenų, kurie bus paimami kaip Įkalčiai, būtina naudoti apsaugą nuo pakeitimų; svarbu surasti ir padaryti laikinų failų kopijas, patikrinti Swap File; jei Įmanoma, reikia surasti ir sulyginti tekstinių dokumentų kopijas;

7) tyrimo veiksmo metu pasitelktas specialistas turėtų patikrinti visas informacijos laikmenas (kietuosius, lanksčiuosius, kompaktinius diskus ir kitas) specialių programinių priemonių pagalba, pakraudamas tiriamąjĮ kompiuterĮ naudojant ne jo operacinę sistemą, bet iš specialiai paruošto kietojo ar kito disko (jei tiriamajame kompiuteryje yra Įdiegta apsaugos sistema (prieigos kodas, slaptažodis ar kt.), tai netinkamas jo Įjungimas gali sąlygoti informacijos, esančios kietajame diske, sunaikinimą, todėl neleidžiama aktyvuoti tokio kompiuterio naudojant jo paties operacinę sistemą);

8) vykdant kompiuterio ar kompiuterinės sistemos poėmĮ, būtina tinkamai sužymėti ir nufotografuoti jų elementus bei jungtis;

9) tyrimo veiksmų metu būtina griežtai laikytis baudžiamojo proceso normų ir visus ne tik tradicinius, bet ir skaitmeninius Įkalčius, esančius kompiuteryje, kompiuterių tinkle ar informacinėje sistemoje, surinkti teisėtais būdais, kad jie galėtų būti pripažinti Įrodymais teisme.

Atsižvelgiant Į kompiuterinių nusikaltimų ypatybes bei Įvertinus kompiuterinės programinės ir techninės Įrangos kaip kriminalistinio objekto sudėtingumą, būtina pastebėti, jog šios rūšies nusikaltimų bylų sėkmingam tyrimui ypač didelę reikšmę turi tinkamas specialiųjų žinių panaudojimas ir ekspertizės, tačiau pastebėtina ir tai, jog plintant nusikaltimams elektroninėje erdvėje, teisėsaugos institucijoms būtina kaupti žinias apie informacinių sistemų veikimo bei saugumo užtikrinimo principus, procedūras, darbo su kompiuterine informacija metodus bei kelti pačių teisėsaugos pareigūnų specialiąją kvalifikaciją ir kurti specialius padalinius kovai su kompiuteriniu nusikalstamumu, nes vienkartinis informatikos specialistų ar ekspertų Įtraukimas tiriant bylas nėra pakankamai efektyvus ir negali užtikrinti moksliškai pagrĮstos šios rūšies nusikaltimų tyrimo metodikos suformavimo.

2006-12-02 Renata Kačinskaitė

SANTRAUKA

Šiame darbe „Kompiuteriniai nusikaltimai ir jų tyrimo ypatumai“ nagrinėjamos baudžiamojo Įstatymo numatytos visuomenei pavojingos veikos, darančios 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 kompiuterinių 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 kėsinamasi į visuomeninius santykius kompiuterinės informacijos apdorojimo procese kaip nusikaltimo objektą.

Kompiuteriniai nusikaltimai, atsižvelgiant į jų pagrindinių struktūrinių elementų, technologijos savitumą (pasikėsinimo dalyko – kompiuterinės informacijos – skaitmeninę formą, duomenų perdavimo tinklų panaudojimą ir kt.), yra atskira nusikaltimų rūšis, kuri ženkliai skiriasi nuo tradicinių nusikaltimų bei nėra tapati nusikaltimų elektroninėje erdvėje sąvokai, o kompiuterinių nusikaltimų išskirtinės savybės sąlygoja ir šių nusikaltimų tyrimo specifiką.

