MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETAS
INFORMATIKOS IR STATISTIKOS KATEDRA

MANTAS SAVICKAS
INFORMATIKOS TEISĖ

TEMA

NUSIKALTIMŲ INFORMATIKAI SAMPRATOS PROBLEMA

Magistro baigiamasis darbas

Darbo vadovas –
Doc. dr.
Darius Štitilis

Vilnius 2006

TURINYS

ĮVADAS

Begalinis ir nesutramdomas naujausiųjų informacinių technologijų vystimasis ir skverbimasis į visas žmonių veiklos sritis neabejotinai iššaukia teigiamų poslinkių žmonijos ekonominėje, socialinėje raidoje. Dar niekada istorijoje žmonija taip gretai neprogresavo, kaip per paskutinius 50 metų. Tačiau visuotinė kompiuterizacija turi ir savo tamsiąją pusę – tai nusikaltimai. Laikui bėgant ši problema darosi vis aktualesnė, atsižvelgiant į tai, kokiais tempais progresuoja informacinės technologijos. Įvairios finansinės, valstybinės institucijos savo veikloje naudojasi informacinėmis technologijomis, jų teikiamais resursais, tarpusavyje sujungtais tinklais ir globaliais tinklais. Kasdiene rutina tarp šių institucijų migruojančios (nuliukų ir vienetukų pavidalu) finansinės ataskaitos, teisinės išvados ir kitokie svarbūs dokumentai. Ir kartais net neįtariama, kad gerai informacines technologijas išmanančiam asmeniui pasitelkus visiems laisvai prieinamą, kasdieniu buitiniu prietaisu tapusį kompiuterį, gali nukopijuoti, sunaikinti ar kitaip pakeisti minėtus dokumentus. Blogiausia ir nuostabiausia tai, kad asmuo darydamas nusikaltimą gali būti visai kitoje šalyje ar net kitame žemyne. Taigi, informacinės technologijos nusikaltimus iškėlė visai į kitą lygmenį. Jos atvėrė duris neteisėtiems, nusikalstamiems veiksmams, kurie anksčiau nebuvo įmanomi. Skaitmeninės sistemos, įstatymų laužytojams pasiūlė naujų galimybių, jos sukūrė visiškai naują terpę. Sparti kompiuterinio tinklo plėtra padidino įvairių sistemų pasiekiamumą ir tuo pačiu jų pažeidžiamumą. Tokiu būdu informacinių technologijų pagalba padarytų nusikaltimų pasekmės gali sukelti rimtų keblumų tiek ekonominėje, tiek politinėje, tiek asmens saugumo srityje.

Dabar galiojančio Lietuvos Respublikos Baudžiamojo kodekso 11 straipsnis nusikaltimą apibrėžia kaip pavojingą ir kodekse uždraustą veiką (veikimą ar neveikimą), už kurią numatyta laisvės atėmimo bausmė.[1] Kaip matome dabartinė nusikaltimo samprata skiriasi nuo tos, kuri buvo senajame LR Baudžiamajame kodekse. Nusikaltimo sampratoje nebevardinami tie visuomeniniai santykiai, kurie yra pažeidžiami nusikaltimo. Tačiau šioje nagrinėjamoje temoje mums nėra svarbūs skirtumai tarp senos ir naujos nusikaltimo sampratos, įtvirtintos LR Baudžiamajame kodekse. Kur kas aktualesnis ir svarbesnis klausimas yra nusikaltimų informatikai vieningos sampratos nebuvimo problema. Dabar galiojantis Baudžiamasis kodeksas nepateikia jokios nusikaltimų informatikai sampratos, tik į atskirą XXX skyrių išskiria nusikaltimus informatikai. Taip pat jokios nusikaltimų informatikai sampratos nepateikia ir Europos Tarybos Konvencija dėl elektroninių nusikaltimų, priimta 2001 m. lapkričio 23 d. Budapešte. Dar 1983 metais Europos bendradarbiavimo ir plėtros organizacijos (OECD)

[1] Lietuvos Respublikos baudžiamasis kodeksas // Valstybės žinios. 2000, Nr. 89-2741.

ekspertų komitetas su kompiuteriais susijusių nusikaltimų problemoms spręsti terminą „kompiuterinis nusikaltimas“ apibrėžė kaip bet kokį neteisėtą, neetišką arba nesankcionuotą elgesį, susijusį su automatiniu kompiuterinių duomenų apdorojimu ir siuntimu, tačiau nepaminėjo, kokios teisės šakos atžvilgiu toks elgesys yra neteisėtas.[2]

Teisinėje literatūroje galima rasti įvairių nuomonių kompiuterinių nusikaltimų apibrėžimų atžvilgiu. Kai kurie autoriai teigia, kad teisine prasme tokie kaip kompiuteriniai nusikaltimai iš vis neegzistuoja. Tačiau tuo pat metu pažymi, kad daugelis tradicinių nusikaltimų modifikuojasi dėka to, kad jiems įvykdyti yra panaudojamos informacinės technologijos. Todėl į atskirą kompiuterinių nusikaltimų grupę tokių nusikaltimų išskirti nereikia, o kalbėti galima tik apie tokių nusikaltimų kompiuterinius aspektus. Tokią nuomonę išsako J. M. Baturin.[3] Kiti autoriai kompiuterinius nusikaltimus apibrėžia net dviem požiūriais: kompiuteriniai nusikaltimai baudžiamosios teisės požiūriu ir kompiuteriniai nusikaltimai kriminalistikos mokslo požiūriu. Pirmuoju atveju pagrindinis akcentas yra skiriamas mašininei informacijai, kaip nusikaltimo objektui, o antruoju atveju – nusikaltimo padarymo būdui.[4] Tokiu būdu lyg ir duodama suprasti, kad ne visi kompiuteriniai nusikaltimai yra nusikaltimai informatikai, tačiau visi nusikaltimai informatikai yra kompiuteriniai nusikaltimai.

Ne ką mažiau aktualus klausimas yra darbe naudojamų sąvokų klausimas. Dabar teisinėje (ir ne tik) literatūroje vartojamos tokios sąvokos kaip „kompiuteriniai nusikaltimai“, „informaciniai nusikaltimai“, „nusikaltimai aukštųjų technologijų srityje“, „nusikaltimai informatikai“, „elektroniniai nusikaltimai“ ir panašiai, apibūdinantys iš esmės panašius ar kitaip susijusius nusikaltimus. Taigi, nėra nusistovėjusios terminijos, kuri yra labai svarbi priimant ir taikant teisės aktus praktikoje.

Kaip matome iš aukščiau pateikto, kad nėra vieningos nuomonės teisinėje literatūroje apibrėžiant nusikaltimų informatikai sampratą. Tai stipriai įtakoja kompiuterinių nusikaltimų tyrimo rezultatus, kadangi vieningo teisinio nusikaltimo supratimo nebuvimas neskatina teisės normų suvienodinimo, kas ypač aktualu atsižvelgiant į kompiuterinių nusikaltimų globalumą. Ši problema nusako mano temos aktualumą.

Darbo tikslas – atskleisti ir išanalizuoti nusikaltimų informatikai sampratą.

Darbo uždaviniai:

1) Išanalizuoti nusikaltimų informatikai ir kitas analogiškas sampratas nustatant ir išnagrinėjant šių sampratų esminius požymius, bei palyginti jas tarpusavyje;

[2] Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. - Vilnius: LTU, 2000. P.5-6.
[3] Мелик Э. Компьютерные преступления // http://melik.narod.ru/index.html (prisijungimo laikas: 2004-09-18).
[4] Вехов В.Б. Компьютерные преступления: способы совершения, методика расследования. – Москва: Право и закон, 1996. P.23-24.

2) išanalizuoti nusikaltimų, aprašytų LR Baudžiamojo kodekso XXX skyriuje „Nusikaltimai informatikai“, sudėtis nusikaltimų informatikai sampratos kontekste.
3) Pasiūlyti priimtiną nusikaltimų informatikai sampratą remiantis išnagrinėta teisine medžiaga ir nustatyti pasiūlytos sampratos galimą įtaką kai kurių nusikaltimų informatikai teisiniam reguliavimui.

Darbo objektas: nusikaltimų informatikai sampratos problema.

Darbo dalykas: nusikaltimų informatikai samprata ir jos esminiai požymiai; vyraujančios nusikaltimų informatikai sampratos ir panašių nusikaltimų sampratos, jų lyginamoji analizė; nusikaltimai, numatyti LR Baudžiamojo kodekso XXX skyriuje nusikaltimų informatikai sampratos kontekste.

Darbas susideda iš keturių dalių. Pirmoje darbo dalyje nagrinėjama nusikaltimų informatikai samprata ir jos esminiai požymiai bei analizuojamos teisinėje literatūroje vyraujančios nusikaltimų informatikai ir panašių nusikaltimų sampratos. Antroje darbo dalyje nagrinėjami nusikaltimai, numatyti Lietuvos Respublikos Baudžiamojo kodekso XXX skyriuje nusikaltimų informatikai sampratos kontekste. Trečiame skyriuje nagrinėjama darbo autoriaus požiūrį atitinkanti nusikaltimų informatikai samprata, padėsianti vienaip ar kitaip spręsti problemą. Ketvirtoje darbo dalyje nagrinėjama galima pateiktos trečioje dalyje nusikaltimų informatikai sampratos įtaka nusikaltimų informatikai reguliavimui Lietuvoje. Darbo gale pateiktos išvados ir pasiūlymai.

1. NUSIKALTIMŲ INFORMATIKAI IR KITŲ ANALOGIŠKŲ NUSIKALTIMŲ SAMPRATOS, JŲ ESMINIAI POŽYMIAI, PANAŠUMAI BEI SKIRTUMAI:

1.2 nusikaltimų informatikai samprata ir jos esminiai požymiai

Taip susiklostė baudžiamosios teisės teorijoje, kad bet kokio nusikaltimo požymius įprasta nagrinėti nuo nusikalstamos veikos objekto. Kaip žinome iš baudžiamosios teisės teorijos, nusikalstamos veikos objektai yra skirstomi į bendrąjį, rūšinį ir tiesioginį. Bendrasis objektas – tai visų teisinių gėrių, kurie yra saugomi valstybės baudžiamųjų įstatymų, visuma. Rūšinis objektas – tai atitinkama vienarūšių ar tapačių teisinių gėrių dalis, saugoma baudžiamojo įstatymo. Ir tiesioginiu nusikaltimo objektu pripažįstamas tas teisinis gėris į kurį kėsinamasi konkrečiu nusikaltimu.[5] Nagrinėjant nusikaltimų informatikai sampratos vieną iš požymių – objektą, mums aktualiausi yra pastarieji du – tai rūšinis ir tiesioginis objektai.

Bet kurios visuomenės egzistavimas yra pagrįstas tam tikrais visuomeniniais santykiais – politiniais, ekonominiais, ūkiniais, finansiniais, informaciniais. Bet kokio nusikaltimo prigimtis yra nukreipta į tokių visuomeninių santykių nutraukimą, pažeidimą, išardymą, pakeitimą. Taigi, bet kuris nusikaltimas yra nukreiptas prieš visuomeninus santykius ir jo tikslas yra bet kokiomis priemonėmis neigiamai paveikti juos, sukeliant tam tikrus neigiamus padarinius, tai yra padaroma žala tam tikriems teisiniams gėriams. Nusikaltimai informatikai irgi ne išimtis. Jie pažeidžia visuomeninus santykius, susijusius su teisėtu informacijos kūrimu, saugojimu, naudojimu, platinimu ir kitais veiksmais. Rusijos teisėje teigiama, kad nusikaltimų informatikai bendrasis objektas yra „visuma visuomeninių santykių, sudarančių visuomenės saugumo ir viešosios tvarkos turinį“.[6] Taip manyti rusų teisininkus įgalina įstatymų leidėjas ir Rusijos Federacijos baudžiamojo kodekso struktūra. Nusikaltimai informatikai, tiksliau nusikaltimai kompiuterinės informacijos sferoje[7] yra aprašyti Rusijos Federacijos baudžiamojo kodekso IX skyriuje „Nusikaltimai prieš visuomenės saugumą ir viešėją tvarką“. Tokiu būdu Rusijos Federacijos įstatymų leidėjas nustatė nusikaltimų informacijos srityje bendrąjį objektą. Tačiau remiantis tik tokiu bendrojo objekto nustatymu dar negalima išskirti nusikaltimus informatikai į atskirą nusikaltimų rūšį. Tokio objekto nustatymas mums mažai duoda naudos. Minėtas objektas gali būti vadinamas bendriniu arba kaip atskaitos taškas, iš kurio išvedamas objektas mus priartinantis prie nagrinėjamos nusikalstamų veikų rūšies. V. Krylovas teigia, kad nusikaltimų

[5] Abramavičius A., Čepas A., Drakšienė A. ir kt. Baudžiamoji teisė: bendroji dalis. –Vilnius: Eugrimas, 1998.P.163-165.
[6] Гаврилин Ю.В., Пушкин А.В., Соцков Е.А. и др. Расследование неправомерного доступа к компьютерной информации. Учебное пособие. Изд-е второе, дополненное и переработанное / Под ред. д.ю.н. проф. Н.Г. Шурухнова. – Москва: Московский университет МВД России, 2004.P.74.
[7] Būtent taip yra įvardinti nusikaltimai informatikai Rusijos Federacijos baudžiamajame kodekse, kuris buvo priimtas 1996 metais.

kompiuterinės informacijos sferoje rūšinis objektas yra „visuomenės saugumas ir tvarka santykiuose, susijusiuose su informaciniais procesais – informacijos rinkimo, apdorojimo, kaupimo, saugojimo, paieškos ir platinimo procesais, panaudojant ESM[8], jų sistemas ir tinklus“.[9] V. S. Komisarovas teigia, kad šių nusikaltimų objektas yra „santykiai, susiję su informacijos ir informacinių resursų saugiu kūrimu, saugojimu, naudojimu ir platinimu, arba jų apsauga“.[10] Taip pat sutinkamas ir platesnis objekto apibrėžimas - „tai visuma baudžiamojo įstatymo saugomų interesų, susijusių su saugiu kompiuterinės informacijos, informacinių resursų, informacinių sistemų ir technologijų kūrimu, naudojimu ir platinimu“.[11] Dvi pastarosios nuomonės dėl nusikaltimų informatikai objekto nustatymo iš esmės galėtų būti teisingos, tačiau yra vienas bet. Atidžiau panagrinėjus tiek V.S. Komisarovo, tiek Rusijos baudžiamosios teisės vadovėlyje išreikštas nuomones, kliūna vienas žodelis – *saugus* kompiuterinės informacijos kūrimas, naudojimas, platinimas ir pan. Šiuo atveju mes negalime tapatinti saugaus informacijos kūrimo, naudojimo su, pavyzdžiui, saugiu transporto priemonių eksploatavimu, saugiu radioaktyvių medžiagų naudojimu ar saugaus elgesio su ugnimi. Juk kompiuterinės informacijos pasisavinimas, kopijavimas, ištrynimas, pašalinimas negali būti pats savaime saugus ar nesaugus tiek pačiam kompiuterinės informacijos teisėtam naudotojui, tiek ir asmeniui, kuris kėsinasi nusikalstama veika. Pati kompiuterinės informacijos specifika, kaip reiškinio, apsprendžia tai, kad atliekant kopijavimo, pašalinimo, ištrynimo, kūrimo veiksmus ji pereina iš vienos būsenos į kitą arba tiesiog išnyksta nepadarydama jokios fizinės žalos.

V.B. Vechovas pateikia kategorišką savo nuomonę dėl nusikaltimų informatikai objekto. Jo teigimu, „dviejų nuomonių dėl nusikalstamo kėsinimosi objekto būti negali – juo, savaime aišku, yra informacija, o nusikaltėlio veiksmus reikia vertinti kaip pasikėsinimą į informacinius visuomeninius santykis.“[12] Pradedant nagrinėti šį jo kategorišką teiginį iš karto mintyse kyla prieštaravimas. Viena teiginio pusė prieštarauja kitai. Mes žinome, kad nusikalstamos veikos objektas yra teisinis gėris, kuriam nusikalstamais veiksmais yra padaroma žala. V.B. Vechovas teigia, kad nusikaltimo objektas yra *informacija*. Tuomet galima manyti, kad teisinis gėris ir yra kompiuterinė informacija. Natūraliai kyla klausymas ar galima kompiuterinei informacija padaryti žalą ją kažkaip paveikiant. Juk, pavyzdžiui, kompiuterinės informacijos pasisavinimo atveju ji nėra pažeidžiama. Dėl to, autoriaus manymu, informaciją

[8] Elektroninė skaičiavimo mašina.
[9] Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. // Уголовное право, 1998. №3. P.83.
[10] Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность //Юридический мир, Февраль 1998. P.11.
[11] Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева, А.В. Наумова. – Москва: Юристъ, 1997. P.346.
[12] Вехов В.Б. Компьютерные преступления: способы совершения, методика расследования. - Москва: Право и закон, 1996. P.21.

įvardinti kaip teisinį gėrį į kurį kėsinamasi nusikalstamu veikimu nėra tikslu, greičiau informacija yra nusikaltimo nematerialus (idealus) dalykas – tai, kas yra tiesiogiai veikiama nusikalstamais veiksmais. Antra teiginio pusė nurodo, kad *nusikaltėlio veiksmus reikia vertinti kaip pasikėsinimą į informacinius visuomeninius santykius*. O nusikalstamu kėsinimusi gali būti padaroma arba padaroma tam tikra žala, tuomet objektą galėtume vertinti kaip informacinius visuomeninius santykius.

Teisiniu gėriu galima pavadinti tai, ko visuomenė savo santykiuose tikisi iš informacijos – tai jos konfidencialumo, vientisumo ir teisėto prieinamumo. Manytina, kad pagrindinis klasifikacinis kriterijus, leidžiantis nusikaltimus informatikai išskirti į atskirą nusikaltimų rūšį yra visuomenės informacinių interesų ir joje vykstančių informacinių procesų saugumo užtikrinimas. Todėl rūšiniu nusikaltimų informatikai objektu aš įvardinčiau informacijos konfidencialumą, vientisumą ir teisėtą prieinamumą. Vis dėl to, žvelgiant iš įstatymo pozicijos, pastarasis saugo tam tikras teisines vertybes. Lietuvos Respublikos „BK saugoma vertybė gali būti suprasta kaip netrukdomas, nekliudomas, neslopinamas automatinis ir paprastas informacijos apdorojimas ir/arba nekliudomas informacinės sistemos valdymas ir kontrolė. Todėl siekiant tikslumo ir vengiant dviprasmybių ... rūšinį objektą teisingiau įvardyti kaip **kompiuterinės informacijos saugumą**“[13]

Kitas labai svarbus požymis nagrinėjant nusikaltimų informatikai sampratą yra nusikaltimo dalykas. Šis nusikaltimo sudėties elementas yra glaudžiai susijęs su nusikaltimo objektu, tačiau nėra tapatus jam. Nors nusikaltimų informatikai objekto nustatymas nėra labai sudėtingas, šios rūšies nusikaltimų dalykas reikalauja daug platesnės ir išsamesnės analizės. Kaip mes gerai žinome iš baudžiamosios teisės teorijos, nusikaltimo dalykas – tai konkretūs materialaus pasaulio daiktai, kuriuos veikiant daroma žala teisiniams gėriams ar keliama tokios žalos grėsmė.[14]

Nusikaltimo dalyko teisingas nustatymas yra labai svarbus momentas, kadangi tai raktinis požymis, leidžiantis mums atskirti nusikaltimus, aprašytus Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje nuo kitų nusikalstamų veikų, patalpintų kituose skyriuose. Analizuojant nusikaltimų informatikai dispozicijas mes matome, kad įstatymų leidėjas pats mums sufleruoja, kad nusikalstamų veikų, kuriomis yra kėsinamasi į informacinius visuomeninus santykius, dalykas, pirmiausia, yra informacija kompiuterinėje formoje. Kodekse ji įvardinama kaip kompiuterinė informacija.

---

[13] Civilka M., Lamanauskas T., Osinaitė G. ir kt./red. D. Sauliūnas. Informacinių technologijų teisė. - Vilnius: NVO Teisės Institutas, 2004.P. 529.

[14] Abramavičius A., Čepas A., Drakšienė A. ir kt. Baudžiamoji teisė: bendroji dalis. –Vilnius: Eugrimas, 1998.P.166.

Kompiuterinės leksikos aiškinamasis žodynas pateikia tokį informacijos apibrėžimą: informacija – tai žinios, perduodamos vienų asmenų kitiems žodžiu arba žiniasklaidos priemonėmis: per spaudą, radiją, televiziją, kiną, kompiuterių tinklus.[15] Tai bendrinis informacijos termino suvokimas. Jų galima rasti ir daugiau. Kiekvienas mokslas suformuoja savitą požiūrį į informacijos sampratą. Informacijos terminą galima apibrėžti skirtingai įvairių mokslų požiūriu. Pavyzdžiui, „informacijos ir komunikacijos moksluose, remdamiesi mokslininkų (P. Ingwersen, B. Dervin, N. J. Belkin, A. Vickery ir kt.) darbais, galime daryti išvadą, kad informacija - *tai, kas suvokiama, vartojama ir tampa žiniomis*.“[16] Galima teigti, kad informacija yra tarpinis reiškinys tarp duomenų ir žinių. Tai paaiškinti nėra sudėtinga. Žmogus turėdamas duomenis apie vieną ar kitą reiškinį, apdorojimo procese gauna informaciją, kuri yra tik objektyvi reiškinio išraiška. Informacijos suvokimo procese žmogus įgauna žinias.

Tačiau šiame darbe mums aktualesnis informacijos apibrėžimas teisės mokslo požiūriu. Analizuodamas Lietuvos Respublikos teisės aktus, aš padariau išvadą, kad informacija, kaip terminas, nėra apibrėžtas ir paaiškintas įstatymiškai, kas suteikia teisę laisvai manipuliuoti šiuo terminu. Dėl to, manome, kad gali iškilti sunkumų interpretuojant vienas ar kitas teisės normas. Daug paprasčiau pasielgė Rusijos Federacijos įstatymų leidėjas įstatymiškai apibrėždamas informacijos sąvoką, taip eliminuodamas bet kokias „spekuliacijas“ šiuo terminu. Federalinis įstatymas apibrėžia informaciją taip: *informacija – duomenys apie asmenis, daiktus, faktus, įvykius, reiškinius ir procesus, nepriklausomai nuo pateikimo formos.*[17] Panašiai apibrėžiama informacijos sąvoka ir informacijos terminų standarte ISO 2382: „informacija vadinamos žinios apie faktus, įvykius, daiktus, procesus, idėjas, sąvokas ir kitus objektus, kurios tam tikrame kontekste turi kokią nors prasmę“.[18] Taigi, galima padaryti išvadą, kad informacija yra tam tikri duomenys apie mus supantį išorinį pasaulį. Tačiau šie duomenys tampa informacija tik tuomet, kai yra žmogaus apdorojami ir įgauna tam tikrą savęs prasmę.

Atkreiptinas dėmesys į tai, kad Lietuvos Respublikos baudžiamojo kodekso normomis yra saugoma kompiuterinė informacija - informacija fiziškai neatsiejama nuo kompiuterio, kompiuterių sistemos ar kompiuterių tinklo. Dėl to, autoriaus manymu, tikslinga būtų panagrinėti kompiuterio sampratą, o tada pereiti prie kompiuterinės informacijos suvokimo analizės.

---

[15]Kompiuterinės leksikos aiškinamasis žodynas // http://aldona.mii.lt/pms/terminai/term/z2odynas.html (prisijungimo laikas: 2005-11-09).
[16] Janiūnienė E. Biblioteka - žinių institucija // Informacijos mokslai, 2001. T.17. http://www.leidykla.vu.lt/inetleid/inf-mok/17/tomas17.html (prisijungimo laikas: 2005-10-20).
[17] Федеральный закон "Об информации, информатизации и защите информации" от 20 февраля 1995 г. N 24-ФЗ (с изменениями от 10 января 2003 г.) Принят Государственной Думой 25 января 1995 года. 2 str. // http://www.minsvyaz.ru/site.shtml?id=1066 (prisijungimo laikas: 2005-11-09).
[18] Janiūnienė E. Biblioteka - žinių institucija // Informacijos mokslai, 2001. T.17. http://www.leidykla.vu.lt/inetleid/inf-mok/17/tomas17.html (prisijungimo laikas: 2005-10-20).

Kompiuteris – tai duomenų apdorojimo įrenginys, kuris priima duomenis, juos apdoroja pagal programą ir pateikia rezultatus.[19] Kitaip sakant, kompiuteriu galime pavadinti visumą tarpusavyje sąveikaujančių techninių sprendimų, naudojančių elektros impulsus bei programines priemones, kurios suteikia galimybę atlikti įvairias operacijas su juose užfiksuotais elektroniniais duomenimis ir galimybe perteikti juos simboline išraiška. Kompiuterių sistema – tai įtaisas arba tarpusavyje sujungtų ar susijusių įtaisų grupė, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja duomenis.[20] Kompiuterių tinklas – tai du ar daugiau kompiuterių, sujungtų tarpusavyje ryšio priemonėmis (laidinėmis ryšio priemonėmis - IEEE-802.3 standartu arba belaidžiu būdu – pvz. IEEE-802.11b,a,g standartais (WiFi)) ir turintys programines priemones, leidžiančias užtikrinti šį tarpusavio ryšį. Pagrindinis skirtumas tarp kompiuterinių sistemų ir kompiuterių tinklų yra tas, kad kompiuterių sistemoje kompiuteris ar tarpusavyje sujungti kompiuteriai atlieka vieną priskirtą užduotį visi kartu. Kompiuterių tinkluose taip nėra. Kiekvienas kompiuteris gali atlikti tik jam skirtą, vartotojo nurodytą užduotį.

Rusijos ir Ukrainos teisininkai vienbalsiai teigia, kad informatikos nusikaltimų dalykas yra kompiuterinė informacija. Kartu jie pateikia ir kompiuterinės informacijos sampratas. M.V. Bogomolovas kaip kompiuterinę supranta visą informaciją, kuri cirkuliuoja kompiuteryje ar kompiuterių tinkle, taip pat įrašytą į kompiuterinę laikmeną bei įkrautą operatyvioje kompiuterio atmintyje.[21] Tačiau toks kompiuterinės informacijos apibrėžimas, autoriaus manymu, yra diskutuotinas, kadangi ne visiškai suprantamas kompiuterinės informacijos *cirkuliavimas.* Žodis *cirkuliavimas* daugiau tinkamas apibūdinti tokius dalykus, kurie nuolatos yra judėjime, nebūna nuolatos toje pačioje vietoje. Informacija, kaip žinia, gali būti užtvirtinta kompiuterinėje laikmenoje ir nekeisti savo buvimo vietos ilgą laiko tarpą. Todėl daug priimtinesnę kompiuterinės informacijos sampratą pateikia V. Golubevas. Jis teigia, kad kompiuterinė informacija - tai bet kokia informacija (duomenys), kuri egzistuoja elektroniniame pavidale, yra kompiuteryje arba kompiuterinėje laikmenoje ir kurią galima sukurti, pakeisti arba panaudoti kompiuterio pagalba.[22] Kaip matome iš šio apibrėžimo tarp informacijos ir duomenų, galima sakyti, padėtas lygybės ženklas. Tai yra, Rusijos ar Ukrainos teisininkai neišskiria šių sąvokų ir savo baudžiamuosiuose įstatymuose įtvirtino informatikos nusikaltimų dalyką – kompiuterinę informaciją. Reikia pažymėti, kad Lietuvos Respublika irgi nuėjo šiuo keliu. Tačiau lygybės ženklą tarp informacijos ir duomenų ne visada galima dėti. Kaip žinia, duomenys yra patys

[19] Kompiuterinės leksikos aiškinamasis žodynas // http://aldona.mii.lt/pms/terminai/term/z2odynas.html (prisijungimo laikas: 2005-11-09).
[20] Konvencija dėl elektroninių nusikaltimų // Valstybės žinios.2004, Nr. 36-1188.
[21] Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации // http://pu.boom.ru/book/index.html (prisijungimo laikas: 2006-11-10).
[22] Голубев В. Компьютерная информация, как объект правоотношений // http://www.crime-research.ru/library/Golubev09_03.html (prisijungimo laikas: 2005-09-27).

pirminiai faktai, kurie grupuojami, įvairiomis formomis apibendrinami ir transformuojami, kad taptų informacija.[23] Todėl galimi tokie atvejai, kai tam tikrais būdais paveikiant (modifikuojant) duomenis, informacija gali išlikti nepakitusi. Kaip pavyzdį galime pateikti interneto puslapyje esantį tam tikrą paveiksliuką su reklama, kuris yra susietas su hipertekstine nuoroda į kitą interneto puslapį ir kurį paspaudus atsiverčia reklamuojamas puslapis. Modifikavus tam tikrus duomenis, šiuo atveju hipertekstinę nuorodą, kuri kompiuterio ekrane nėra matoma, paveiksliuko duodama informacija liks nepakitusi, tačiau paspaudus ant jo atsidarys visai kitas interneto puslapis, negu yra reklamuojamas paveikslėlyje. Taigi, kaip matome modifikavus tam tikrus hipertekstinius duomenis, paveiksliuko informacija išlieka nepakitusi. Todėl kitų šalių teisė nusikaltimų informatikai dalyku pripažįsta ne kompiuterinę informaciją, o kompiuterinius duomenis. Tiek 2001 m. lapkričio 23 d. Europos Tarybos Konvencija dėl elektroninių nusikaltimų, tiek 2005 m. vasario 24 d. Tarybos pamatinis sprendimas 2005/222/TVR, dėl atakų prieš informacines sistemas mums sufleruoja, kad nusikaltimų informatikai kėsinimosi dalykas yra kompiuteriniai duomenys. Konvencija dėl elektroninių nusikaltimų pateikia kompiuterinių duomenų sąvokos apibrėžimą. Ten teigiama, kad kompiuteriniai duomenys – tai bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat programa, pagal kurią kompiuterinė sistema gali vykdyti tam tikrą funkciją.[24] Atsižvelgiant į tai, kad Lietuvos Respublikos baudžiamasis įstatymas vis dėlto nusikaltimų informatikai dalyku įvardina kompiuterinę informaciją, aš šioje darbo dalyje nagrinėdamas nusikaltimų informatikai esminius požymius remsiuosi pastaruoju požiūriu.

Atkreiptinas dėmesys į tai, kad kompiuterinė informacija apima ir kompiuterines programas. Tačiau Ukrainos teisininkas N.V. Karčevskij nesutinka su tokia nuomone, teigdamas, kad toks teiginys nėra teisingas. Jis pritaria pozicijai tų mokslininkų, kurie mano, kad informacija yra išskirtinai žmogaus sąmonės ir bendravimo savybė ir sieja ją su subjekto gebėjimu pažinti. O kalbėti apie tai, kad kompiuteris vykdydamas kompiuterines programas kaip komandų rinkinį atlieka pažinimo procesą yra neteisinga. Todėl, jo teigimu, kompiuterinės programos negali būti priskirtos prie kompiuterinės informacijos kaip nusikaltimo dalyko.[25] Nepritariu šiam teiginiui, nes remiantis tuo, kad kompiuterinė programa iš esmės yra sutvarkytas duomenų rinkinys[26], o duomenys, kaip išsiaiškinome aukščiau, apdorojimo procese tampa informacija. Todėl manytina, kad kompiuterinės programos yra tam tikra kompiuterinės

[23] Dzemydienė D., Naujikienė R. Informacinės sistemos. Duomenų struktūros ir valdymas. – Vilnius: Lietuvos teisės universitetas. 2004. P.13.
[24] Konvencija dėl elektroninių nusikaltimų // Valstybės žinios. 2004, Nr. 36-1188.
[25] Карчевский Н.В. Компьютерные преступления: определение, объект и предмет // Доклад на V Международной конференции «Право и интернет: теория и практика» http://www.ifap.ru/pi/05/karchev.htm (prisijungimo laikas: 2006-10-15).
[26] Texas penal code // http://tlo2.tlc.state.tx.us/statutes/petoc.html (prisijungimo laikas: 2006-09-01).

informacijos forma, kurios sudaro galimybę kompiuteriui atlikti tam tikrą užduotį ar funkciją, pasiekti tam tikrą rezultatą.

Pagrindinis kompiuterinės informacijos požymis yra duomenys elektronų išraiška arba, kitaip tariant, elektroniniai duomenys, kurie Lietuvos Respublikos elektroninio parašo įstatyme yra įvardinami kaip duomenys, kurie tvarkomi informacinių technologijų pagalba.[27]

Pažymėtinas svarbus momentas informacijos resursų ir informacijos procesų apsaugoje baudžiamųjų teisės normų pagalba yra įstatymų leidėjo nuoroda į įstatymų saugomą kompiuterinę informaciją. Baudžiamojo kodekso 198 straipsnio dispozicijoje sakoma, kad tas, kas pasisavino *įstatymų saugomą kompiuterinę informaciją* apie juridinį ar fizinį asmenį, baudžiamas bauda arba laisvės atėmimu iki trejų metų. Taigi, tokiu būdu kompiuterinei informacija yra nustatomas tam tikras teisinis statusas, kuris yra nusakomas Lietuvos Respublikos įstatymais. Įstatymai saugo informaciją, kurią vienaip ar kitaip paveikiant nusikalstamu kėsinimusi, bus padaryta žala tos informacijos savininkui, valdytojui ar teisėtam naudotojui. Kompiuterinės informacijos savininku, valdytoju ar naudotoju gali būti valstybė, juridinis ar fizinis asmuo. Tokios kompiuterinės informacijos apsaugos lygis ir rėžimas yra nustatomas atskirais Lietuvos Respublikos teisės aktais. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas nustato apsaugos lygį ir rėžimą informacijai, kuri sudaro valstybės ar tarnybos paslaptį ir kurios savininkas yra valstybė. Šiame įstatyme valstybės paslaptis apibrėžiama kaip įstatymo nustatyta tvarka įslaptinta politinė, karinė, žvalgybos, kontržvalgybos, teisėsaugos, mokslo ir technikos informacija, kurios praradimas arba neteisėtas atskleidimas gali sukelti grėsmę Lietuvos Respublikos suverenitetui, teritorijos vientisumui, gynybinei galiai, padaryti žalos valstybės interesams, sukelti pavojų žmogaus gyvybei. Tarnybos paslaptis – tai įstatymo nustatyta tvarka įslaptinta politinė, karinė, ekonominė, teisėsaugos, mokslo ir technikos informacija, kurios praradimas arba neteisėtas atskleidimas gali pakenkti valstybės ar jos institucijų interesams arba sudaryti prielaidas neteisėtam valstybės paslaptį sudarančios informacijos atskleidimui, sukelti pavojų žmogaus sveikatai. Taip pat, Įstatymas pateikia išsamų sąrašą duomenų, kurie gali sudaryti valstybės ar tarnybos paslaptį.[28]

Kompiuterinę informaciją, kurios savininkas yra juridinis asmuo ir kurios apsaugos režimus nustato Lietuvos Respublikos civilinis bei baudžiamasis kodeksai, dažniausiai sudaro komercinę (gamybinę) ir profesinę paslaptis. Lietuvos Respublikos civilinis kodeksas pripažindamas informaciją civilinių teisių objektu, kartu nustato ir teisinę apsaugą komercinei (gamybinei) ar profesinei paslaptimis. Informacija laikoma komercine (gamybine) paslaptimi,

---

[27] Lietuvos Respublikos elektroninio parašo įstatymas // http://www3.lrs.lt/cgi-bin/preps2?Condition1=169880&Condition2=, (prisijungimo laikas: 2005-11-09).
[28] Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas // http://www3.lrs.lt/cgi-bin/preps2?Condition1=238376&Condition2= , (prisijungimo laikas: 2005-11-09).

jeigu turi tikrą ar potencialią komercinę (gamybinę) vertę dėl to, kad jos nežino tretieji asmenys ir ji negali būti laisvai prieinama dėl šios informacijos savininko ar kito asmens, kuriam savininkas ją yra patikėjęs, protingų pastangų išsaugoti jos slaptumą.[29] Komercine paslaptimi gali būti:

- technologinės paslaptys – visos technologinės naujienos (duomenų apdorojimo būdai ir pan.), ruošiamos įdiegti ar jau įdiegtos įmonės paslaugų teikimo metu atliekamų tyrimų rezultatai;
- įmonės sudarytos sutartys ar susitarimai su klientais: duomenys apie klientus (jų pavadinimas, adresas ir kita klientą leidžianti atpažinti informacija), sutarčių ir susitarimų objektas, atsiskaitymo tvarka ir kita informacija, kuri pagal įmonės sudarytas sutartis ar susitarimus yra laikoma konfidencialia;
- informacija apie klientus, kurios viešas atskleidimas padarytų įmonei turtinę ir (ar) neturtinę žalą;
- informacija apie įmonės materialaus ir finansinio turto investicijas;
- informacija apie įmonės darbuotojų darbo užmokestį, jo mokėjimo būdus ir tvarką.

Informacija pripažįstama profesine paslaptimi, jei ją pagal įstatymus ar sutartį privalo saugoti tam tikros profesijos asmenys (advokatai, gydytojai, auditoriai ir kt.).[30]

Atskirai reikėtų paminėti informaciją, kuri sudaro bankų paslaptį. Lietuvos Respublikos bankų įstatymas nustato, kad banko paslaptimi laikomi visi bankui žinomi duomenys ir informacija apie:

- banko kliento turimas banke sąskaitas, lėšų likučius šiose sąskaitose, kliento vykdomas operacijas su jo sąskaitoje esančiomis lėšomis, sutarčių, pagal kurias klientui buvo atidarytos sąskaitos, sąlygas;
- banko kliento skolinius įsipareigojimus bankui, sutarčių, pagal kurias atsirado šie skoliniai įsipareigojimai, sąlygas;
- kitas banko klientui suteiktas finansines paslaugas, sutarčių, pagal kurias teikiamos finansinės paslaugos, sąlygas;
- banko kliento finansinę būklę ir turtą, veiklą, veiklos planus, skolinius įsipareigojimus kitiems asmenims ar sandorius su kitais asmenimis, kliento komercines (gamybines) ar profesines paslaptis.[31]

Kompiuterinę informaciją, kurią sudaro fizinių asmenų asmeniniai duomenys, visų pirma gina Lietuvos Respublikos Konstitucija. Jos 22 straipsnis nustato, kad „žmogaus privatus

[29] Lietuvos Respublikos civilinis kodeksas // Valstybės žinios. 2000, Nr. 74-2262.
[30] ten pat.
[31] Lietuvos Respublikos bankų įstatymas.// http://www3.lrs.lt/cgi-bin/preps2?Condition1=259449&Condition2=, (prisijungimo laikas: 2005-11-09).

gyvenimas neliečiamas. Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami.“ Lietuvos respublikos asmens duomenų teisinės apsaugos įstatymo 2 straipsnis nustato, kad asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai. Įstatymas, taip pat pateikia ir ypatingų asmens duomenų apibrėžimą - duomenys, susiję su fizinio asmens rasine ar etnine kilme, politiniais, religiniais, filosofiniais ar kitais įsitikinimais, naryste profesinėse sąjungose, sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą.[32]

Pažymėtina, kad nusikaltimų informatikai dalyku taip pat gali būti kompiuteris, kompiuterių sistema ar jų tinklas. Tik reikia atkreipti dėmesį į keletą šios situacijos momentų. Jeigu nusikalstama veika yra kėsinamasi į kompiuterį, jų sistemą arba kompiuterių tinklą kaip į aparatinę struktūrą ir materialų daiktą, pavyzdžiui vagystės atveju arba turto sugadinimo atvejais, tai tokia veika turi būti kvalifikuojama pagal atitinkamą Baudžiamojo kodekso straipsnį, numatantį atsakomybę už konkrečią nusikalstamą veiką nusikaltimų nuosavybei, turtinėms teisėms ir turtiniams interesams. Tai nulemia požymiai apibūdinantys kompiuterį kaip materialaus pasaulio objektą – daiktą, turintį savo materialinę vertę – kainą ir esantį svetimu kaltininkui, ir turintį visus kitus požymius, atitinkančius nusikaltimų nuosavybei dalyką. Tačiau praktikoje gali pasitaikyti, kai piktavalis pasinaudodamas programinėmis priemonėmis gali paveikti kompiuterį ar kompiuterinį tinklą taip, kad iš esmės juose bus neįmanoma atlikti jokių informacinių procesų.

Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje nurodytos nusikalstamos veikos priskiriamos prie nesunkių. Tik nusikalstama veika, apimanti įstatymų saugomos kompiuterinės informacijos paskleidimą, paskelbimą, platinimą ar kitokį jos panaudojimą, prieš tai pasisavinus ją, aprašyta 198 straipsnio 2 dalyje yra apysunkė. Visi nusikaltimai informatikai, numatyti XXX skyriuje gali būti įvykdyti tik aktyviais kaltininko veiksmais. Kompiuterinės informacijos sunaikinimo ar pakeitimo, bei kompiuterinės programos sunaikinimo ar pakeitimo ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymo atvejais nusikalstama veika yra baigta tik kilus pasekmėms - didelei žalai. Tokiais atvejais reikalinga nustatyti priežastinį ryši tarp veikos ir pasekmės. Nusikalstami veiksmai. Numatyti minėtame Baudžiamojo kodekso skyriuje gali būti įvykdomi tik tyčia. Nusikaltimo subjektas – bet kuris fizinis, sukakęs 16 metų amžiaus asmuo, bei juridinis asmuo.