Kompiuterinį nusikaltimą galima būtų apibrėžti kaip baudžiamojo Įstatymo numatytą visuomenei pavojinga veiką, darančią 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 kitokį veiksmą arba veiksmų rinkinį. Nusikaltimų elektroninėje erdvėje sąvoka yra platesnė, apimanti ir kompiuterinius nusikaltimus, ir kitas nusikalstamas veikas, susijusias ne tik su kompiuterinių, bet ir su telekomunikacinių technologijų panaudojimu. Lietuvos Respublikos baudžiamajame kodekse terminas „kompiuterinis nusikaltimas“ nėra apibrėžtas, taigi jis oficialiai nėra įteisintas *de jure*, tačiau kalbant apie veikas, susijusias su kompiuterinėmis technologijomis bei elektronine erdve, dažniausiai vartojamas *de facto*. Įvertinus kompiuterinių 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 didele problema Lietuvoje lieka šios srities terminijos teisinis neapibrėžtumas.

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

Įsilaužėlius mėgėjus *(crackers)*, profesionalius nusikaltėlius *(criminals)* ir vandalus *(vandals)*; pagal specializaciją tokie asmenys skirstomi Į hakerius, krekerius, karderius ir frekerius *(hacker, cracker, carder, phracker)*. Siekiant sėkmingai ištirti kompiuterinius nusikaltimus, būtina Įvertinti kompiuterinės informacijos, kaip *pasikėsinimo dalyko*, išskirtines kriminalistines ypatybes: kompiuterinė informacija palyginti paprastai ir greitai keičiama, kopijuojama, dauginama Įvairia technine Įranga, siunčiama Įvairiausiu atstumu, ribojamu tik elektroninių ryšių Įrangos veikimo plotu; paimant kompiuterinę informaciją (atliekant poėmĮ), skirtingai nei materialų objektą (daiktą), ji išlieka pirminiame šaltinyje, nes prieigą prie jos gali turėti tuo pačiu metu keli asmenys. Kompiuterinių nusikaltimų *Įvykdymo būdai* nuolat tobulėja, jų turinys gali būti sudarytas iš Įvairiausių veiksmų derinių, priklausančių nuo pažeidėjo kvalifikacijos, intelekto ir naudojamos Įrangos lygio. Tačiau, nepaisant kompiuterinių nusikaltimų Įvykdymo būdų Įvairovės, juos galima sugrupuoti pagal metodus Į keturias grupes: 1) perėmimo; 2) neteisėtos prieigos; 3) manipuliacijų; 4) kompleksinius.

Tipinėse kompiuterinių nusikaltimų tyrimo situacijose pagrindiniai *pirminiai tyrimo veiksmai* yra šie: Įvykio vietos apžiūra; kompiuterinės Įrangos apžiūra (paties kompiuterio ir kitų Įrenginių), kompiuterinės informacijos laikmenų apžiūra, nusikalstamo poveikio jai pėdsakų paieška ir poėmis, liudytojų apklausa, nukentėjusiojo apklausa. Jei Įtariamasis nesulaikytas, greta minėtų pirminių tyrimo veiksmų, būtina organizuoti jo paiešką, taip pat, pasitelkus nukentėjusĮ asmenĮ ir specialistus, nustatyti nusikaltimo padarymo būdo 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 Įvykio vietos apžiūrą atlikti naudojant ekscentrinĮ taktinĮ būdą („nuo centro – iki periferijos“), kur „centru“ (Įvykio vietos apžiūros išeities tašku) laikoma konkreti kompiuterinė Įranga (arba kompiuterinės informacijos kaupiklis, laikmena), o kompiuterinės informacijos laikmenų (dažniausiai kietojo disko, lanksčiųjų diskų, kompaktinių diskų ir kt.) apžiūrą atlikti naudojant taktinĮ būdą „nuo bendro prie atskiro“.