[32] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas.// http://www3.lrs.lt/cgi-bin/preps2?Condition1=231799&Condition2=, (prisijungimo laikas: 2005-11-09).

Apibendrinant visą tai, kas išnagrinėta aukščiau, galima teigti, kad nusikaltimų informatikai objekto nustatymas neturi vieningos nuomonės literatūroje. Vieni autoriai teigia, kad nusikaltimų informatikai objektu galima įvardinti santykius, susijusius su informacijos ir informacinių resursų saugiu kūrimu, saugojimu, naudojimu ir platinimu. Kiti teigia, kad dviejų nuomonių dėl objekto būti negali, teigdami, kad nusikaltimo objektas yra informacija. Tačiau atsižvelgiant į pateiktus argumentus galima teigti, kad nusikaltimų informatikai objektu galima įvardinti visuomeninius santykius, susijusius su kompiuterinės informacijos saugumu.

Kitas nusikaltimų informatikai sampratos požymis – nusikaltimo dalykas taip pat neišvengė prieštaravimų. Rusijos, Ukrainos, taip pat ir Lietuvos teisėje nusistovėjęs požiūris, kad nusikaltimų informatikai dalykas yra kompiuterinė informacija – bet kokia informacija, kuri yra elektroniniame pavidale, esanti kompiuteryje ar kompiuterinėje laikmenoje ir kurią galima sukurti, pakeisti ar panaudoti kompiuterio pagalba. Tačiau informacija gaunama apdorojant duomenis, o paveikiant duomenis, ne visada yra paveikiama informacija. Dėl to Konvencija dėl elektroninių nusikaltimų pagrindiniu nusikaltimo dalyku įvardina kompiuterinius duomenis, kaip bet kokių faktų, informacijos arba sąvokų pateikimą tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat programą, pagal kurią kompiuterinė sistema gali vykdyti tam tikrą funkciją.

Nusikaltimai informatikai yra nesunkūs nusikaltimai ir įvykdomi tik tyčiniais veiksmais. Nusikaltimų informatikai subjektas gali būti tiek fizinis tiek ir juridinis asmuo.

1.2 vyraujančios informatikos nusikaltimų ir analogiškų nusikaltimų sampratos teisinėje literatūroje: lyginamoji analizė

Vyraujančiomis nusikaltimų informatikai sampratomis, kurios yra nagrinėjamos teisinėje literatūroje, reikėtų vadinti tik su tam tikra išlyga. Nėra įmanoma kategoriškai teigti, kad samprata, pateikiama Rusijos teisinėje literatūroje yra daugiau vyraujanti (daugiau paplitusi), negu samprata analizuojama JAV, Anglijos ar kitos šalies teisinėje literatūroje. Pirmiausia, vyravimą mes turėtume tapatinti su šalies teisinės sistemos ir teisinės kultūros kūrėjų apsisprendimu priimti vieną ar kitą informatikos nusikaltimų sampratą. Kitais žodžiais tariant, sampratos vyravimas priklauso nuo nacionalinės teisės kūrėjų pasirinkto kelio, nuo nuostatų, įtvirtintų nacionaliniuose teisės aktuose. Tačiau nūdienos realijos rodo, kad dauguma šalių įtvirtindamos vienas ar kitas teisines nuostatas nacionaliniuose teisės aktuose, stengiasi pasiekti teisinio vienodumo su kitomis šalimis. Tiksliau sakant, priimant nacionalinius teisės aktus – nagrinėjamu atveju susijusius su nusikaltimų informatikai reglamentavimu, - yra ratifikuojamos konvencijos. 2001 metų lapkričio 23 dieną Europos Taryba priėmė Konvenciją dėl elektroninių nusikaltimų, kurios vienas iš tikslų bendros baudžiamosios politikos formavimas priimant nacionalinius teisės aktus.[33] Todėl noriu dar kartą pabrėžti, kad nusikaltimų informatikai sampratos vyravimas yra sąlyginis dalykas.

Pažymėtina, kad nagrinėjant teisinę literatūrą retai sutinkamas terminas nusikaltimai informatikai. Dažniausiai sutinkami terminai, apibūdinantys mūsų nagrinėjamų nusikaltimų rūšį yra šie: kompiuteriniai nusikaltimai, elektroniniai nusikaltimai, nusikaltimai elektroninėje erdvėje, nusikaltimai aukštųjų technologijų srityje ir panašiai. Tokia terminijos įvairovė neretai įneša nemažą sumaištį atskiriant naujai atsiradusius (palyginti su tradicinių nusikaltimų amžiumi, keli dešimtmečiai kompiuterinių nusikaltimų gyvavimo leidžia juos priskirti prie naujai atsiradusių) nusikaltimus, nuo šiek tiek pakitusių tradicinių nusikaltimų. Nusikaltimai, numatyti Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje „Nusikaltimai informatikai“, Rusijos Federacijos baudžiamojo kodekso 28 skirsnyje „Nusikaltimai kompiuterinės informacijos sferoje“, Ukrainos baudžiamajame kodekse – „Nusikaltimai panaudojant elektronines skaičiavimo mašinas“ ir kitų šalių baudžiamuosiuose kodeksuose ar baudžiamuosiuose įstatymuose yra vadinami paprastu ir apibendrintu terminu – kompiuteriniai nusikaltimai. Dėl to, nenorėdamas įvesti didelės sumaišties, tik šioje darbo dalyje nusikaltimams, numatytiems LR baudžiamojo kodekso XXX skyriuje, įvardinti naudosiu terminą kompiuteriniai nusikaltimai.

[33] Konvencija dėl elektroninių nusikaltimų // Valstybės žinios.2004, Nr. 36-1188.

Prasitarsiu, kad visi nusikaltimai informatikai yra kompiuteriniai nusikaltimai, tačiau ne visi kompiuteriniai nusikaltimai gali būti priskirti prie nusikaltimų informatikai rūšies. Bet apie viską iš eilės.

Norėčiau pabrėžti, kad analogiškų nusikaltimų „analogiškumas“ šioje darbo dalyje turėtų būti suprantamas kaip įrankių, priemonių ir būdų nusikaltimo padarymui panašumas, kai kuriais atvejais – vienodumas.

Istorine prasme svarbu paminėti, kad vienas iš pirmųjų bandymų pateikti kompiuterinių nusikaltimų sampratą tarptautiniu mastu buvo dar 1983 metais. Ekonominio bendradarbiavimo ir vystymo organizacija (OECD), sudarė grupę ekspertų, kurie apibrėžė kompiuterinį nusikaltimą kaip bet kokį neteisėtą, neetišką ar nesankcionuotą elgesį, susijusį su automatiniu duomenų kompiuterinėje formoje apdorojimu ir siuntimu.[34] Pateikę šią kompiuterinio nusikaltimo sampratą OECD ekspertai kartu pabandė išskirti tokio elgesio objektą. Šioje definicijoje galima įžvelgti, kad tokio elgesio objektas yra visuomeniniai santykiai susiję su automatiniais kompiuterinės informacijos procesais. Tačiau negalime nepastebėti ir šios sampratos trūkumų. Esminis trūkumas yra tas, kad joje „nepaminėta, kokios teisės šakos atžvilgiu toks elgesys yra neteisėtas“.[35] Nepaisant to, ši kompiuterinio nusikaltimo samprata davė pradžią tolimesniems teisiniams tyrimams.

Negaliu nepaminėti ir Jungtinių Valstijų Teisingumo departamento pateiktos kompiuterinių nusikaltimų sampratos: kompiuteriniai nusikaltimai – bet koks baudžiamosios teisės pažeidimas, kurio įvykdymui ar tyrimui panaudojamos kompiuterinių technologijų žinios. Plačiai kritikuojama samprata. Remiantis tokia logika visi nusikaltimai, numatyti Baudžiamajame kodekse galėtų būti priskirti prie kompiuterinių nusikaltimų. Tirdamas bet kokius Baudžiamajame kodekse įvardintus nusikaltimus, tyrėjas gali panaudoti savo turimas kompiuterines žinias. Pavyzdžiui, tyrėjas liudininko pagalba sudarinėja kompiuterinį nusikaltėlio robotą, ekspertas atlieka lyginamąją balistinę ekspertizę. Išvardintais atvejais visuomet bus pasinaudota turimomis kompiuterinių technologijų žiniomis. Tokia minčių eiga, kokia išreiškiama aukščiau minėtu apibrėžimu, autoriaus manymu, nėra priimtina.

Dabartinėje teisinėje literatūroje plačiai aptarinėjamos, nagrinėjamos, analizuojamos visuomenei pavojingos veikos, pavadintos terminu kompiuteriniai nusikaltimai, savo esme yra labai įvairiapusiškos. Todėl yra susidariusios dvi teisinės minties kryptys, kurios kompiuterinius nusikaltimus dalina į dvi dideles kategorijas. Pirmai kategorijai priskiriami tie nusikalstami veiksmai, kuriais kėsinamasi arba yra susiję su neteisėtu įsikišimu į kompiuterio, kompiuterinės sistemos ar kompiuterinio tinklo darbą ir kai nusikalstamo kėsinimosi dalykas yra kompiuterinė

[34] Sieber U. Legal aspects of computer-related crime in the information society – comcrime study -// 1998. P.34, galima rasti adresu http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc (prisijungimo laikas: 2005-09-10).
[35] Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. - Vilnius: LTU, 2000. P.6.

informacija. Šią nusikaltimų grupę atitinka nusikaltimai informatikai. Antrai kategorijai priskiriami nusikaltimai, kuriuose kompiuteris yra nusikaltimo objektas arba panaudojamas kaip būtina techninė priemonė kitų nusikaltimų padarymui. Tokiu būdu yra išskiriamos kompiuterinių nusikaltimų sampratos siaurąją ir plačiąja prasmėmis.

Rusijos teisininkas V.B. Vechovas nagrinėdamas kompiuterinių nusikaltimų fenomeną, savo darbuose pateikia dvi jų sampratas – vieną baudžiamosios teisės požiūriu, kitą kriminalistikos mokslo požiūriu. Remiantis pirmąja jo pateikta samprata, kompiuteriniai nusikaltimai – tai baudžiamojo įstatymo numatytos visuomenei pavojingos veikos, kai mašininė informacija yra nusikalstamos veikos objektas.[36] Atrodo viskas paprasta, patogu ir aišku. Duotu apibrėžimu būtų galima lengvai apibūdinti nusikaltimus informatikai. Tačiau atidžiau panagrinėjus šį jo teiginį, kyla šiokių tokių prieštaravimų. Visų pirma, prie tokių nusikalstamų veikų, kuriomis yra kėsinamasi į kompiuterinę informaciją kaip teisinį gėrį galima būtų priskirti ir tokias veikas, kaip sukčiavimas su magnetinėmis mokėjimo kortelėmis ir panašias veikas. Antra, kaip jau buvo minėta prieš tai nagrinėtame skyriuje, nusikaltimo objektas nusikalstamo kėsinimosi metu visuomet yra pažeidžiamas, patiria žalą. Priešingu atveju, kai objektas veikiamas tam tikrų piktybiškų veiksmų nepatiria jokios žalos, tai yra jis nėra kaip nors žalingai pakeičiamas, tai ir kalbos apie baudžiamąją atsakomybę už tą veiką negali būti. Kompiuterinė informacija (mašininė informacija – pagal V.B. Vechov) pasižymi tokiomis savo savybėmis, kad, pavyzdžiui, jos pasisavinimo (kopijavimo) ar pašalinimo atveju pati kompiuterinė informacija nėra pažeidžiama, jos pradinė struktūra gali išlikti nepakitusi. Vienintelis dalykas kuris keičiasi informacijos pašalinimo atveju tai jos buvimo vieta. O kopijavimo atveju viskas dar paprasčiau. Kompiuterinės informacijos originalas lieka pas nukentėjusįjį, o asmuo savo neteisėtais veiksmais įgyja tik tos informacijos kopiją. Dėl to, kaip matome, kompiuterinė informacija ne visuomet gali atitikti nusikalstamo kėsinimosi objekto reikalavimus, dėl ko kompiuterinės informacijos įvardinimas kaip nusikaltimų informatikai objektu neatskleidžia šios nusikaltimų rūšies ypatumų.

Gerai teisininkams, nagrinėjantiems kompiuterinių nusikaltimų problematiką, žinoma, daugelyje straipsnių cituojama V.S. Komisarovo pateikta kompiuterinių nusikaltimų samprata. Jis teigia, kad „nusikaltimus kompiuterinės informacijos srityje galima apibrėžti kaip tyčines visuomenei pavojingas veikas (veikimą ar neveikimą), darančias žalą arba sukeliančias tokios žalos atsiradimo grėsmę visuomeniniams santykiams, reglamentuojantiems saugų informacijos ar informacinių resursų kūrimą, naudojimą, platinimą arba jų saugumą“.[37] Tačiau ir ši

[36] Вехов В.Б. Компьютерные преступления: способы совершения, методика расследования // Москва: Право и закон, 1996. P.23.
[37] Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность //Юридический мир, Февраль 1998. P.13.

kompiuterinių nusikaltimų samprata neišvengė kritikos. V.S. Komisarovas savo pateiktoje sampratoje mini *„visuomeninius santykius, reglamentuojančius saugų informacijos ar informacinių resursų kūrimą, naudojimą, platinimą arba jų saugumą“*. M.V. Bogomolovas teigia, kad dažniausiai tokie visuomeniniai santykiai yra suprantami kaip normatyviniai aktai arba naudojimosi taisyklės, tai yra neteisėtai kopijuojant informaciją kenčia santykiai tarp teisėto savininko ir valstybės, kuri normatyvinių teisės aktų pagalba reglamentuoja jam monopolinį informacijos panaudojimą.[38]

Autoriaus nuomone, priimtiną kompiuterinių nusikaltimų sampratą, atitinkančią nagrinėjamą temą, pateikia N.V. Karčevskij. Jis teigia, kad kompiuterinius nusikaltimus būtų galima apibūdinti taip: „visuomenei pavojingos, kaltos, neteisėtos, baudžiamosios veikos, kurios daro žalą informaciniams santykiams, kurių užtikrinimo priemonės yra elektroninės skaičiavimo mašinos, sistemos arba kompiuteriniai tinklai.“[39]

Pažinimo tikslais verta paminėti tai, kad kai kurie teisininkai iš viso norėtų atsisakyti termino „kompiuteriniai nusikaltimai“, argumentuodami, kad teisine prasme šis terminas yra stipriai pažeidžiamas. Tokios teisinės minties laikosi V.V. Krylovas. Vietoje termino „kompiuteriniai nusikaltimai“ siūlydamas naudoti terminą „informaciniai nusikaltimai“. Tokia V.V. Krylovo nuomonė reikalauja tam tikro paaiškinimo. Jo teigimu informaciniai nusikaltimai apima daug platesnį nusikalstamų veikų ratą, negu numatytieji Rusijos Federacijos baudžiamojo kodekso 28 skirsnyje. V.V. Krylovo manymu, šiuos nusikaltimus į atskirą skirsnį leido išskirti tik jų kompiuterinis aspektas ir nusikalstamo kėsinimosi dalykas – informacija kompiuterinėje (skaitmeninėje) formoje. Jis teigia, kad „informaciniai nusikaltimai – visuomenei pavojingos veikos, įvykdytos informacinių teisinių santykių srityje ir uždraustos baudžiamojo įstatymo grasinant bausmėmis“. [40] V.V. Krylovo nuomonei pritaria ir V.A. Parchomovas, teigdamas, kad yra teisinga traktuoti kompiuterinius nusikaltimus kaip baudžiamajame įstatyme numatytas visuomenei pavojingas veikas, kuriose nusikaltimo dalykas yra informacija kompiuterinėse laikmenose. Tokių nusikalstamų veikų, kai neteisėtai yra naudojama kompiuterinė informacija pasekmės gali būti labai įvairios, pradedant nuo neteisėtos prieigos prie kompiuterinės informacijos, intelektinės nuosavybės pažeidimų, jautrių duomenų apie asmenis paviešinimu, komercinės, valstybinės paslapties paviešinimu ir baigiant įmonės reputacijos praradimu ir panašių pasekmių. Tačiau čia pat jis pažymi, kad tokios pat pasekmės gali kilti ir tada, kai

[38] Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации. // http://pu.boom.ru/book/index.html (prisijungimo laikas: 2006-11-10).
[39] Карчевский Н.В. Компьютерные преступления: определение, объект и предмет // Доклад на V Международной конференции «Право и интернет: теория и практика» http://www.ifap.ru/pi/05/karchev.htm (prisijungimo laikas: 2006-10-15).
[40] Крылов В.В. Расследование преступлений в сфере информации. – Москва: Издательство «Городец», 1998. P.164.

informacija yra kitokioje, nekompiuterinėje laikmenoje. Dėl to jis siūlo kalbant apie kompiuterinius nusikaltimus naudoti terminą „informaciniai nusikaltimai“. [41]

Kompiuterinių nusikaltimų sampratą siaurąja prasme pateikia JAV teisinės sistemos atstovas M. Goodman[42], kuris savo pranešime teigia, kad tradiciškai, visas kompiuterinis saugumas turi būti nukreiptas į informacinių sistemų konfidencialumo (angl. - *confidentiality*), vientisumo (angl. - *integrity*) ir prieinamumo (angl. – *availability*) apsaugos užtikrinimą. Konfidencialumas kompiuterinėse sistemose užkerta kelią informacijos atskleidimui neįgaliotiems asmenims. Asmuo, kuris įsilaužia į kito asmens kompiuterinę sistemą arba viršija savo įgaliojimus prieiti prie tam tikros informacijos, pažeidžia savininko teisėtą teisę laikyti savo asmeninę informaciją paslaptyje. Informacijos elektroniniame pavidale vientisumas garantuoja, kad niekas, neturėdamas tam teisės nepakeitė jos turinio. Tokiu būdu, neteisėtas iškraipymas, sugadinimas ar pakeitimas kompiuterinės informacijos yra priskiriamas kaip nusikaltimas prieš tokios informacijos vientisumą. Kompiuterinių duomenų prieinamumas reiškia tai, kad informacija išlieka prieinama, o su ja susijusios kompiuterinės programos išlieka funkcionalios tuomet, kai to reikia teisėtam tokios informacijos vartotojui. Dažniausiai tokie nusikaltimai yra įvykdomi panaudojant DDoS (angl.- denial of service) atakas. M. Goodman teigia, kad šie nusikaltimai kartu paėmus sudaro taip vadinamus „pure-play“ kompiuterinius nusikaltimus. Šį savo teiginį jis grindžia tuo, kad minėti kompiuteriniai nusikaltimai yra tiesiogiai nukreipti prieš kompiuterines sistemas. Tokį traktavimą mes sutinkame ir Europos Sąjungos teisinėje bazėje. 2001 m. lapkričio 23 d. Europos Tarybos priimtos Konvencijos dėl elektroninių nusikaltimų II skyriaus 1 skirsnio 1 dalyje yra numatytos kriminalizuotinos baudžiamosios veikos, kuriomis kėsinamasi į kompiuterinių duomenų ir sistemų konfidencialumą, vientisumą ir prieinamumą: neteisėta prieiga, neteisėta perimtis, poveikis duomenims ir netinkamas įtaisų naudojimas.

Kad suprastume kompiuterinių nusikaltimų sampratų įvairovę, pagrindinius skirtumus ir panašumus, panagrinėkime kompiuterinių nusikaltimų sampratą plačiąja prasme.

1993 metais Rusijos Federacijoje pastoviai veikiančiame tarpžinybiniame seminare „Kriminalistika ir kompiuterinis nusikalstamumas“, kurį organizavo kriminalistikos koordinacinis biuras prie Rusijos Federacijos Generalinės prokuratūros teisėtumo ir teisėtvarkos stiprinimo problemų mokslinio-tiriamojo instituto ir Rusijos VRM Ekspertinio – kriminalistinio centro, buvo pamėginta suformuluoti kompiuterinių nusikaltimų sampratą. Šiame seminare buvo prieita prie išvados, kad kompiuteriniai nusikaltimai – tai baudžiamojo įstatymo numatytos visuomenei pavojingos veikos, kuriose mašininė informacija yra arba priemonė arba

[41] Пархомов В.А. К определению понятия "Информационное преступление" // Вестник ИГЭА, 2001. № 2. http://www.etasu.isea.ru/attorn/s5.htm (prisijungimo laikas: 2005-09-05).
[42] Goodman M. Making computer crime count // FBI Law Enforcement Bulletin,The:. 2001. http://www.findarticles.com/p/articles/mi_m2194/is_8_70/ai_78413303 (prisijungimo laikas: 2005-10-25).

nusikalstamo kėsinimosi objektas.[43] Toks požiūris gerokai išplečia kompiuterinių nusikaltimų sampratos ribas, apimdamas ne tik mūsų nagrinėjamus kompiuterinius nusikaltimus, numatytus LR BK XXX skyriuje „Nusikaltimai informatikai“, bet ir kituose skyriuose aprašytas nusikalstamas veikas. Kompiuterinės informacijos kaip priemonės nusikalstamai veiklai padaryt panaudojimo klausimas turi pagrindo diskusijai. Kompiuterinę informaciją traktuojant kaip priemonę reikia prisiminti, kad ji negali pati viena tvyroti ore, tai yra kompiuterinė informacija yra neatsiejama nuo kompiuterio kaip aparatinės struktūros ir veikia ji sąveikoje su kompiuterine technika. Todėl tiek technine tiek ir teisine prasme kompiuterinė informacija priemone nusikalstamai veikai padaryti gali būti traktuojama tik sąveikoje su kompiuterine technika kaip vieninga struktūra. Dėl kompiuterinės informacijos kaip nusikalstamo kėsinimosi objekto kartotis nėra prasmės, nes autoriaus jau buvo nagrinėta aukščiau ir prieita prie išvados, kad kompiuterinė informacija negali būti nusikalstamo kėsinimosi objektu. N.V. Karčevskij taip pat pažymi, kad dažnai mokslinėje literatūroje kompiuterinis nusikaltimas traktuojamas pakankamai plačiai ir suprantamas kaip nusikaltimas, kurį darant kompiuterinė technika, informacija arba elektroninis informacijos apdorojimas gali būti tiek nusikaltimo padarymo įrankiais, tiek ir nusikalstamos veikos dalykais. Kartu jis pažymi, kad toks traktavimas negali būti teisingas, nes tokia kompiuterinių nusikaltimų samprata prie kompiuterinių gali priskirti beveik kiekvieną nusikaltimą, kurį darant buvo naudojamas kompiuteris.[44] Tokios sampratos pavyzdį galime rasti antroje V.B. Vechovo pateiktoje kompiuterinių nusikaltimų sampratoje, tačiau jau visai kitos mokslo šakos požiūriu – kriminalistikos mokslo požiūriu. Jis teigia, kad kompiuteriniai nusikaltimai kriminalistikos požiūriu – tai baudžiamojo įstatymo numatytos visuomenei pavojingos veikos, padarytos panaudojant elektroninę skaičiavimo (kompiuterinę) techniką.[45] Pateikdamas tokią kompiuterinių nusikaltimų sampratą V.B. Vechovas kartu nustato ir kvalifikacinį požymį, leidžiantį priskirti nusikaltimus kompiuterinių rūšiai – tai kompiuterinės technikos panaudojimas nepriklausomai kokioje nusikaltimo stadijoje ji buvo panaudota. Šioje situacijoje kompiuterinė technika (kompiuteris) yra panaudojama kaip nusikaltimo įvykdymo priemonė arba viena iš priemonių. Kompiuteris kaip nusikalstamos veiklos priemonė gali būti panaudotas darant neteisėtas veikas, nukreiptas prieš informacinių visuomeninių santykių saugumą, tai yra darant nusikaltimus informatikai. Tada kyla klausimas, kuom skiriasi V.B. Vechovo pateiktos kompiuterinių nusikaltimų sampratos. Priešpastačius vieną kompiuterinių

[43] Вехов В.Б. Компьютерные преступления: способы совершения, методика расследования. - Москва: Право и закон, 1996.P.24.
[44] Карчевский Н.В. Компьютерные преступления: определение, объект и предмет // Доклад на V Международной конференции «Право и интернет: теория и практика» http://www.ifap.ru/pi/05/karchev.htm (prisijungimo laikas: 2006-10-15).
[45] Вехов В.Б. Компьютерные преступления: способы совершения, методика расследования. - Москва: Право и закон, 1996. P.24.

nusikaltimų sampratą priešais kitą nesunkiai galima padaryti išvadą, kad pirmąja samprata jis bandė apibūdinti šiame darbe nagrinėjamas nusikalstamas veikas, tai yra nusikaltimus informatikai. Antrąja kompiuterinių nusikaltimų samprata V.B. Vechovas pabrėžia, kad tai „*baudžiamojo įstatymo numatytos visuomenei pavojingos veikos"*, tačiau konkrečiai neįvardina jų. Dėl ko darytina išvada, kad tai gali būti bet kurios baudžiamosios veikos, taip pat ir atskirame skyriuje numatyti nusikaltimai informatikai, į kurias kėsinantis yra panaudojama kompiuterinė technika. Tiksliau tariant, kai kompiuteris yra priemonė padaryti nusikalstamą veiką, nusikaltimo objektas gali būti tiek saugomas, pavyzdžiui, LR Baudžiamojo kodekso XXX skyrium „Nusikaltimai informatikai", tiek ir kitais skyriais. Kaip buvo minėta, toks požiūris labai išplečia kompiuterinių nusikaltimų sampratą. Nagrinėdamas užsienio (neįskaitant Rusijos ar Ukrainos) teisinę literatūrą aš padariau išvadą, kad dažniausiai nagrinėjant kompiuterinius nusikaltimus yra remiamasi būtent tokiu plačiu požiūriu. Nors dar 1983 metas Donas Parkeris (Donn Parker) kompiuterinius nusikaltimus apibūdino kaip nusikalstamas veikas, kurioms sėkmingai įvykdyti reikalingos kompiuterinės žinios. O Marko D. Rašo (Mark D. Rasch) nuomone tokia kompiuterinių nusikaltimų samprata leidžia atskirti tikrus kompiuterinius nusikaltimus nuo su kompiuteriais susijusių nusikaltimų, kuriuose kompiuteris yra naudojamas kaip priemonė arba yra nusikaltimo objektas, bet kuriems sėkmingai įvykdyti nėra būtinos kompiuterinės žinios.[46] Tačiau, kaip minėjau, daugiausia sutinkamas platesnis požiūris į kompiuterinių nusikaltimų sampratą. Australijos kriminologijos instituto daktaras Toni Kronas (Tony Krone) savo tyrime nurodo, kad kompiuterinis nusikaltimas yra tik bendrinis nusikaltimų apibūdinimas kai kompiuteris yra nusikaltimo objektas arba nusikaltimo įvykdymo priemonė. Tačiau jis pažymi, kad yra naudojama eilė kitų teisinių terminų, kurie naudojami kaip sinonimai kalbant apie nusikalstamas veikas, kurioms įvykdyti yra naudojami kompiuteriai: tai su kompiuteriais susiję (angl. – *computer-related*) nusikaltimai, kai kompiuterio panaudojimas yra būtinas įvykdyti nusikaltimą, pavyzdžiui kompiuterinį klastojimą; interneto nusikaltimai (angl. – *internet crime*) – taip apibūdinami nusikaltimai, kai interneto panaudojimas yra pagrindinis jo bruožas ir apima tokias veikas kaip su turiniu susijusius nusikaltimus (angl. - conten–related offences). [47] Dar platesnę kompiuterinių nusikaltimų sampratą pateikia Mičigano valstijos (JAV) universiteto profesorius Davidas L. Karteris (David L. Carter) Jis pateikia kompiuterinių nusikaltimų tipologiją suskirstydamas juos į keturis tipus. D.L. Karterio kompiuterinių nusikaltimų tipologiją sudaro:

[46] Rasch M. D. Criminal law and the internet. // This is one of eleven chapters contained in The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, published by the Computer Law Association. http://www.sgrm.com/art14.htm (prisijungimo laikas: 2004-06-13).

[47] Krone T. Concepts and terms // High Tech Crime Brief. ISSN 1832-3413. 2005. http://www.aic.gov.au/publications/htcb/htcb001.html (prisijungimo laikas: 2006-09-02).

1) Kompiuteris kaip objektas (angl. - *computer as the target*). Šio tipo nusikaltimams jis priskiria tokius teisės pažeidimus kaip intelektinės nuosavybės vagystė, verslo informacijos vagystė, kompiuterinis sabotažas, kompiuterinis vandalizmas, neteisėta prieiga prie kompiuterinės informacijos ir netgi šantažą, pagrįstą informacija iš kompiuterinių failų.
2) Kompiuteris kaip nusikaltimo priemonė (angl. – *computer as the instrumentality of the crime*). Šioje kategorijoje nusikaltimams daryti yra pasitelkiami kompiuterio technologiniai procesai. Tokiems nusikaltimams priskiria sukčiavimą su mokėjimo kortelėmis, telekomunikacijų sukčiavimą, sukčiavimą su kompiuterinėmis transakcijomis.
3) Kompiuteris kaip palengvinanti kito nusikaltimo padarymo priemonė (angl. – *computer is incidental to other crime*). Šiai kategorijai D.L. Karteris (David L. Carter) priskiria nusikaltimus, kai nusikaltimo padarymui nėra būtinas kompiuteris, tačiau jo panaudojimas palengvina jo įvykdymą, pavyzdžiui, pinigų padirbinėjimas.
4) Nusikaltimai susiję su kompiuterių paplitimu (angl. – *crimes associated with the prevalence of computers*). D.L. Karteris (David L. Carter) pažymi, kad kompiuterinių technologijų paplitimas išplečia nusikalstamų veikų objektus. Šiam tipui jis priskiria tokias nusikalstamas veikas kaip kompiuterinių programų piratavimas, padirbinėjimas, autorinių teisių į kompiuterines programas pažeidimas ir net kompiuterinės įrangos klastotes.[48]

Pateikta D.L. Karterio (David L. Carter) kompiuterinių nusikaltimų samprata, autoriaus nuomone, yra nepagrįstai išplėsta. Paimkime, pavyzdžiui, trečiam tipui priskirtas nusikalstamas veikas. Aš visiškai nematau esminio skirtumo tarp to, kaip bus padirbami pinigai – ar panaudojant kompiuterį ar spaustuvines stakles. Šiuo atveju svarbus yra pinigų padirbimo faktas, bet visiškai neturi reikšmės kokiomis priemonėmis tai padaryta. Pats kompiuterio panaudojimo kaip priemonės tokioms nusikalstamoms veikoms įvykdyti faktas dar nedaro pačio nusikaltimo kompiuterinio.

Užsienio literatūroje apibūdinant mus dominančias nusikalstamas veikas taip pat dažnai naudojamas terminas *cybercrime*. Šis terminas „simbolizuoja globaliai stipriai kompiuterizuotai interneto visuomenei būdingas nusikalstamas veikas“.[49] Verčiant į lietuvių kalbą *cybercrime* – elektroninis nusikaltimas. Toks terminas yra naudojamas 2001 m. lapkričio 23 d. Europos

[48] Carter D.L. Computer crime categories: how techno-criminals operate // http://www.lectlaw.com/files/cri14.htm (prisijungimo laikas: 2006-09-22).
[49] Civilka M., Lamanauskas T., Osinaitė G. ir kt./red. D. Sauliūnas. Informacinių technologijų teisė. - Vilnius: NVO Teisės Institutas, 2004.P. 511.

Tarybos Konvencijoje dėl elektroninių nusikaltimų oficialiame vertime į lietuvių klabą. Elektroniniai nusikaltimai literatūroje suprantamai kaip žalingi veiksmai padaryti iš ar prieš kompiuterį ar kompiuterių tinklą.[50] A.G. Važeninas elektroninius nusikaltimus įvardina kaip tyčinius, kaltai padarytus veiksmus, atliekamus kompiuterinės sistemos ar tinklo pagalba, kompiuterinėje sistemoje ar tinkle, nukreiptus prieš kompiuterinių sistemų, jų tinklų ir kompiuterinių duomenų konfidencialumą, vientisumą ir prieinamumą, kurie sukelia esminius asmens, visuomenės ir valstybės teisių ir įstatymų saugomų interesų pažeidimus.[51] Iš esmės, manytina, kad elektroniniai nusikaltimai nėra atskira nusikaltimų rūšis. Į elektroninių nusikaltimų sampratą daugeliu atveju įeina tiek nusikaltimai informatikai, tiek ir kompiuteriniai nusikaltimai plačiąja prasme. Tai patvirtina ir K.A. Taipalė (K.A. Taipale). Jis teigia, kad *cybercrime* plačiai apibūdina nusikalstamas veiklas, kuriose kompiuteris ar kompiuterinis tinklas yra priemonė, objektas arba nusikalstamos veiklos vieta. Čia pat jis priduria, kad elektroninis nusikaltimas kaip terminas yra daugiau tinkamas apibūdinti tokias nusikalstamas veikas, kuriose kompiuterio ar kompiuterinio tinklo vaidmuo yra būtinas, tačiau kartais jis naudojamas apibūdinant tradicinius nusikaltimus, kuriuose kompiuteris ar kompiuterinis tinklas yra panaudojami palengvinti įvykdyti uždraustas veiklas arba kuriuose kompiuteris ar tinklas išsaugo tradicinių nusikaltimų įkalčius.[52]

2005 metais Ženevoje vykusiame WSIS (*World Summit of Informatikon Society*) teminiame susitikime dėl elektroninio saugumo teigta, kad elektroniniai nusikaltimai gali būti suprantami kaip atakos prieš kompiuterinių sistemų ir tinklų infrastruktūrą internete, įskaitant interneto klastotes ir sukčiavimus. Buvo pasiūlyta iš elektroninių nusikaltimų sampratos eliminuoti su turiniu susijusias (angl. – *content-related*) nusikalstamas veikias, nes tokios veikos, kaip autorių teisių pažeidimai, rasizmas, ksenofobija ir vaikų pornografija daugumos teisininkų nuomone nėra priskiriami prie elektroninių nusikaltimų. Autorių teisių pažeidimai pagrinde remiasi civiliniais santykiais ir daugumoje šalių nėra traktuojamos kaip nusikalstamos veikos. Autorių teisių pažeidimai labai dažnai išsprendžiami civiliniais teisiniais gynimo būdais. Vaikų pornografija visada buvo nusikalstama veika, tai yra ir iki paplintant informacinėms technologijoms.[53]

---

[50] Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Informatikon // http://www.mcconnellinternational.com/services/cybercrime.htm (prisijungimo laikas: 2005-10-10).
[51] Важенин А.Г. Интернет и преступность: криминологические и правовые аспекты взаимосвязи. // http://www.crime.vl.ru/docs/stats/stat_197.htm (prisijungimo laikas: 2006-05-30).
[52] Taipale K.A. Cybercrime, Cyberterrorism, and Digital law enforcement // http://cybercrime.advancedstudies.org (prisijungimo laikas: 2006-11-18).
[53] Schjølberg S. & Hubbard A.M. Harmonizing national legal approaches on cybercrime // WSIS thematic meeting on cybersecurity. Geneva, 28 June – 1 July, 2005.P.4. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (prisijungimo laikas: 2006-10-10).

Taigi, galima teigti, kad elektroniniai nusikaltimai yra nusikalstami veiksmai vykdomi globaliuose kompiuterių tinkluose ir pasitelkiant kompiuterius ar jų sistemas.

2001 m. lapkričio 23 d. Europos Tarybos Konvencija dėl elektroninių nusikaltimų elektroninius nusikaltimus apibrėžia 2-10 straipsniuose išskirdama juos į keturias kategorijas:

1) nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui, kurie apima tokias nusikalstamas veikas, kaip neteisėta prieiga, neteisėta perimtis, poveikis duomenims, poveikis sistemai ir netinkamas įtaisų naudojimas;

2) su kompiuteriais susiję nusikaltimai, kurie apima su kompiuteriais susijusias klastotes ir su kompiuteriais susijusį sukčiavimą;

3) turinio nusikaltimai – apima nusikaltimus, susijusius su vaikų pornografija;

4) nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais.

Apibendrinant visa kas aukščiau išdėstyta galima teigti, kad vyraujančios nusikaltimų informatikai ir analogiškų nusikaltimų sampratos yra kompiuterinių nusikaltimų sampratos siaurąja ir plačiąja prasmėmis. Pagrindinis skirtumas tarp šių sampratų yra tas, kad kompiuteriniai nusikaltimai plačiąja prasme apima didesnį ratą nusikalstamų veikų. Kompiuteriniai nusikaltimai siaurąja prasme apima tik tas baudžiamąsias veikas, kuriomis kėsinamasi į visuomeninius santykius, susijusius su kompiuterinės informacijos teisėtu apdorojimu, naudojimu ir valdymu – kompiuterinės informacijos saugumu, o nusikalstamo kėsinimosi dalykas yra pati kompiuterinė informacija, nepriklausomai kokioje kompiuterinėje laikmenoje ji yra. Į šią kompiuterinių nusikaltimų sampratą įeina tokios nusikalstamos veikos, kokios ir yra aprašytos Lietuvos Respublikos Baudžiamojo kodekso XXX skyriuje, o būtent: 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.

Kompiuterinių nusikaltimų samprata plačiąja prasme yra kur kas sudėtingesnė. Plačiąja prasme kompiuteriniams nusikaltimams yra priskiriamos tokios baudžiamosios veikos, kai kompiuteris, kompiuterinė informacija gali būti arba nusikalstamos veikos kėsinimosi dalyku arba nusikaltimo padarymo priemone, įrankiu. Kiekvienu atskiru atveju nusikalstamos veikos kėsinimosi objektas nustatomas individualiai, atsižvelgiant kokius teisinius santykius pažeidžia nusikalstama veika. Taigi, kompiuteriniai nusikaltimai plačiąja prasme apima tiek nusikaltimus siaurąja prasme, tiek ir kitas baudžiamajame įstatyme numatytas nusikalstamas veikas,

pavyzdžiui, klastotės panaudojant kompiuterius, sukčiavimas panaudojant kompiuterius ir panašios veikos.

Elektroniniai nusikaltimai iš esmės yra tie patys kompiuteriniai nusikaltimai plačiąja prasme, tik įvykdomi pasitelkiant globalią elektroninę erdvę – Internetą.

2. NUSIKALTIMŲ, NUMATYTŲ LR BAUDŽIAMOJO KODEKSO XXX SKYRIUJE ANALIZĖ NUSIKALTIMŲ INFORMATIKAI SAMPRATOS KONTEKSTE:

2.1 kompiuterinės informacijos sunaikinimas ar pakeitimas

Lietuvos Respublikos Baudžiamojo kodekso 196 straipsnio 1 dalis nustato, kad:

Tas, kas neteisėtai sunaikino, sugadino, pašalino ar pakeitė kompiuterinę informaciją arba įrenginiais ar kompiuterinėmis programomis apribojo naudojimąsi tokia informacija padarydamas didelės žalos,

baudžiamas viešaisiais darbais arba bauda, arba laisvės atėmimu iki trejų metų.

Pažinimo tikslais verta paminėti, kad dabartinė straipsnio dispozicija skiriasi nuo kodekso įsigaliojimo pradžioje buvusios redakcijos. Straipsnis buvo pakeistas ir papildytas 2004 metais, po to, kai tų pačių metų sausio 22 dieną Lietuvos Respublikos Seimas ratifikavo 2001 m. lapkričio 23 dienos Europos Tarybos narių pasirašytą Konvenciją dėl elektroninių nusikaltimų (*Convention on cybercrime*). Derinant Konvencijos reikalavimus prie Lietuvos Respublikos norminių aktų, BK 196 straipsnyje buvo padaryti pakeitimai. Konvencijos dėl elektroninių nusikaltimų 4 straipsnis nusako, kad kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterinių duomenų sugadinimą, sunaikinimą, apgadinimą, pakeitimą arba galimybės naudotis tokiais duomenimis panaikinimą.[54] Dėl to, Lietuvos Respublikos BK 196 straipsnis buvo papildytas tokiais kvalifikuojamaisiais požymiais, kaip kompiuterinės informacijos „pašalinimas“ ir „įrenginiais ar kompiuterinėmis programomis apribojo naudojimąsi tokia informacija“. Visi veiksmai, numatyti BK 196 straipsnyje tapo „netesėti“. Po metų, kai buvo padaryti minėti teisiniai pakeitimai, tai yra 2005 m. vasario 24 d. buvo priimtas Tarybos pamatinis sprendimas 2005/222/TVR, dėl atakų prieš informacines sistemas[55], kurio tikslas yra pagerinti valstybių narių teisminių ir kitų kompetentingų institucijų, įskaitant policijos ir kitas specializuotas teisėsaugos tarnybas, bendradarbiavimą derinant valstybėse narėse baudžiamosios teisės taisykles aktų prieš informacines sistemas srityje. Šiame Tarybos pamatiniame sprendime taip pat nurodoma, kad kiekviena valstybė narė imasi būtinų priemonių užtikrinti, kad už tyčinį informacinėje sistemoje esančių kompiuterinių duomenų ištrynimą, sugadinimą, pažeidimą, pakeitimą, nuslėpimą arba prieigos prie jų užkirtimą, jei tai padaryta

[54] Konvencija dėl elektroninių nusikaltimų // Valstybės žinios.2004, Nr. 36-1188.
[55] 2005 m. vasario 24 d. Tarybos pamatinis sprendimas 2005/222/TVR, dėl atakų prieš informacines sistemas // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:LT:NOT (prisijungimo laikas: 2006-08-22).

neturint tam teisės, būtų baudžiama kaip už nusikaltimą, bent tais atvejais, kurie nėra nereikšmingi.