Atsižvelgiant Į tai, jog tiriant kompiuterinius nusikaltimus nepakanka profesinių teisinių žinių, tyrėjui patariama pasitelkti informacinių technologijų specialistą atliekant bet kurĮ tyrimo veiksmą. Vykdant kompiuterinės techninės bei programinės Įrangos apžiūrą, kratą ar poėmĮ, svarbu elgtis ypač atidžiai, atsižvelgti Į kompiuterinės informacijos saugojimo, pėdsakų slėpimo priemonių ir būdų ypatybes, numatyti kaltininko priešiškų veiksmų bei kitų faktorių 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.

LITERATŪROS SĄRAŠAS

I. Teisės aktai ir teismų praktika

1. Lietuvos Respublikos Konstitucija // Valstybės žinios, 1992, Nr.33-1014.
2. Lietuvos Respublikos administracinių 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 teisinės apsaugos Įstatymas // Valstybės žinios, 1996, Nr. 63-1479; 2003, Nr. 15-597.
6. Lietuvos Respublikos autorių teisių ir gretutinių teisių Įstatymas // Valstybės žinios, 1999, Nr. 50-1598.
7. Lietuvos Respublikos Įstatymas „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 Įstatymas „Dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo“ // Valstybės žinios, 2004, Nr. 36-1178).
9. Lietuvos Respublikos Įstatymas „Dėl Konvencijos dėl elektroninių nusikaltimų Papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo ratifikavimo“ // Valstybės žinios, 2006, Nr. 75-2848)
10. Lietuvos Respublikos elektroninių ryšių Įstatymas // Valstybės žinios, 2004, Nr. 69-2382.
11. Lietuvos Respublikos mokėjimų Įstatymas // Valstybės žinios, 1999, Nr. 97-2775; 2003, Nr. 61-2753.
12. Lietuvos Respublikos patentų Įstatymas // Valstybės žinios, 1994, Nr. 8-120.
13. Lietuvos Respublikos teismo ekspertizės Įstatymas // Valstybės žinios, 2002, Nr. 112-4969.
14. Lietuvos Respublikos valstybės ir tarnybos paslapčių Įstatymas // Valstybės žinios, 1999, Nr. 105-3019; 2004, Nr. 4-29.
15. Lietuvos Respublikos valstybės registrų Įstatymas // Valstybės žinios, 1996, Nr.86-2043; 2004, Nr. 124-4488.
16. Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimas Nr. 451 „Dėl Valstybės informacinių sistemų steigimo ir Įteisinimo taisyklių 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 atakų 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, patvirtinantį 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. Recomendation 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 sukčiavimo 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 millenium // http://www.crime-research.org/ library/bileng.htm.

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

30. Burda R. Kompiuterinės Įrangos 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., Osinaitė G. ir kt. Informacinių technologijų teisė./ Red. Sauliūnas D./ – Vilnius: NVO Teisės institutas, 2004.
34. Čėsna R., Štitilis D. Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. – Vilnius: Lietuvos teisės akademija, 2000.
35. Danisevičius P., Kazlauskas M., Palskys E. Kriminalistika. - Vilnius, 1985.
36. Deringas A., Rinkevičienė Z., Sakalauskas L. Kompiuteriniais spausdintuvais išspausdintų dokumentų 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. Elektroninių ryšių teisė.– Vilnius: Eugrimas, 2005.
40. Kligys V., Jankauskas V. Informacinių technologijų ekspertizė LTEC: dabartis ir perspektyva // Vilnius: Mykolo Romerio universitetas, 2005.
41. Kuklianskis S. Nusikaltimų tyrimo organizavimo pradmenys. - Vilnius, 1995.
42. Lamanauskas T. Informacinių technologijų teisės kronika // Justitia, 2001, Nr. 4–5.
43. Lamanauskas T. Informacinių technologijų teisės naujienos // Justitia, 2001, Nr. 1-3.
44. Malevski H. Įvykio vietos apžiūra. – Vilnius: Lietuvos teisės 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., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. - Vilnius: Lietuvos teisės akademija, 2000.
48. Sabaliauskas G. Informacijos saugumas internete: teisininkų ir informatikų 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. Tarptautinių žodžių žodynas. – Vilnius, 1985.
52. Teismo ekspertizių 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.