Nusikaltimų informatikai (kompiuterinių nusikaltimų siaurąja prasme) teisinė samprata nurodo, kad nusikaltimų informatikai objektas yra visuomeniniai santykiai, susiję su kompiuterinės informacijos saugumu[56]. Kompiuterinės informacijos saugumas yra suprantamas kaip jos konfidencialumas, vientisumas ir prieinamumas. Žvelgiant iš nusikaltimų informatikai sampratos konteksto matyti, kad įstatymų leidėjas Lietuvos Respublikos Baudžiamojo kodekso 196 straipsnyje aprašydamas nusikalstamą veiką būtent ir nustato ginamuosius visuomeninius santykius, susijusius su kompiuterinės informacijos saugumu. Papildomu šio nusikaltimo objektu galima būtų įvardinti asmens nuosavybės teisė į informaciją kompiuterinėje (skaitmeninėje) formoje. Kitaip sakant, nusikalstamu kėsinimusi pažeidžiama savininko teisė valdyti, naudoti ir kitaip tvarkyti informaciją.

Straipsnyje kriminalizuojant nusikaltimą informatikai, kuriuo yra pažeidžiamas kompiuterinės informacijos vientisumas ir prieinamumas yra nustatomas ir nusikalstamo kėsinimosi dalykas – tai kompiuterinė informacija. Kaip jau buvo nagrinėta ankstesnėse darbo dalyse, kompiuterinės informacijos, kaip nusikaltimo dalyko įvardinimas ne visuomet atskleidžia nusikaltimų informatikai esmę. Nagrinėjamo straipsnio atžvilgiu kompiuterinės informacijos pakeitimas turėtų būti siejamas su duomenų pakeitimu, tačiau pakeičiant duomenis ne visuomet gali kisti pati kompiuterinė informacija. Dėl to manytina, kad įstatymų leidėjas turėtų atsižvelgti į kompiuterinės informacijos ir kompiuterinių duomenų sąveikos ypatumus.

Analizuojant straipsnio dispoziciją galima teigti, kad įstatymų leidėjo kriminalizuoti tokie nusikalstami veiksmai kaip kompiuterinės informacijos sunaikinimas, sugadinimas, pašalinimas ar pakeitimas yra nukreipti prieš kompiuterinės informacijos vientisumą. Vientisumas užtikrina tokios informacijos turinio buvimą nepakitus tol, kol jos nepakeičia teisėtas teisės į kompiuterinę informaciją turėtojas. Taigi, kompiuterinės informacijos vientisumas pažeidžiamas ją sunaikinant. Iš esmės, sunaikinimo samprata teisinėje literatūroje nesukelia didelių problemų. V.V. Krylov informacijos sunaikinimą supranta, kaip fiziškai visišką informacijos panaikinimą arba panaikinimą tokių jos elementų, kurie paveikia esminius informaciją individualizuojančius požymius.[57] V. Golubev teigia, kad kompiuterinės informacijos sunaikinimas yra jos praradimas, kada informacija elektroninių skaičiavimo mašinų (kompiuterių), sistemų ar kompiuterinių tinklų sferoje nustoja egzistuoti fiziniams ir juridiniams

[56] Civilka M., Lamanauskas T., Osinaitė G. ir kt./red. Sauliūnas D. Informacinių technologijų teisė. - Vilnius: NVO Teisės Institutas, 2004.P.529.
[57] Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. // Уголовное право, 1998. - №3. – P.83.

asmenims, kurie turi visiškas arba apribotas informacijos savininko teises.[58] Pirmiausia, kompiuterinės informacijos sunaikinimą reikėtų suprasti kaip jos ištrynimą iš kompiuterio atminties arba iš bet kokios kitos išorinės kompiuterinės informacijos laikmenos, kurią paveikiant programiniais būdais yra įmanoma ištrinti (pvz. iš išorinio standžiojo disko). Manytina, kad tais atvejais, kai kompiuterinės laikmenos, kurioje yra įrašyta (saugoma) kompiuterinė informacija, negalima paveikti programinėmis priemonėmis (akivaizdus pavyzdys yra vienkartinio įrašymo optinė duomenų laikmena), kompiuterinės informacijos sunaikinimas pasireiškia pačios laikmenos padarymu netinkama naudoti – sulaužoma, sudeginama ir pan. (tada nusikalstama veika gali būti papildomai kvalifikuojama pagal atitinkama BK straipsnį, numatantį atsakomybę už nusikaltimus nuosavybei).

Probleminis klausimas gali iškilti dėl kompiuterinės informacijos *visiško* ištrynimo. Kaip žinia, kompiuterio atmintyje esanti informacija įvykdant trynimo operaciją nėra negrįžtamai ištrinama iš atminties netgi tada, kai informacija ištrinama iš, taip vadinamos, šiukšlinės – vietos, kur laikinai padedami pašalinti objektai. Operacinė sistema tik pažymi failų sistemos lentelėje, kad ištrinto failo rodyti nereikia, o į jo vietą galima įrašyti kitą informaciją. Dėl to egzistuoja galimybė ją atstatyti pasitelkiant tam skirtas kompiuterines programas. Tačiau, autoriaus nuomone, galimybė atstatyti ištrintą informaciją neturėtų kaip nors įtakoti nusikaltimo kvalifikavimo, kadangi informacijos atstatymui gali būti panaudotos nemažos laiko ir kompiuterių specialistų darbo sąnaudos.

Nusikalstama veika kėsinantis į kompiuterinę informaciją sugadinant ją, ta informacija yra paveikiama taip, kad jokia kompiuterine programa negalima atvaizduoti jos turinio. Kitaip sakant, rinkmenos turinys negali būti perskaitomas, atvaizduojamas, išvedamas į vaizduoklio ekraną, dėl ko informacijos savininkas nebetenka galimybės ja naudotis, disponuoti ar kitaip ją valdyti. Menkiausia galimybė atstatyti rinkmenos turinį panaudojant kompiuterinio programavimo žinias nusikaltimo kvalifikavimui įtakos neturi.

Remiantis dabartinės lietuvių kalbos žodynu[59], žodis *pašalinti* – tai padaryti, kad nebebūtų. Tokiu būdu, kompiuterinė informacija šalinant ją iš saugojimo vietos yra perkeliama į kitą kompiuterinę sistemą, kitą kompiuterinę duomenų laikmeną ištrinant iš pirminės buvimo vietos. Vaizdžiai tariant, rinkmenų tvarkymo programose atitinka komandą *move* (perkelti).

[58] Голубев В. Уголовно-правовые аспекты противодействия преступности в сфере использования электронно-вычислительных машин // http://www.crime-research.ru/library/Golubev1003.html (prisijungimo laikas: 2006-11-08).
[59] Dabartinės lietuvių kalbos žodynas. Interneto versija // http://www.autoinfa.lt/webdic/ (prisijungimo laikas: 2006-11-02).

V. Golubevas mano, kad kompiuterinės informacijos pakeitimas taip pat apima ir informacijos vientisumo pažeidimą, ir net dalinį jos sunaikinimą.[60] Australijos Federacijos Baudžiamajame kodekse nurodoma, kad modifikavimas kompiuteryje laikomų duomenų atžvilgiu, yra: a) duomenų perdirbimas arba pašalinimas; arba b) į duomenis daromas papildymas (*angl. – modification, in respect of data held in a computer, means: (a) the alteration or removal of the data; or (b) an addition to the data*).[61] Apibendrinant galiu teigti, kad kompiuterinės informacijos pakeitimas - tai bet koks informacijos iškraipymas su tikslu padaryti ją kitokia, negu buvo nustatęs pats informacijos savininkas, padaryti informacijos turinį neatitinkantį tų tikslų, kuriems ji buvo sukurta originalioje versijoje.

Kompiuterinės informacijos prieinamumas pažeidžiamas įrenginiais ar kompiuterinėmis programomis apribojant naudojimąsi kompiuterine informacija. Apribojimas pasireiškia tuo, kad tam tikromis kompiuterinėmis programomis ar įrenginiais pasinaudodamas piktavalis užblokuoja tam tikram laikui arba visam priėjimą prie informacijos, esančios kompiuteryje, kompiuterių sistemose ar jų tinkluose. Tokiu būdu informacija negali pasinaudoti nei jos teisėtas savininkas, nei asmuo, kuriam savininkas leido susipažinti su kompiuterine informacija. Šią nuomonę patvirtina ir V.V. Krylov, teigdamas, kad blokavimas – elektroninės skaičiavimo mašinos ir jos elementų poveikio rezultatas, ko pasėkoje neįmanoma laikinai ar pastoviai atlikti kokius nors veiksmus su kompiuterine informacija.[62] Klasikinis pavyzdys tokių veiksmų yra DoS (angl. – *Denial of Service*) „atakos", kai į aukos kompiuterį ar jų sistemą specialiai suprogramuotomis priemonėmis yra pasiunčiama daugybė užklausų, kurių kompiuteris auka nesugeba pagal savo pajėgumus apdoroti, dėl ko sutrinka jo darbas.

Visi aukščiau išvardinti nusikalstami veiksmai turi būti neteisėti. Iš esmės turėjimo teisės kriterijus, kuris buvo įvestas tik po straipsnio pakeitimo, yra labai svarbus nagrinėjant nusikaltimų informatikai sampratą apskritai. Nusikaltimai informatikai pasižymi tam tikru specifiškumu, kadangi tie patys veiksmai, kurie yra įvardinti straipsnio dispozicijoje, atliekami turint tam teisę niekaip negali būti suprantami kaip nusikalstami. Pavyzdžiui, sistemos administratorius, kaip asmuo turintis įgaliojimus tvarkyti kompiuterinė sistemą, apriboja kompiuterinėmis programomis ar įrenginiais priėjima prie kompiuterinės informacijos taip tikrindamas sistemos atsparumą galimoms išorinėms atakoms; kriptografinėmis priemonėmis užkoduoja kompiuterinę informaciją, perduodamą kompiuteriniais tinklais taip formaliai

[60] Голубев В. Уголовно-правовые аспекты противодействия преступности в сфере использования электронно-вычислительных машин // http://www.crime-research.ru/library/Golubev1003.html (prisijungimo laikas: 2006-11-08).
[61] Australian Criminal code act 1995 // http://www.comlaw.gov.au/ComLaw/Management.nsf/current/bytitle/8F20DA53B8CF2FAFCA256F7100071F90?OpenDocument&VIEW=compilations (prisijungimo laikas: 2006-09-05).
[62].Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. // Уголовное право, 1998. - №3. – Р.83.

pakeisdamas ją, tačiau tai daro saugumo tikslais. Tuo tarpu, paimkime, pavyzdžiui, turto grobimą. Pats grobimas negali būti nei teisėtas nei neteisėtas, kadangi vien terminas *grobimas* mums sufleruoja apie veiksmų neteisėtumą. Negalima teisėtai pagrobti svetimą turtą. Grobimas visada yra atliekamas neteisėtai. Neturėjimo tam teisės sąvokos apibrėžimą mes galime rasti 2005 m. vasario 24 d. Tarybos pamatiniame sprendime 2005/222/TVR, dėl atakų prieš informacines sistemas. Šiame sprendime nurodoma, kad „neturėjimas tam teisės“ – tai prieiga ar įsikišimas, kuriam nesuteikė leidimo sistemos ar jos dalies savininkas, kitas teisės turėtojas, arba kurio neleidžia nacionalinės teisės aktai.[63] Autoriaus nuomone tai pamatinis apibrėžimas, kuris turėtų būti taikomas visoms LR BK XXX skyriuje aprašytoms nusikalstamoms veikoms.

Nustatant kaltės formą nusikaltimų informatikai sampratoje taip pat neišvengta nesutarimų. Rusijos teisėje manoma, kad nusikaltimai informatikai yra padaromi tiek tyčia, tiek ir dėl neatsargumo sunkių pasekmių atžvilgiu. Tačiau Lietuvos teisėje vyrauja nuomonė, kad visi nusikaltimai informatikai gali būti įvykdomi tik tyčia.

Už nusikaltimus informatikai atsakomybėn gali būti trauktinas ne tik fizinis asmuo, bet ir juridinis asmuo.

Apibendrinant galima teigti, kad neteisėtas kompiuterinės informacijos sunaikinimas, sugadinimas, pašalinimas ar pakeitimas arba įrenginiais ar kompiuterinėmis programomis apribojimas naudotis tokia informacija iš esmės atitinka nusikaltimų informatikai požymius ir neišeina iš sampratos konteksto ribų. Tačiau reikėtų pažymėti, kad kompiuterinės informacijos kaip nusikaltimo dalyko nustatymas yra diskusinis klausimas ir nepilnai atspindi nusikaltimų informatikai esmę apskritai. Taip pat, nusikaltimas informatikai turi būti suprantamas kaip daromas be teisės, nes tie patys veiksmai, bet sankcionuoti, tai yra suteikiant tam teisę (leidimą) nesudaro nusikaltimo, skirtingai negu kituose Baudžiamojo kodekso skyriuose numatytos nusikalstamos veikos.

[63] 2005 m. vasario 24 d. Tarybos pamatinis sprendimas 2005/222/TVR, dėl atakų prieš informacines sistemas // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:LT:NOT (prisijungimo laikas: 2006-08-22).

2.2 kompiuterinės programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas

Lietuvos Respublikos Baudžiamojo kodekso 197 straipsnio 1 dalis nustato, kad:

Tas, kas neteisėtai sunaikino, sugadino, pašalino ar pakeitė kompiuteryje esančią programą arba sutrikdė ar pakeitė kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbą padarydamas didelės žalos,

baudžiamas bauda arba laisvės atėmimu iki trejų metų.

2004 metais atlikti straipsnio pakeitimai[64] buvo orientuoti pagal 2001 m. lapkričio 23 dienos Europos Tarybos priimtos Konvencijos dėl elektroninių nusikaltimų reikalavimus. Lietuvos Respublikos BK 197 straipsnis buvo derintas ir jame atlikti atitinkami pakeitimai remiantis Konvencijos 5 straipsniu, kuriame sakoma, kad kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą didelį kompiuterinės sistemos darbo trukdymą įvedant, perduodant, sugadinant, sunaikinant, apgadinant, pakeičiant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis.[65] Iš esmės BK 197 straipsnis *mutatis mutandis*[66] atitinka Konvencijos 5 straipsnio nuostatas.

Kadangi straipsnis susideda iš dviejų loginių dalių ir sudaro du atskirus nusikaltimus informatikai, teisingiau būtų nagrinėti juos atskirai.

Analizuojant šiame Baudžiamojo kodekso straipsnyje aprašytą nusikalstamą veiką kaip nusikaltimą informatikai galima pastebėti, kad numatytoji veika pažeidžia visiems nusikaltimams informatikai būdingą teisinį gėrį, tai yra objektą. Sunaikinant, sugadinant, pašalinant ar pakeičiant kompiuterinę programą yra pakeičiamas jos vientisumas. Dėl to tokiais veiksmais yra pažeidžiami visuomeniniai santykiai, susiję su kompiuterinės informacijos saugumu. Tačiau iš karto kyla natūralus klausimas kuo skiriasi nusikalstami veiksmai, kuriais yra sugadinama, sunaikinama, pašalinama ar pakeičiama kompiuterinė informacija nuo tokių pat nusikalstamų veiksmų, kai nusikaltimo informatikai dalykas yra kompiuterinė programa, kad reikėtų juos išskirti į atskirus straipsnius. Šioje vietoje noriu pateikti truputėli istorijos. Tada, kai Lietuvos Respublikos Teisės ir Teisėtvarkos komitetas savo posėdyje svarstė pasiūlymus dėl straipsnio pakeitimo ir papildymo, Lietuvos Aukščiausiasis teismas siūlė apsvarstyti galimybę

---

[64] Lietuvos Respublikos Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymas // Valstybės žinios. 2004, Nr. 25-760

[65] Konvencija dėl elektroninių nusikaltimų // Valstybės žinios.2004, Nr. 36-1188.

[66] Lietuvos Respublikos Seimo Teisės ir teisėtvarkos komiteto išvada Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymo projektui // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=224985 (prisijungimo laikas: 2006-10-29).

BK 196 ir 197 straipsnius apjungti į vieną baudžiamojo kodekso straipsnį su trimis dalimis. Tačiau Teisės ir Teisėtvarkos komitetas nepritarė šiam siūlymui, argumentuodamas tuo, kad LR BK 196 ir 197 straipsniai numato skirtingą nusikalstamos veikos dalyką: kompiuterinę informaciją (196 str.) ir kompiuterių programas (197 str.).[67] Taigi darome išvadą, kad pagrindinė nusikalstamos veiklos išskyrimo į atskirą straipsnį priežastis yra skirtingi nusikaltimo informatikai dalykai – kompiuterinė informacija ir kompiuterinė programa. Tačiau žvelgiant iš nusikaltimų informatikai sampratos pozicijos yra diskutuotina ar minėti nusikaltimų informatikai dalykai yra tokie skirtingi, kad juos išskirti į atskirus Baudžiamojo kodekso straipsnius. Dar kartą pažvelkime į kompiuterinės informacijos ir kompiuterinės programos santykį. Kompiuterinės programos sąvoka yra pateikiama Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatyme. Šio įstatymo 2 straipsnio 18 punkte sakoma, kad kompiuterių programa – žodžiais, kodais, schemomis ar kitu pavidalu pateikiamų instrukcijų, kurios sudaro galimybę kompiuteriui atlikti tam tikrą užduotį ar pasiekti tam tikrą rezultatą, visuma, kai tos instrukcijos pateikiamos tokiomis priemonėmis, kurias kompiuteris gali perskaityti; ši sąvoka apima parengiamąją projektinę tokių instrukcijų medžiagą, jeigu pagal ją galima būtų sukurti minėtą instrukcijų visumą.[68] Kaip matome iš pateikto apibrėžimo, kompiuterinę programą galime apibrėžti dviem požymiais: 1) instrukcijų visuma; 2) galimybė perskaityti kompiuteriui. Šiuo atveju, svarbus požymis yra *instrukcijų visuma*. Galima drąsiai teigti, kad instrukcija, kaip taisyklių visuma yra sudaroma iš atitinkamų duomenų. 2005 m. vasario 24 d. Tarybos pamatinio sprendimo 2005/222/TVR, dėl atakų prieš informacines sistemas 1 straipsnio b) punktas nusako, kad kompiuteriniai duomenys – tai faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją. Dėl to, sutinku su teisininkų nuomone, kad kompiuterinė programa yra faktiškai ta pati kompiuterinė informacija, kurios sudedamoji dalis yra kompiuteriniai duomenys, tik pateikta kita išraiška (forma). Iš viso darytina išvada, kad įstatymų leidėjų Lietuvos Respublikos BK 196 ir 197 straipsnių dispozicijų išskyrimas į atskirus straipsnius nėra pakankamai argumentuotas. Tuo labiau, kad ir sankcijos griežtumas už nusikalstamas veikas yra identiškas.

Darykim prielaidą, kad kompiuterinės programos vientisumo apsauga išskiriant į atskirą straipsnį iš nusikaltimų informatikai sampratos pusės galėtų būti pagrysta. Tada nėra suprantamas baudžiamųjų įstatymų leidėjo nusikaltimo informatikai formuluotė eliminuojant kompiuterinių programų prieinamumo apsaugą. Aukščiau nagrinėto nusikaltimo informatikai dalykas kompiuterinė informacija yra saugoma nuo naudojimosi ja apribojimo. O juk yra

[67] Lietuvos Respublikos Seimo Teisės ir teisėtvarkos komiteto išvada Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymo projektui // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=224985 (prisijungimo laikas: 2006-10-29).

[68] Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas // Valstybės žinios. 1999, Nr. 50-1598.

galimybė nusikalstamais veiksmais apriboti, panaudojant įrenginius ar kompiuterines programas, naudojimąsi kompiuterinėmis programomis, kaip ir kompiuterine informacija. Tai tik dar sustiprina abejones dėl šių dviejų lygiaverčių nusikaltimų informatikai dalykų išskyrimo į atskirus straipsnius, tuo labiau, kad jų apsaugos lygis nėra vienodas.

Kompiuterinės programos sunaikinimas, sugadinimas, pašalinimas ar pakeitimas - tai nusikalstami veiksmai, kurių sampratos buvo nagrinėtos kompiuterinės informacijos sunaikinimo ir pakeitimo kaip nusikaltimo informatikai atveju.

Antroje straipsnio loginėje dalyje yra aprašyta nusikalstama veikla, kurios kėsinimosi objektu, be jau minėto, galima būtų papildomai išskirti kompiuterių tinklo, duomenų bazės ar informacinės sistemos tinkamą darbą, tinkamą numatytų funkcijų atlikimą. Konvencijos dėl elektroninių nusikaltimų paaiškinamajame rašte taip pat nurodoma, kad nustatant baudžiamąją atsakomybę už poveikį sistemai yra ginamas kompiuterio ar telekomunikacijų sistemos vartotojo ar operatoriaus teisėtas interesas, kad kompiuteris ar telekomunikacijų sistema gebėtų atlikti savo funkcijas tinkamai.[69] O, kadangi, kompiuteriniuose tinkluose, ar informacinėse sistemose apskritai, vyksta informaciniai procesai, kurie ir yra užtikrinami kompiuterinių tinklų ar informacinių sistemų tinkamu darbu, tai galima teigti, kad sutrikdžius ar kitaip pakeitus jų darbą yra pažeidžiamas kompiuterinės informacijos saugumas. Taigi, kaip matome, nusikalstamos veiklos objektas atitinka nusikaltimų informatikai sampratą.

Straipsnyje aprašytu nusikaltimu informatikai yra tiesiogiai kėsinamasi į kompiuterinę tinklą, duomenų banką ir informacinę sistemą – tai nusikalstamo kėsinimosi dalykai. Kompiuterinis tinklas yra suprantamas kaip kompiuterių grupė, sujungta tam tikrų įrenginių, užtikrinančių skaičiavimo sistemos resursų bendrą panaudojimą ir duomenų apsikeitimą tarp bet kurių kompiuterių grupių, pagalba. Paprasčiau sakant, kompiuterinis tinklas – tai tarpusavyje laidinėmis ar belaidėmis priemonėmis sujungti kompiuteriai informacijos apsikeitimo ir bendro naudojimo tikslui. Duomenų bankas - „tai informacinės sistemos dalis. Kitaip tariant, tai yra informacijos sutvarkymo forma arba informacija plačiąja prasme“.[70] Informacinė sistema – „tai prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą, taip pat juose saugomi, tvarkomi, iš jų išrenkami arba jais perduodami kompiuteriniai duomenys su tikslu juos apdoroti, panaudoti, apsaugoti ir prižiūrėti“.[71] Minėti nusikaltimo informatikai dalykai reikalauja šiek tiek

[69] Convention on cybercrime explanatory report.// http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (prisijungimo laikas: 2006-11-11).
[70] Civilka M., Lamanauskas T., Osinaitė G. ir kt./red. Sauliūnas D. Informacinių technologijų teisė. - Vilnius: NVO Teisės Institutas, 2004.P. 533.
[71] 2005 m. vasario 24 d. Tarybos pamatinis sprendimas 2005/222/TVR, dėl atakų prieš informacines sistemas // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:LT:NOT (prisijungimo laikas: 2006-08-22).

platesnio paaiškinimo. Kas liečia duomenų banką, tai čia abejonių dėl patekimo į nusikaltimų informatikai sampratą neturėtų kilti. Juk duomenų bankas iš esmės yra informacija plačiąja prasme. Tačiau, kompiuterinis tinklas ar informacinė sistema susideda tiek iš techninių įtaisų, kurie yra materialūs daiktai, tiek ir kompiuterinių programų sprendimų. Todėl, kompiuterinio tinklo ar informacinės sistemos kaip nusikaltimo dalyko darbo sutrikdymo ar pakeitimo vertinimas iš nusikaltimų informatikai sampratos pusės turėtų remtis tik kompiuterinių programų lygmenyje. Tiksliau sakant, nagrinėjamu atveju kompiuterinio tinklo ar informacinės sistemos darbo sutrikimas turėtų būti siejamas su juos valdančių kompiuterinių programų darbo sutrikimu, bet ne su fiziniu kompiuterinį tinklą ar informacinę sistemą sudarančių prietaisų sugadinimu. Nors fiziškai sugadinant techninius prietaisus taip pat gali sutrikti arba pakisti kompiuterinio tinklo ar informacinės sistemos darbas, tačiau tada nusikalstama veikla nepatenka į nusikaltimų informatikai sampratos ribas, bet gali būti vertinama kaip nusikaltimas nuosavybei, turtinėms teisėms ar turtiniams interesams.

Tiek kompiuterinis tinklas, tiek duomenų bankas, tiek informacinės sistemos yra sukuriamos atlikti tam tikras žmogui reikalingas iš anksto numatytas darbines funkcijas. Šios sistemos gali būti paveikiamos įrenginiais ar kompiuterinėmis programomis taip, kad:

1) visiškai ar iš dalies nebegalima atlikti numatytų darbinių funkcijų – sutrikdymas;

2) sistemos atlikinėja visiškai ar iš dalies ne tas darbines funkcijas, kurioms jos buvo sukurtos.

Apibendrinimui galima pasakyti, kad aprašytas nusikaltimas yra beveik identiškas nusikaltimui informatikai, kuris buvo nagrinėtas aukščiau. Dėl to jo išskyrimas į atskirą straipsnį nėra pakankamai argumentuotas. Taip pat, pažymėtina, kad pirmoje straipsnio loginėje dalyje aprašyti nusikalstami veiksmai neapima pilnai nusikaltimų informatikai sampratos, nes nėra nustatytos apsaugos kompiuterinės programos prieinamumui. Kompiuterinio tinklo ar informacinės sistemos darbo sutrikdymo ar pakeitimo vertinimas iš nusikaltimų informatikai pusės turėtų remtis tik kompiuterinių programų lygmeniu, tokiu būdu atskiriant nusikaltimus informatikai nuo nusikaltimų nuosavybei, turtinėms teisėms ir turtiniams interesams.

2.3 kompiuterinės informacijos pasisavinimas ir skleidimas

Lietuvos Respublikos Baudžiamojo kodekso 198 straipsnis nustato, kad:

1. Tas, kas pasisavino įstatymų saugomą kompiuterinę informaciją apie juridinį ar fizinį asmenį,

baudžiamas bauda arba laisvės atėmimu iki trejų metų.

2. Tas, kas viešai paskleidė, paskelbė, platino ar kitaip panaudojo informaciją, kurią gavo darydamas šio straipsnio 1 dalyje numatytą veiką,

baudžiamas bauda arba areštu, arba laisvės atėmimu iki ketverių metų.

Straipsnyje aprašyto nusikaltimo informatikai kėsinimosi objektu galima įvardinti visuomeninius santykius, susijusius su įstatymų saugomos kompiuterinės informacijos saugumu, tačiau iš karto kyla klausimas ar mes galime teigti, kad nusikalstama veikla neišeina iš nusikaltimų informatikai sampratos konteksto. Abejonių kilimo pagrindas yra pati *įstatymų saugomos* kompiuterinės informacijos kaip nusikaltimo dalyko samprata. Kaip nagrinėta buvo aukščiau, įstatymų saugoma kompiuterinė informacija gali būti suprantama, kaip informacija, kuriai atitinkamomis teisinėmis normomis yra suteiktas teisinis statusas ir nustatytas apsaugos rėžimas, kurio lygis nustatomas pagal informacijos svarbą. Taip yra ribojamas asmenų ratas, kurie turi (gali turėti) teisę susipažinti, valdyti ar kitaip naudoti įstatymų saugomą kompiuterinę informaciją. Įstatymų saugoma kompiuterinė informacija gali priklausyti fiziniam asmeniui (informacija apie privatų asmens gyvenimą), juridiniam asmeniui (komercinės paslaptys, banko paslaptys ir kt.) ar valstybei (valstybės, tarnybos paslaptys), nors valstybė, remiantis Lietuvos Respublikos civilinio kodekso 2.35 straipsnio nuostatomis yra pripažįstama juridiniu asmeniu.[72] Tačiau informacija apie privatų asmens gyvenimą yra ginama ir Baudžiamojo kodekso 167 straipsniu „Neteisėtas informacijos apie privatų asmens gyvenimą rinkimas“, 168 straipsniu „Neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas“; komercinės paslaptys yra ginamos 210 straipsniu „Komercinis šnipinėjimas“, 211 straipsniu „Komercinės paslapties atskleidimas“. Dar kebliau yra su valstybės paslaptimi. Baudžiamojo kodekso 119 straipsnis „Šnipinėjimas“, 124 straipsnis „Neteisėtas disponavimas informacija, kuri yra valstybės paslaptis“, 125 straipsnis „ Valstybės paslapties atskleidimas“ gina valstybės paslapties slaptumą, o informacijos pripažinimas valstybės paslaptimi nepriklauso nuo jos fiksavimo būdo. Taigi, valstybės paslaptimi gali būti ir kompiuterinė informacija. Atsižvelgiant į tai, nėra visiškai aišku ar įstatymų saugomos kompiuterinės informacijos susijusios su juridiniu ar fiziniu asmeniu pasisavinimas, viešas paskleidimas, paskelbimas, platinimas ar kitoks panaudojimas pilnutinai patenka į nusikaltimų informatikai sampratą ar pažeidžia kitus,

[72] Lietuvos Respublikos civilinis kodeksas // Valstybės žinios. 2000, Nr. 74-2262.

nesusijusius su kompiuterinės informacijos saugumu interesus. Manome, kad pagrindinis kriterijus informacijos pasisavinimo atveju, kurį nustačius būtų galima šią nusikalstamą veiką priskirti prie nusikaltimų informatikai, galėtų būti *neteisėto prisijungimo* prie kompiuterio ar kompiuterinio tinklo, kuriame yra įstatymų saugoma ir susijusi su juridiniu ar fiziniu asmeniu kompiuterinė informacija, faktas. Viešo informacijos paskleidimo, paskelbimo, platinimo ar kitokio panaudojimo atveju, autoriaus nuomone, atskyrimo kriterijumi galėtų būti kompiuterinis aspektas, tai yra kompiuterinių tinklų, tokių kaip Internetas panaudojimas. Būtent neteisėtos prieigos būdu įstatymų saugomos kompiuterinės informacijos pasisavinimas, taip pat, pavyzdžiui, Interneto panaudojimas tokios informacijos viešam paskleidimui, paskelbimui, platinimui leistų priskirti šią nusikalstamą veiklą prie nusikaltimų informatikai.

2.4 neteisėtas prisijungimas prie kompiuterinio tinklo

Lietuvos Respublikos Baudžiamojo kodekso 198[1] straipsnio 1 dalis nustato, kad:

Tas, kas neteisėtai prisijungė prie kompiuterio ar kompiuterinio tinklo pažeisdamas kompiuterio ar kompiuterinio tinklo apsaugos priemones,

baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki vienerių metų.

Šis baudžiamojo kodekso straipsnis, numatantis atsakomybę už neteisėtą prisijungimą prie kompiuterio bei kompiuterinės sistemos yra logiška tąsa to darbo, kurį atliko įstatymų leidėjas derindamas nacionalinius teisės aktus su tarptautinių teisės aktų reikalavimais. Baudžiamasis kodeksas 198[1] straipsniu buvo papildytas 2004 metais.[73] 2001 m. lapkričio 23 dienos Europos Tarybos priimtos Konvencijos dėl elektroninių nusikaltimų 2 straipsniu siekiama, kad būtų nustatyta baudžiamoji atsakomybė už neteisėtą prieigą prie kompiuterinės sistemos. Konvencijos 2 straipsnyje nurodyta, kad kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą prieigą prie visos kompiuterinės sistemos arba jos dalies. Šalis gali reikalauti, kad toks nusikaltimas būtų padarytas pažeidžiant apsaugos priemones, ketinant gauti kompiuterinius duomenis ar turint kitą nesąžiningą ketinimą, arba kad jis būtų susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema.[74] 2005 metais Europos Sąjungos Taryba atsižvelgdama į atakų prieš informacines sistemas, ypač dėl organizuoto nusikalstamumo grėsmės, ir didėjančio susirūpinimo galimomis teroristų atakomis prieš informacines sistemas, kurios yra valstybių narių ypač svarbios infrastruktūros dalis, įrodymų buvimą, priėmė pamatinį sprendimą, beveik visiškai antrinantį Konvencijos dėl elektroninių nusikaltimų 2 straipsnį. Šiuo pamatiniu sprendimu reikalaujama, kad už neteisėtą prieigą prie informacinių sistemų būtų baudžiama kaip už nusikaltimą. Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte[75] teigiama, kad „*neteisėta prieiga*“ kaip viena iš esminių nusikalstamų veiklų, nukreiptų prieš kompiuterines sistemas ir kompiuterinius duomenis, reikalinga kriminalizuoti. Reikalingumas atspindi organizacijų ir asmenų interesus tvarkyti, valdyti ir kontroliuoti jiems priklausančias kompiuterines sistemas nekliudomai ir nevaržomai. Taip pat pabrėžiama, kad vien tik neteisėtas kišimasis (angl. – *unautorised intrusion)* į kompiuterines sistemas, tai yra „hakingas“ (angl. –

[73] Lietuvos Respublikos Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymas // Valstybės žinios. 2004, Nr. 25-760.

[74] Konvencija dėl elektroninių nusikaltimų // Valstybės žinios. 2004, Nr. 36-1188.

[75] Convention on cybercrime explanatory report // http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (prisijungimo laikas: 2006-11-11).

hacking), „krekingas“ (angl.- *cracking*) ir „kompiuterinis piktnaudžiavimas“ (angl.- *computer trespass*) iš principo turi būti neteisėti patys savaime.

Žvelgiant iš nusikaltimų informatikai sampratos pozicijos, atrodytu, kad nusikaltimo objekto nustatymas šiuo atveju yra komplikuotas, nes kriminalizuota veika nesukelia jokios apčiuopiamos realios žalos. Dėl to natūraliai kyla klausymas ar iš vis ši veika yra pavojinga ir ar už ją buvo būtina nustatyti baudžiamąją atsakomybę. Juk, jeigu padaroma veika nekyla jokios pavojingos pasekmės, neatsiranda žala, tai ir pati veika nėra pavojinga. Tačiau mes žinome iš baudžiamosios teisės teorijos, jog kėsinantis į teisinius gėrius gali būti padaroma ne tik reali žala, bet gali kilti ir tokios žalos grėsmė. Esant žalos atsiradimo grėsmei, įstatymų saugomame objekte irgi įvyksta tam tikri pakitimai.[76] V.S. Komisarovas pateikdamas nusikaltimų kompiuterinės informacijos srityje sampratą taip pat nurodė, kad nusikalstami veiksmai gali ne tik padaryti žalą visuomeniniams santykiams, bet ir sukelti tokios žalos atsiradimo grėsmę.[77] Dėl to, „neteisėta prieiga pažeidžiant saugumo priemones sukelia realią grėsmę visuomeniniams santykiams saugant ir apdorojant informaciją, pažeidžia nukentėjusiųjų slaptumo sritį“[78], kas leidžia teigti, kad neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo iš esmės atitinka nusikaltimo informatikai sampratos požymius.

Neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo, kitaip – neteisėta prieiga, teisinėje literatūroje aptarinėjama gan plačiai. U. Sieber neteisėtą prieigą supranta kaip prasiskverbimą į kompiuterių sistemas, kai tikslas yra ne manipuliacija, sabotažas ar šnipinėjimas, o pasitenkinimas, susijęs su kompiuterinės sistemos apsaugos priemonių įveikimu.[79] M.V. Bogomolov neteisėtą prieigą supranta kaip nesankcionuotas informacijos savininko ar valdytojo asmens susipažinimas su duomenimis, kurie yra kompiuterinėje laikmenoje ar kompiuteryje ir turintys apsaugos lygį, nustatytą teisės aktais.[80] Jis remiasi kito teisininko V.V. Krylovo nuomone, kad prieiga prie elektroninės skaičiavimo mašinos yra informacinės sistemos savininko sankcionuota ir sureguliuota asmens sąveika su kompiuteriniais įrenginiais ir (arba) asmens susipažinimas su duomenimis, esančiais kompiuterinėse laikmenose ar kompiuteryje.[81] M.M. Karelina teigia, kad pripažįstama neteisėta tokia asmens prieiga prie kompiuterinės informacijos, kai asmuo neturi teisės gauti ir dirbti su tokia informacija arba

---

[76] Abramavičius A., Čepas A., Drakšienė A. ir kt. Baudžiamoji teisė: bendroji dalis. –Vilnius: Eugrimas, 1998.P. 177.
[77] Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность //Юридический мир, Февраль 1998. P.13.
[78] Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai // Jurisprudencija 2003, 47 (39). P. 72.
[79] Ten pat. P.67.
[80] Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации. // http://pu.boom.ru/book/index.html (prisijungimo laikas: 2006-11-10).
[81]Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. // Уголовное право, 1998. - №3. – P.84.

kompiuterine sistema.[82] Taip pat ji priduria, kad tiek informacijos, tiek kompiuterinės sistemos atžvilgiu turi būti naudojamos apsaugos priemonės. Apibendrinant galima teigti, kad neteisėtas prisijungimas prie kompiuterio ar kompiuterių tinklo – tai tokie nusikalstami asmens veiksmai, kai pasinaudojant atitinkamais prisijungimo būdais yra pažeidžiamos kompiuterio ar kompiuterių tinklo apsaugos priemonės ir įgyjama galimybė naudoti ar kitaip valdyti tiek esamą kompiuterinę informaciją, tiek kompiuterinę sistemą, ir nesant kompiuterio ar jų tinklo savininko aiškiai išreikšto leidimo šiems veiksmams.

Nors nagrinėjant neteisėtą prisijungimą prie kompiuterio ar kompiuterinio tinklo nusikaltimų informatikai kontekste mums ne tiek yra svarbu patys nusikalstamos veikos padarymo būdai[83], tačiau pažintiniais tikslai juos verta paminėti. Neteisėtai prisijungti prie kompiuterio ar jų tinklo galima:

1) pasinaudojant specialiais techniniais įrenginiais arba kompiuterinėmis programomis, kurių pagalba yra apeinamos, pasinaudojant kompiuterių programų klaidomis, arba pažeidžiamos apsaugos priemonės ir prisijungiama prie dalies ar visos kompiuterinės sistemos;

2) slaptažodžių ar apsaugos kodų panaudojimas neteisėtam prisijungimui prie kompiuterio art kompiuterinio tinklo ir kitos priemonės.

Pažymėtina, kad į nusikaltimų informatikai sampratos požymius neįeina nusikalstami tikslai, tačiau Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje nurodoma, kad *„Šalis gali reikalauti, kad nusikaltimas būtų padarytas ..., ketinant gauti kompiuterinius duomenis“*. Svarstant Baudžiamojo kodekso papildymą 198[1] straipsniu, Lietuvos Respublikos Seimo Teisės ir teisėtvarkos komitetui Teisės institutas davė siūlymą straipsnio dispozicijoje numatyti nusikalstamos veikos tikslą – *siekį gauti informaciją.*[84] Šis siūlymas buvo motyvuotas tuo, kad esama straipsnio redakcija užtraukia baudžiamąją atsakomybę už pernelyg platų veikų ratą. Praktiškai kiekvienas savo žinias bei jėgas išbandyti sumanęs paauglys, neteisėtai prisijungęs prie kompiuterio ar jų tinklo pažeisdamas apsaugos priemones, būtų baudžiamas už nusikaltimo padarymą. Šiam siūlymui nebuvo pritarta motyvuojant tuo, kad atskleidžiant straipsnyje numatytą veiką, sunku būtų įrodyti „*siekimo gauti duomenis*“ požymį.

[82] Карелина М.М. Преступления в сфере компьютерной информации // http://www.relcom.ru/Archive/1997/ComputerLaw/New_code.htm (prisijungimo laikas: 2006-11-10).
[83] Faktiškai būtų neįmanoma ir netikslinga išvardinti visus nusikalstamos veikos padarymo būdus straipsnio dispozicijoje, nes informacinės technologijos nuolatos tobulėja, o nusikalstamas veikas darantys asmenys darosi vis išradingesni naudojant informacines technologijas nusikalstamiems tikslams (autoriaus pastaba).
[84] Lietuvos Respublikos Seimo Teisės ir teisėtvarkos komiteto išvada Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymo projektui // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=224985 (prisijungimo laikas: 2006-10-29).

Neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo pažeidžiant apsaugos priemones formaliai yra vienas iš esminių nusikaltimų informatikai, nes tiek neteisėtas kompiuterinės informacijos, kompiuterinės programos sugadinimas, sunaikinimas, pašalinimas ar kitoks pakeitimas, įstatymų saugomos informacijos pasisavinimas daugeliu atveju bus įvykdomi neteisėtai prisijungiant prie kompiuterio ar kompiuterinio tinklo. Todėl neteisėta prieiga iš esmės sukelia grėsmę visuomeniniams santykiams, susijusiems su kompiuterinės informacijos saugumu. Neteisėtas prisijungimas suprantamas kaip prisijungimas pažeidžiant apsaugos priemones, dėl ko įgyjama galimybė valdyti kompiuteryje ar kompiuteriniame tinkle esančią informaciją.