54. Батурин Ю.М. Проблемы компьютерного права. Москва: Юридическаялитература, 1991.

55. Батурин Ю.М. Компьютерное преступление – что за термином? // Право и информатика. Москва: МГУ, 1990.

56. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – Москва: Юридическая литература, 1991.

57. Безруков Н.Н. Компьютерные вирусы. - Москва: Наука, 1991.

58. Белкин Р.С. Курс криминалистики. Т. 3: Криминалистические средства, приемы и рекомендации. - Москва: Юристъ, 1997.

59. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. - Москва: Право и закон, 1996.

60. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. Волгоград: ВА МВД России, 1998.

61. Вехов В.Б, Голубев В.А. Расследование компьютерных преступлений в странах СНГ. – Волгоград: ВА МВД России, 2004.

62. Воронов И.А. Некоторые проблемы действующего законодательства по вопросам уголовной ответственности за преступления в сфере использования электронно-вычислительных машин // http://www.crime-research.org/ library/voron.htm.

63. Воронов И.А. Понятие преступлений в сфере высоких технологий // http://www.crime-research.org/ library/cyberpon.htm.

64. Голубев В.А. Информационная безопасность: проблемы борьбы с киберпреступлениями.– Запорожье: ГУ „ЗИГМУ“, 2003.

65. Голубев В.А. Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий // http://www.crime-research.ru.

66. Голубев В.А. Некоторые вопросы расследования компьютерных преступлений // Сборник научных трудов международной конференции „Информационные технологии и безопасность“. Выпуск 3. – Киев, 2003.

67. Горбатов В.С., Полянская О.Ю. Мировая практика криминализации компьютерных правонарушений. - Москва: МИФИ, 1998.

68. Дулов А.В. Криминалистический анализ компьютерных преступлений. // Проблемы «компьютерной преступности»: Выпуск 2. - Минск: НИИ ПККСЭ МЮРБ, 1992.

69. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность // Юридический мир, 1998.

70. Компьютерная преступность и кибертерроризм: сборник научных статей / Подред. Голубева В.А., Рыжкова Э.В. – Запорожье: Центр исследования компьютерной преступности, 2005.
71. Конявский В.А., Лопаткин С.В. Компьютерная преступность. – Москва: РФК – Имидж Лаб, 2006, Т. 1.
72. Криминалистическая методика: методика расследования преступлений в сфере экономики, взяточничества и компьютерных преступлений. – Москва, 2001, Т. 3.
73. Мелик Э. Компьютерные преступления. Информационно-аналитический обзор // http://www.melik.narod.ru.
74. Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации. // Конфидент, С.Петербург, 1999. №4-5.
75. Минаев В.А., Саблин В.Н. Основные проблемы борьбы с компьютерными преступлениями в России // http://www.mte.ru/www/toim.nsf.
76. Румянцев А.Г. Информационное право // http://www.aha.ru/~andrew_r/infolaw.
77. Селиванов Н.А. Проблемы борьбы с компьютерной преступностью // Законность.- Москва, 1993, №8.
78. Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика расскрытия и расследования.- Курган, 1999.
79. Экенвайлер М. Преступная деятельность, совершаемая с использованием режима „онлайн“ (Тезисы докладов на международной конференции „Проблемы борьбы с новыми видами экономических преступлений в России и США“, 20–21 мая 1997 года) // http://www.uic.ssu.samara.ru/~cclub/navigator/uglaw.htm.
80. Яковлев А.Н. Использование специальных познаний при расследовании «компьютерных» преступлений // Конфидент, С.Петербург, 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
87. http:// www.cybercellmumbai.com
88. http:// www.cybercrime.gov
89. 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
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
105. http://www3.lrs.lt/dokpaieska/forma_l.htm
106. http://www3.lrs.lt/pls/inter1/dokpaieska.forma_l