2.5 neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti

Lietuvos Respublikos Baudžiamojo kodekso 198² straipsnis nustato, kad:

1. Tas, kas neteisėtai gamino, gabeno, pardavė ar kitaip platino šio Kodekso 166, 198 ir 198¹ straipsniuose numatytiems nusikaltimams daryti tiesiogiai skirtus ar pritaikytus įrenginius ar kompiuterines programas, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis arba turėdamas tikslą daryti tuos nusikaltimus juos įgijo ar laikė,

baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki vienerių metų.

2. Tas, kas neteisėtai gamino, gabeno, pardavė ar kitaip platino šio Kodekso 196 ar 197 straipsniuose numatytiems nusikaltimams daryti tiesiogiai skirtus ar pritaikytus įrenginius ar kompiuterines programas, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis arba turėdamas tikslą daryti tuos nusikaltimus juos įgijo ar laikė,

baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki trejų metų.

Kaip ir aukščiau nagrinėti straipsniai, taip ir BK 198² straipsnis buvo įtrauktas į baudžiamąjį įstatymą 2004 metais.[85] Konvencijos dėl elektroninių nusikaltimų 6 straipsnis nustato, kad kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą:

a) gaminimą, pardavimą, įsigijimą naudoti, įvežimą, platinimą arba kitokį galimybės naudotis suteikimą:

i) įtaiso, įskaitant kompiuterinę programą, sukurto ar pritaikyto pirmiausia neteisėtai prieigai, neteisėtai perimčiai, poveikiui duomenims ir poveikiui sistemai daryti;

ii) kompiuterio slaptažodžio, prieigos kodo arba panašių duomenų, kuriais galima prieiti prie visos kompiuterinės informacinės sistemos arba jos dalies, kai ketinama juos panaudoti neteisėtai prieigai, neteisėtai perimčiai, poveikiui duomenims ir poveikiui sistemai daryti ir,

b) a punkto i ir ii papunkčiuose minimo dalyko turėjimą ketinant jį panaudoti neteisėtai prieigai, neteisėtai perimčiai, poveikiui duomenims ir poveikiui sistemai daryti. Šalis vadovaudamasi savo teise, gali reikalauti, kad baudžiamoji atsakomybė būtų užtraukiama tik turint keletą tokių dalykų.[86]

---

[85] Lietuvos Respublikos Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymas // Valstybės žinios. 2004, Nr. 25-760.

[86] Konvencija dėl elektroninių nusikaltimų // Valstybės žinios,2004, Nr. 36-1188.

Nusikaltimų informatikai sampratos vienas iš požymių – objektas, yra visuomeniniai santykiai, susiję su kompiuterinės informacijos saugumu, kai nusikalstamais veiksmais yra pažeidžiamas kompiuterinės informacijos konfidencialumas, vientisumas ir prieinamumas. Nusikalstamos veiklos, nagrinėjamos šioje darbo dalyje aprašyme įstatymų leidėjas tiesiogiai nenurodo jokio poveikio kompiuterinės informacijos saugumui, dėl ko gali kilti abejonių dėl nusikalstamos veikos priskyrimo nusikaltimams informatikai. Tačiau atidžiai nagrinėjant nusikalstamą veiklą, galime pastebėti, kad kompiuterinių programų ar įrenginių, skirtų nusikaltimams daryti gaminimas, gabenimas, pardavimas, kitoks platinimas, įgijimas iš esmės yra pasiruošimas įvykdyti nusikalstamus veiksmus kito teisinio gėrio atžvilgiu. Tiksliau tariant, priemonių gaminimas ar kitoks susiieškojimas nagrinėjamu atveju kelia potencialią grėsmę kilti toms pasekmėms, kurias sukelia kiti nusikaltimai, tame tarpe ir nusikaltimai informatikai. Pasitelkiant tokias kompiuterines programas ar įrenginius neprireikia daug pastangų, kad sugadinti, pakeisti, pasisavinti ar kitaip paveikti tiek įstatymų saugomą kompiuterinė informaciją susijusią su juridiniu ar fiziniu asmeniu, tiek ir kitą kompiuterinę informaciją, užblokuoti priėjimą prie jos, neteisėtai prisijungti prie kompiuterio ar kompiuterinio tinklo, pasinaudojant kompiuterine informacija, tokia kaip slaptažodžiai ar prisijungimo kodai, paveikti kompiuteriuose, kompiuterių tinkluose ar informacinėse sistemose esančios kompiuterinės informacijos konfidencialumą. Tokiu būdu yra sudaroma grėsmė santykiams, susijusiems su kompiuterinės informacijos saugumu kaip nusikaltimų informatikai objektui. Dėl to galima teigti, kad nusikalstamos veikos, aprašytos šiame straipsnyje, kėsinimosi objektas yra grėsmės kilimas tiems santykiams, kurie reguliuoja informacijos kompiuterinėje formoje konfidencialumą, vientisumą ir prieinamumą.

Nusikaltimų informatikai samprata numato, kad nusikalstamos veiklos dalykas turi būti kompiuterinė informacija. Analizuojamos nusikalstamos veiklos dalykas yra įrenginiai, kompiuterinės programos, slaptažodžiai, prisijungimo kodai ar kitokie duomenys. Asmuo gamindamas įrenginius, kompiuterines programas, įgydamas slaptažodžius, prisijungimo kodus savo nusikalstamai veiklai nepadaro realios tiesioginės žalos kompiuterinei informacija. Pats gaminimo, pardavimo ar platinimo faktas nesugadina kokioje nors informacinėje sistemoje esančios informacijos, neužblokuoja priėjimo prie informacijos, tačiau sudaro grėsmę tokių pasekmių atsiradimui, jei asmuo turi tikslą tokius nusikaltimus daryti. Kaip tik čia mes prieiname prie dar vieno svarbaus dalyko, leidžiančio neteisėtą disponavimą įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitais duomenimis priskirti prie nusikaltimų informatikai. Tai *neteisėtumo* požymis. Iš esmės tai kertinis momentas, kuris, kaip ir aukščiau aptartuose nusikaltimuose, vaidina labai svarbų vaidmenį ir kurio buvimas mums leidžia nusikalstamą veiką (esant visiems kitiems požymiams) vertinti kaip nusikaltimą informatikai.

Negali būti suprantami veiksmai kaip nusikaltimas informatikai kai, pavyzdžiui, programuotojas pagal savo profesiją gabena arba laiko kenksmingą kompiuterinę programą (pvz. – „virusą“) su tikslu nustatyti jos kenksmingumo lygį ir sukurti programinį kodą naikinantį kenksmingą programą. Taigi, jis neturi tikslo pasinaudodamas kompiuterine programa daryti nusikalstamą veiklą, dėl ko jo veiksmai yra teisėti. Nors sunku įsivaizduoti teisėtai gaminamas, parduodamas ar kitaip platinamas kompiuterines programas nusikaltimams daryti, bet sutinkama ir tokių atvejų. Viena neįvardinta komercinė įmonė visiškai legaliai parduoda programą „Acallno“ skirtą vykdyti šnipinėjimo veiksmus mobiliuose telefonuose, veikiančiuose Symbian operacinės sistemos pagrindu. Programa slepia savo buvimą mobiliajame telefone ir dubliuoja siunčiamas SMS trumpąsias žinutes persiusdama jų kopijas programoje nurodytu telefono numeriu.[87] Toks kompiuterinės programos veikimas vertinamas kaip kenksmingas, kadangi pažeidžia informacijos konfidencialumą.

Pilnai nusikaltimo sampratai yra tikslinga aptarti įrenginių ir kompiuterinių programų, skirtų nusikaltimams daryti sampratas. Įrenginiai, skirti nusikalstamoms veikoms daryti - tai įrenginiai skirti tiesioginiam perėmimui, elektromagnetiniam perėmimui ar radioelektroniniai pasiklausymo įrenginiai. Kompiuterinės programos skirtos daryti nusikaltimams dažniausiai yra vadinamos kenksmingomis kompiuterinėmis programomis (angl. – harmful software). Toks pavadinimas yra kilęs dėl to, jog tokios programos veikdamos kompiuterinėje ar informacinėje sistemoje vykdo destrukcinius veiksmus, tai yra daro žalą. Tokių programų programinis kodas yra specialiai suprogramuojamas taip, kad veikdama sistemoje ji kenktų jos normaliam darbui ar atlikinėtų kitus nekorektiškus, neteisėtus veiksmus. Kenksmingos kompiuterinės programos dažniausiai yra skirstomos į tris dideles grupes - „*kompiuterinius virusus*“ (angl. – computer viruses), „*Trojos arklius*“ (angl. – Trojan horse) ir „ *kirminus*“ (angl. – Worms). Kompiuterinis virusas – tai programa ar dalis programinio kodo, kuri prisijungia prie programos ar kito failo, dažniausiai vykdomojo (angl. – executable), trikdo jos normalų darbą bei daro savo kopijas, kurios prijungiamos prie kitų failų. Kitaip sakant, tokio tipo kompiuterinės programos turi suprogramuotą automatinį dauginimosi ir maskavimosi mechanizmą „Trojos arklys“ – iš pirmo žvilgsnio atrodanti naudinga kompiuterinė programa, tačiau iš tikrųjų savyje maskuojanti kenksmingas kompiuteriui funkcijas, pavyzdžiui, suteikia piktavaliui galimybę pasijungti prie kompiuterio arba renka tam tikrą informaciją, esančią kompiuteryje ir išsiunčia piktavaliui. „Kirminas“ – tai galima sakyti viruso poklasis, kuris be vartotojo veiksmų daro savo kopijas ir plinta kompiuterių tinklais. Didžiausias jų keliamas pavojus ir jų sugebėjimas daugintis didžiuliais kiekiais ir greitai išplisti po kompiuterių tinklą siunčiant savo kopijas. Tokiu būdu yra

[87] Гостев А. Современные информационные угрозы, III квартал 2006 // http://www.crime-research.ru/articles/art15/ (prisijungimo laikas: 2006-11-20).

labai sutrikdomas kompiuterių tinklų darbas, kompiuteriai gali nustoti reaguoti į bet kokias komandas.[88]

Nagrinėjant straipsnio dispoziciją lengvai galima pastebėti, kad įstatymų leidėjas aprašydamas nusikalstamą veiką naudoja daugiskaitą – „*įrenginius, kompiuterines programas, slaptažodžius, prisijungimo kodus ir kitokius duomenis*“. Dėl to natūraliai galima galvoti, jog baudžiamoji atsakomybė už BK 198² straipsnyje numatytą nusikalstamą veiką nekyla tuomet, kai yra gaminama, gabenama, parduodama ar kitaip platinama viena kompiuterinė programa, vienas įrenginys, slaptažodis, prisijungimo kodas nusikaltimams daryti. Tokį įstatyminės technikos netikslumą pastebi ir teisininkai nagrinėjantys Rusijos Federacijos Baudžiamojo kodekso 272 straipsnį, nustatantį atsakomybę už elektroninėms skaičiavimo mašinoms žalingų programų gaminimą, naudojimą ir platinimą. Šiame straipsnyje taip pat aprašant nusikalstamą veiką panaudota daugiskaita. Kas liečia Lietuvos Respublikos Baudžiamojo kodekso 198² straipsnį, tai galima pagrįstai manyti, jog įstatymų leidėjas kriminalizuodamas nusikalstamą veiką vadovavosi Konvencijos dėl elektroninių nusikaltimų 6 straipsnio nuostata – „*Šalis, ..., gali reikalauti, kad baudžiamoji atsakomybė būtų užtraukiama tik turint keletą tokių dalykų*“.[89] Tačiau, manytina, reikėtų pritarti V.S. Komisarovo nuomonei[90], kad nustatant baudžiamąją atsakomybę už minėtą nusikalstamą veiką reikia vadovautis ne tiek kiekybiniu kriterijumi, kiek potencialiai kenksmingomis kompiuterinės programos ar įrenginio savybėmis ir realiomis galimybėmis sukelti žalą kompiuterinei informacijai ar visai informacinei sistemai. Dėl to, autoriaus nuomone, veiksmai, kai neteisėtai yra gaminamas, gabenamas, parduodamas ar kitaip platinamas vienas įrenginys, viena kompiuterinė programa, slaptažodis ar prisijungimo kodas atskirais atvejais gali būti vertinamas kaip nusikaltimas informatikai.

Nors neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ar kitais duomenimis ar jų įsigijimas pats savaime nepažeidžia nusikaltimų informatikai objekto, tačiau šie veiksmai yra vertintini kaip pavojingi, nes kaip ir neteisėto prisijungimo prie kompiuterio ar kompiuterinio tinklo atvejų sukelia realią grėsmę visuomeniniams santykiams, kaip teisiniam gėriui. Aprašytos nusikalstamos veiklos pavojingumas vertintinas atsižvelgiant į neturėjimo teisės kriterijų. Sankcionuoti tokie veiksmai nesudaro nusikaltimo informatikai ir neturėtų būti vertinami kaip pavojingi. Taip pat nemanytina, kad įrenginių ir kompiuterinių programų, slaptažodžių ir prisijungimo kodų kiekybinis kriterijus turėtų būti vertinamas kaip požymis priskirti veiką prie nusikaltimų informatikai. Visuomet turėtų

[88] Informacija imta iš Microsoft Lietuva interneto puslapio http://www.microsoft.com/lietuva/security/home/antivirus/virus101.mspx (prisijungimo laikas: 2006-11-12).
[89] Konvencija dėl elektroninių nusikaltimų // Valstybės žinios.2004, Nr. 36-1188.
[90] Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность //Юридический мир, Февраль 1998. P.16.

būti vertinama įrenginio ar kenksmingos kompiuterinės programos potenciali galimybė pažeisti visuomeninį interesą ir sukelti žalingas pasekmes.

3. NUSIKALTIMŲ INFORMATIKAI SAMPRATA – PROBLEMOS SPRENDIMAS

Nors Peter N. Graboskis (Peter N. Grabosky) remdamasis kriminologiniu nusikaltimo aiškinimu, paremtu trimis faktoriais – motyvacija (*angl. – motivation*), galimybe (*angl. – opportunity*) ir tinkamos apsaugos stoka (*angl. – the absence of a capable guardian*), - mano, kad „virtualus nusikalstamumas“ iš esmės niekuo nesiskiria nuo žemiško (*angl. – terrestrial*) nusikaltimo, kurį mes gerai pažįstam. Aišku, teigia jis, kai kurie reiškiniai yra nauji, bet dauguma nusikaltimų, įvykdytų su ar prieš kompiuterius skiriasi tik įvykdymo terpe (*angl. – in terms of medium*).[91]

Tačiau, nuomonių, kad kompiuteriniai, elektroniniai nusikaltimai nesudaro visiškai naujų nusikaltimų rūšies buvo ir daugiau. Bet remiantis daugybės teisinių studijų buvo prieita prie išvados, kad kai kurie iš šių nusikaltimų, vis dėlto, sudaro naujus nusikalstamos veiklos reiškinius, kurie reikalauja ne tik atskiro reguliavimo, bet ir atitinkamos sampratos, nusakančios jų esmę.

Nors Harvardo teisiniame žurnale yra sutikta nuomonė, kad elektroniniams nusikaltimams tampant vis lengviau įvykdomiems, visuomenei tampant vis labiau priklausomai nuo Interneto, didėjant katastrofinių atakų grėsmei, remiantis atsparios sistemos (*angl. – immune system*) idėja kompiuteriniai tinklai, o tiksliau Internetas tampa atsparesnis tam tikram žalingam poveikiui. Atsparios sistemos idėja remiasi prielaidomis, kad saugumo spragų panaudojimas priverčia gamintojus „užlopyti“ saugumo spragas, tobulinant sistemas akcentuoti į jų saugumą, o vartotojus įdieginėti saugumo pataisas ir pasinaudoti saugumo praktika, kas leistų sumažinti katastrofinių atakų tikimybę. Taip pat teigiama, kad kai kurie elektroniniai nusikaltimai gali atnešti daugiau naudos negu žalos (*angl. – beneficial cybercrime*), todėl kad jie atkreipia dėmesį į su saugumu susijusius pavojus, paskatina taisyti saugumo spragas, imtis kitų atsargumo priemonių, kurios gali užkirsti kelia daug žalingesnėms atakoms. Tokie nusikaltimai, be abejo, turėtų būti vertinami tik naudos tinklui požiūriu, jeigu kilusi žala yra mažesnė negu tikėtinos žalos dydis nuo galimų atakų, jeigu saugumo spragos nebūtų pataisytos.[92]

Tačiau, savireguliacinis požiūris į kai kuriuos elektroninius, tame tarpe ir nusikaltimus informatikai, pripažįstant jų tam tikrą teigiamą poveikį kompiuteriniams tinklams (Internetui), galėtų kardinaliai pakeisti nusikaltimų informatikai ir kompiuterinių nusikaltimų apskritai sampratas. Toks požiūris yra ganėtinai jaunas ir reikalaujantis išsamesnių studijų, bet jau dabar

[91] Grabosky P.N. Virtual Criminality: Old Wine In New Bottles? // Social & Legal Studies. 2001.
[92] Immunizing the Internet, or: how I learned to stop worrying and love the worm // Harvard Law Review Vol. 119 – June 2006 – Nr. 8 http://www.harvardlawreview.org/issues/119/june06/june06.shtml (prisijungimo laikas: 2006-11-30).

galintis dar labiau paaštrinti vieningos reiškinio esmę atspindinčios nusikaltimų informatikai sampratos problemą.

Autoriaus nuomone, daugeliu atveju teisinės problemos sprendimas remiasi naujų arba koreguojančių tezių, teiginių suformulavimu. Todėl bandydamas spręsti nusikaltimų informatikai sampratos problemą autorius pateiks jo nuomone tinkamiausią šiam laikotarpiui nusikaltimų informatikai sampratą. Samprata, kuri bus pateikta žemiau, remsis jau suformuotais teisniais principais ir susidarys iš pagrindinių požymių, kuriuos, manau, pirmiausia ir reikėtų aptarti.

Remdamasis ankstesnėse darbo dalyse nagrinėtais klausimais, vis dėlto autorius mano, kad nusikaltimų informatikai objektas yra teisėti asmenų, tiek fizinių tiek ir juridinių, interesai naudojant ar kitaip valdant kompiuterinę informaciją. Asmenų teisėtas interesas, kaip buvo kalbėta anksčiau, tai asmens pagrįstas tikėjimas, kad kompiuterinė informacija išliks konfidenciali, vientisa ir prieinama. Negaliu paneigti, kad nustatant nusikaltimų informatikai objektą aš vadovavausi Konvencijos dėl elektroninių nusikaltimų nuostatomis. Tačiau autorius mano, kad šios nuostatos šiuo metu yra fundamentalios ir negalima į jas neatsižvelgti.

Nusikaltimų informatikai dalyku aš išskirčiau kompiuterinius duomenis ir informacinę struktūrą. Kompiuterinius duomenis kaip nusikaltimo dalyką aš įvardinu netik dėl to, kad jis yra nurodomas ir Budapešto Konvencijoje dėl elektroninių nusikaltimų, bet ir dėl kompiuterinių duomenų savybės kisti nekeičiant pačios kompiuterinės informacijos, kas leidžia tiksliau atskleisti nusikaltimų informatikai esmę. Informacinę struktūrą aš suprantu kaip kompiuterinių duomenų ir techninių sprendimų bendrasąveikos terpė. Informacinę struktūrą kaip nusikaltimų informatikai dalyką aš įvardinau neatsitiktinai, bet laikydamasis technologinio neutralumo principo. Kaip matyti iš Lietuvos Respublikos Baudžiamojo kodekso XXX skyriaus „Nusikaltimai informatikai“, įstatymų leidėjas nusikaltimo dalyku be kompiuterinės informacijos nurodo kompiuterius, kompiuterinius tinklus. Tačiau vykstant informacinių technologijų konvergencijai po kelerių metų toks įstatymo leidėjų požiūris nebeatspindės tikros nusikaltimų informatikai esmės. Jau dabar tinklus tarpusavyje gali sudaryti tiek kompiuteris, mobilus telefonas, tiek kiti daugialypės terpės įrenginiai, taip pat spartus RFID (*angl. – radio frequency identification*) lustų naudojimas tokiose srityse, kur yra padidinta svarbių asmens duomenų praradimo rizika, pavyzdžiui didelės saugumo ekspertų kritikos sulaukęs RFID lustų panaudojimas JAV piliečių pasuose.

Nusikaltimai informatikai, kriminalizuoti Lietuvos Respublikos Baudžiamojo kodekso XXX skyriuje iš esmės yra įvykdomi tiesioginiais kaltininko veiksmais vienaip ar kitaip paveikiant nusikaltimo dalyką. Tačiau manytina, kad nusikaltimo informatikai dalyką taip pat galima paveikti ir netiesioginiais kaltininko veiksmais, tai yra kai kaltininkas pasinaudodamas trečiaisiais nieko neįtariančiais asmenimis, pažeidžia kompiuterinių duomenų ar informacinės

struktūros vientisumą, prieinamumą. Paradoksalu yra tai, kad trečiųjų asmenų kiekvieno atskirai veiksmai gali ir nesudaryti nusikalstamos veikos. Panagrinėkime realų[93] pavyzdį: piktavalis vedinas tam tikrų tikslų, turėdamas viešą priėjimą prie populiarių naujienų grupių (pvz. - useNet), patalpina vienoje iš jų atviras pornografines nuotraukas ir prideda užrašą „parašyk man elektroninį laišką ir aš patalpinsiu arba atsiūsiu dar daugiau tokių nuotraukų“. Atgalinį adresą jis nurodo aukos elektroninio pašto adresą. Kaip reakcija į patalpintą pranešimą aukos elektroninio pašto dėžutę užplūsta tūkstančiai elektroninių laiškų, kurių turinys gali svyruoti nuo paprasčiausio prašymo, grasinimo susidoroti iki pridėtų prie žinutės virusų ar kitokių kenksmingų kompiuterinių programų, bei daugybės kitų nepageidaujamų laiškų - pornografinio spamo. Tokiu būdu sutrikdomas ne tik aukos normalus naudojimasis kompiuterine informacija, bet ir sutrikdomas elektroninio pašto paslaugos tiekėjo kompiuterinės sistemos darbas. Vienintelė išeitis elektroninio pašto adreso pakeitimas ir žinučių, ateinančių senuoju adresu užblokavimas. Tačiau vėl gi tai gali būti susiję su papildomomis išlaidomis jeigu elektroninio pašto adresas buvo išspausdintas vizitinėse kortelėse, įmonės kataloguose ir panašiai. Taigi, kaip matome sisteminė individualių naujienų grupių skaitytojų reakcija į patalpintą žinutę gali sukelti didelius neigiamus padarinius tiek aukai, tiek ir tretiesiems asmenims. Nors individuali elektroninio pašto žinutė ir buvo pasiusta be jokio pikto kėslo ar žinojimo, kad asmuo iš esmės dalyvauja nusikalstamoje veikloje – paskirstytoje atsisakymo aptarnauti atakoje (*angl. – distributed denial of service*). Šis pavyzdys parodo, kad asmuo įdėdamas minimalias pastangas, pasinaudodamas minimaliomis priemonėmis ir informacinių technologijų žiniomis, bei netiesiogiai, o „kitų žmonių rankomis“ gali įvykdyti nusikalstamą veiklą – nusikaltimą informatikai.

Atsižvelgiant į tai, kas aukščiau išdėstyta galiu teigti, kad: **nusikaltimas informatikai – tai neteisėta veikla, kai tiesioginiais ar netiesioginiais veiksmais yra pažeidžiamas kompiuterinių duomenų ir/ar informacinės struktūros konfidencialumas, vientisumas ar prieinamumas, dėl ko kyla žala arba atsiranda žalos kilimo grėsmė teisėtiems interesams naudojant kompiuterinę informaciją.**

Nusikaltimų informatikai sampratos problemą sudaro, autoriaus nuomone, ne tiek vieningos teisinės nuomonės nebuvimas, kiek greitas ir dinamiškas nusikaltimų įvykdymo terpės kitimas neleidžia suformuluoti absoliučios nusikaltimų informatikai sampratos. Dėl to nusikaltimų informatikai sampratos problema liks aktuali visuomet, o sprendimas turėtų apsiriboti tik sampratos koregavimu ir pritaikymu esamam laikotarpiui. Todėl, manytina, kad

[93] Roebuck T. A. The DoS Attack and The DDoS Attack // http://www.crime-research.org/articles/network-security-dos-ddos-attacks/ (prisijungimo laikas: 2006-12-09). Pavyzdyje remtasi šiuo straipsniu.

autoriaus pateikta nusikaltimų informatikai samprata tik atspindi nūdienos teisines realijas, bet neišsprendžia pačios problemos.

4. GALIMA NUSIKALTIMŲ INFORMATIKAI SAMPRATOS ĮTAKA KAI KURIŲ NUSIKALTIMŲ INFORMATIKAI TEISINIAM REGULIAVIMUI LIETUVOJE

Svarstant kokia galima pateiktos nusikaltimų informatikai sampratos įtaka gali būti teisiniams nusikaltimų informatikai reguliavimui pirmiausia reikėtų paminėti Lietuvos Respublikos Baudžiamojo kodekso 198 straipsnį „Kompiuterinės informacijos pasisavinimas ir skleidimas“. Straipsnyje aprašyta nusikalstama veikla sukelia daugiau klausimų, negu duoda atsakymų. Daugiausia prieštaravimų sukelia kompiuterinės informacijos *pasisavinimas*. Pasisavinimo terminas visame Baudžiamajame kodekse yra sutinkamas tik 183 straipsnyje „Turto pasisavinimas“, 185 straipsnyje „Radinio pasisavinimas“, 263 straipsnyje „Narkotinių ar psichotropinių medžiagų vagystė, prievartavimas arba kitoks užvaldymas“ ir nagrinėjamame straipsnyje. Turto pasisavinimo atveju, pasisavinimas suprantamas kaip turto pavertimas savo nuosavybe, o kompiuterinių duomenų konfidencialumas, vientisumas ar prieinamumas, autoriaus manymu, niekaip neapima pasisavinimo sampratos. Taigi, galima teigti, kad pasisavinimo terminas yra labiau artimesnis turtiniams nusikaltimams. Pripažinus, kad pasisavinta kompiuterinė informacija tampa kaltininko nuosavybe kaip turtas, straipsnį reikėtų talpinti kitame Baudžiamojo kodekso skyriuje. Siuzan V. Brener (Susan W. Brenner) nusikaltimą kai kompiuterinė informacija pereina kaltininko nuosavybėn, vadina informacijos vagyste. Ji teigia, kad informacija yra nuosavybė (turtas). Todėl informacijos vagyste yra pripažįstami veiksmai, kai auka visiškai netenka informacijos, tai yra, kai informacijos valdymas yra perkeliamas iš teisėto savininko vagiui. Ji taip pat pripažįsta, kad informacijos vagystė tradicine prasme yra ir tuomet, kai informacija yra nukopijuojama, o originalas lieka pas teisėtą savininką. Kaip argumentą ji pateikia, kad kaltininkas tokiais veiksmais sumenkina informacijos vertę, dėl ko padaro turtinę žalą savininkui.[94] Tačiau, greičiausiai dėl teisinės sistemos skirtumų, Lietuvoje „labai svarbu yra laikytis nuostatos, kad vagystės ... dalyku gali būti tik materialus judamas turtas“.[95] Taigi, kompiuterinės informacijos pasisavinimo mes negalime pripažinti vagyste, taip pat ir į turto pasisavinimo sudėtį ši veika nepatenka. Autoriaus manymu, neatspindi 198 straipsnyje numatyta veika ir tikros nusikaltimų informatikai esmės ir daugeliu atveju gali būti painiojama su turtinais nusikaltimais. Atsižvelgiant į tai, manytina, kad aptariamas straipsnis turėtų būti koreguotinas eliminuojant pasisavinimo elementą. Vietoj jo, pavyzdžiui, galėtų būti panaudotas *perėmimo* terminas.

[94] Brenner S. W. Is There Such a Thing as “Virtual Crime”? ¶45, ¶47 // http://www.boalt.org/CCLR/v4/v4brenner.htm (prisijungimo laikas: 2006-05-10).
[95] Fedosiuk O. Turtinė nauda kaip nusikalstamos veikos dalykas: sisteminė normų analizė. // Jurisprudencija, 2004, T.60(52); P. 84.

Kita galima įtaka nusikaltimų informatikai reguliavime, autoriaus manymu, turėtų pasireikšti nusikaltimo dalyko koregavimu remiantis pateikta nusikaltimų informatikai samprata.

Siūlytina, atsižvelgiant suformuluotą nusikaltimų informatikai sampratą, straipsnyje, nustatančiame atsakomybę už kompiuterinės informacijos sunaikinimą ar pakeitimą, įvesti netiesioginio pažeidimo požymį. Tai galėtų būti įgyvendinta, pavyzdžiui, taip: …įrenginiais, kompiuterinėmis programomis ar *kitaip* apribojo naudojimąsi tokia informacija.

Taip pat, autoriaus manymu, būtų tikslinga remiantis išdėstytu III darbo dalyje, apjungti kompiuterinės informacijos sugadinimą ar pasisavinimą ir kompiuterinės programos sugadinimą ir pasisavinimą į vieną straipsnį, nes iš esmės sudaro vieno nusikaltimo požymius, o atskirai šie nusikaltimai informatikai dubliuoja vienas kitą.

Apibendrinant galima teigti, kad aukščiau suformuluota nusikaltimo informatikai samprata, nors ir neatnešanti didelių naujovių, tačiau galinti įtakoti nusikaltimų informatikai reglamentavimą Lietuvoje, priartinant juos prie šių dienų realijų.

IŠVADOS IR PASIŪLYMAI

Išnagrinėjus nusikaltimų informatikai sampratos esminius požymius, nusikaltimų informatikai ir panašių nusikaltimų sampratas teisinėje literatūroje, išanalizavus Lietuvos Respublikos Baudžiamojo kodekso XXX skyriuje numatytas nusikalstamas veikas nusikaltimų informatikai kontekste, pateikus mūsų suformuluotą nusikaltimų informatikai sampratą, autoriaus nuomone padėsiančią spręsti nusikaltimų informatikai sampratos problemą, bei pateiktos sampratos galimą įtaką nusikaltimų informatikai reguliavimui Lietuvoje galime daryti tokias išvadas:

1. Teisinėje literatūroje iki galo nėra susiformavusi vieninga nuomonė nusikaltimų informatikai objekto atžvilgiu. Vieni autoriai teigia, kad nusikaltimų informatikai objektas yra santykiai, susiję su informacijos ir informacinių resursų saugiu kūrimu, saugojimu, naudojimu ir platinimu. Kitų nuomone nusikaltimų informatikai objektas yra informacija. Tačiau atsižvelgiant į išdėstytus argumentus galima teigti, kad priimtiniausia nuomonė nusikaltimų informatikai objektu įvardijanti visuomeninius santykius, susijusius su kompiuterinės informacijos saugumu.

2. Nuomonė, kad nusikaltimų informatikai dalykas yra kompiuterinė informacija neatskleidžia tikrosios nusikaltimų informatikai esmės. Dėl kompiuterinės informacijos savybės ne visuomet kisti pasikeitus kompiuteriniams duomenims, mūsų manymu tiksliau būtų nusikaltimų informatikai dalyku pripažinti kompiuterinius duomenis.

3. Iki šiol nėra susiformavusios vieningos nuomonės dėl nusikaltimų informatikai sampratos. Teisinėje literatūroje tebevyrauja kompiuterinių nusikaltimų sampratos tiek siaurąją (atitinka nusikaltimų informatikai sampratą) tiek plačiąja prasmėmis. Rusijos ir Ukrainos teisininkai laikosi daugiau kompiuterinių nusikaltimų sampratos siaurąją prasme. Kitų šalių teisėje kompiuteriniai nusikaltimai suprantami išplėstai ir apima ne tik nusikaltimus informatikai, bet ir kitus nusikaltimus.

4. Nusikaltimai, numatyti Lietuvos Respublikos Baudžiamojo kodekso XXX skyriuje tik iš dalies atitinka nusikaltimų informatikai sampratą:

a) nusikaltimas, numatytas BK 197 straipsnyje „Kompiuterinės programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas“ savo dalimi, kurioje kalbama apie kompiuterinės programos neteisėtą sunaikinimą, sugadinimą, pašalinimą ar kitokį pakeitimą dubliuoja nusikalstamą veiklą, numatytą BK 196 straipsnyje „Kompiuterinės informacijos sunaikinimas ar pakeitimas“;

b) BK 197 straipsnyje nepakankamai nustatyta kompiuterinės programos apsauga, tai yra nėra apsaugomas jos prieinamumas;

c) BK 198 straipsnyje „Kompiuterinės informacijos pasisavinimas ir skleidimas“ vartojamas terminas *pasisavinimas* daugiau būdingas nusikaltimams nuosavybei, turtinėms teisėms ir turtiniams interesams;

d) nusikaltimų dalykas kompiuterinė informacija, numatytas skyriaus nusikaltimų sudėtyse, nepilnai atspindi nusikaltimų informatikai esmę dėl kompiuterinės informacijos savybės ne visuomet kisti pakeitus ją sudarančius kompiuterinius duomenis;

5. Nusikaltimų informatikai sampratos problemą sudaro ne tiek vieningos teisinės nuomonės nebuvimas, kiek greitas ir dinamiškas nusikaltimų įvykdymo terpės kitimas. Todėl nusikaltimų informatikai sampratos problema liks aktuali visuomet, o sprendimas turėtų apsiriboti tik sampratos koregavimu ir pritaikymu esamam laikotarpiui.

Pasiūlymai:

1. kadangi, nusikaltimas, numatytas BK 197 straipsnyje „Kompiuterinės programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas“ savo dalimi, kurioje kalbama apie kompiuterinės programos neteisėtą sunaikinimą, sugadinimą, pašalinimą ar kitokį pakeitimą dubliuoja nusikalstamą veiklą, numatytą BK 196 straipsnyje „Kompiuterinės informacijos sunaikinimas ar pakeitimas“, siūloma apjungti BK 197 straipsnį ta apimti, kuri numato kompiuterinės programos apsaugą su BK 196 straipsniu, tokiu būdu išsprendžiant ir nepakankamą kompiuterinių programų apsaugą;

2. kadangi, BK 198 straipsnyje „Kompiuterinės informacijos pasisavinimas ir skleidimas“ vartojamas terminas *pasisavinimas* daugiau būdingas nusikaltimams nuosavybei, turtinėms teisėms ir turtiniams interesams, siūloma Eliminuoti iš 198 straipsnio *pasisavinimo* požymį, pakeičiant jį, pavyzdžiui, *perėmimo* požymiu;

3. kadangi, nusikaltimų dalykas kompiuterinė informacija, numatytas skyriaus nusikaltimų sudėtyse, nepilnai atspindi nusikaltimų informatikai esmę dėl kompiuterinės informacijos savybės ne visuomet kisti pakeitus ją sudarančius kompiuterinius duomenis, siūloma pakeisti Baudžiamojo kodekso XXX skyriuje numatytų nusikaltimų sudėtis ir nusikaltimo dalyku vietoj kompiuterinės informacijos įvardinti kompiuterinius duomenis.

LITERATŪROS SĄRAŠAS

1. Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas // Valstybės žinios. 1999, Nr. 50-1598.
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // http://www3.lrs.lt/cgi-bin/preps2?Condition1=231799&Condition2=, (prisijungimo laikas: 2005-11-09).
3. Lietuvos Respublikos bankų įstatymas.// http://www3.lrs.lt/cgi-bin/preps2?Condition1=259449&Condition2=, (prisijungimo laikas: 2005-11-09).
4. Lietuvos Respublikos baudžiamasis kodeksas // Valstybės žinios. 2000, Nr. 89-2741
5. Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymas // Valstybės žinios. 2004, Nr. 25-760.
6. Lietuvos Respublikos civilinis kodeksas // Valstybės žinios. 2000, Nr. 74-2262.
7. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas // http://www3.lrs.lt/cgi-bin/preps2?Condition1=238376&Condition2= , (prisijungimo laikas: 2005-11-09).
8. Lietuvos Respublikos Seimo Teisės ir teisėtvarkos komiteto išvada Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymo projektui // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=224985 (prisijungimo laikas: 2006-10-29).
9. Konvencija dėl elektroninių nusikaltimų // Valstybės žinios.2004, Nr. 36-1188.
10. 2005 m. vasario 24 d. Tarybos pamatinis sprendimas 2005/222/TVR, dėl atakų prieš informacines sistemas // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:LT:NOT (prisijungimo laikas: 2006-08-22).
11. Australian Criminal code act 1995 // http://www.comlaw.gov.au/ComLaw/Management.nsf/current/bytitle/8F20DA53B8CF2FAFCA256F7100071F90?OpenDocument&VIEW=compilations (prisijungimo laikas: 2006-09-05).
12. Texas penal code // http://tlo2.tlc.state.tx.us/statutes/petoc.html (prisijungimo laikas: 2006-09-01).
13. Lietuvos Respublikos elektroninio parašo įstatymas // http://www3.lrs.lt/cgi-bin/preps2?Condition1=169880&Condition2=, (prisijungimo laikas: 2005-11-09).

14. Федеральный закон "Об информации, информатизации и защите информации" от 20 февраля 1995 г. N 24-ФЗ (с изменениями от 10 января 2003 г.) Принят Государственной Думой 25 января 1995 года. 2 str. // http://www.minsvyaz.ru/site.shtml?id=1066 (prisijungimo laikas: 2005-11-09).
15. Abramavičius A., Čepas A., Drakšienė A. ir kt. Baudžiamoji teisė: bendroji dalis. – Vilnius: Eugrimas, 1998.
16. Civilka M., Lamanauskas T., Osinaitė G. ir kt./red. D. Sauliūnas. Informacinių technologijų teisė. - Vilnius: NVO Teisės Institutas, 2004.
17. Dzemydienė D., Naujikienė R. Informacinės sistemos. Duomenų struktūros ir valdymas. – Vilnius: Lietuvos teisės universitetas, 2004.
18. Fedosiuk O. Turtinė nauda kaip nusikalstamos veikos dalykas: sisteminė normų analizė. // Jurisprudencija, 2004, T.60(52).
19. Janiūnienė E. Biblioteka - žinių institucija // Informacijos mokslai, 2001. T.17. http://www.leidykla.vu.lt/inetleid/inf-mok/17/tomas17.html (prisijungimo laikas: 2005-10-20).
20. Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. - Vilnius: LTU, 2000. P.5-6.
21. Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai // Jurisprudencija 2003, 47 (39).
22. Brenner S. W. Is There Such a Thing as “Virtual Crime”? // http://www.boalt.org/CCLR/v4/v4brenner.htm (prisijungimo laikas: 2006-05-10).
23. Carter D.L. Computer crime categories: how techno-criminals operate // http://www.lectlaw.com/files/cri14.htm (prisijungimo laikas: 2006-09-22).
24. Convention on cybercrime explanatory report.// http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (prisijungimo laikas: 2006-11-11).
25. Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Informatikon // http://www.mcconnellinternational.com/services/cybercrime.htm (prisijungimo laikas: 2005-10-10).
26. Goodman M. Making computer crime count // FBI Law Enforcement Bulletin,The:. 2001. http://www.findarticles.com/p/articles/mi_m2194/is_8_70/ai_78413303 (prisijungimo laikas: 2005-10-25).
27. Grabosky P.N. Virtual Criminality: Old Wine In New Bottles? // Social & Legal Studies. 2001.

28. Immunizing the Internet, or: how I learned to stop worrying and love the worm // Harvard Law Review Vol. 119 – June 2006 – Nr. 8. http://www.harvardlawreview.org/issues/119/june06/june06.shtml (prisijungimo laikas: 2006-11-30).
29. Krone T. Concepts and terms // High Tech Crime Brief. ISSN 1832-3413. 2005. http://www.aic.gov.au/publications/htcb/htcb001.html (prisijungimo laikas: 2006-09-02).
30. Rasch M. D. Criminal law and the internet. // This is one of eleven chapters contained in The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, published by the Computer Law Association. http://www.sgrm.com/art14.htm (prisijungimo laikas: 2004-06-13).
31. Roebuck T. A. The DoS Attack and The DDoS Attack // http://www.crime-research.org/articles/network-security-dos-ddos-attacks/ (prisijungimo laikas: 2006-12-09).
32. Schjølberg S. & Hubbard A.M. Harmonizing national legal approaches on cybercrime // WSIS thematic meeting on cybersecurity. Geneva, 28 June – 1 July, 2005.
33. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (prisijungimo laikas: 2006-10-10).
34. Sieber U. Legal aspects of computer-related crime in the information society – comcrime study -// 1998. http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc (prisijungimo laikas: 2005-09-10).
35. Taipale K.A. Cybercrime, Cyberterrorism, and Digital law enforcement // http://cybercrime.advancedstudies.org (prisijungimo laikas: 2006-11-18).
36. Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации // http://pu.boom.ru/book/index.html (prisijungimo laikas: 2006-11-10).
37. Важенин А.Г. Интернет и преступность: криминологические и правовые аспекты взаимосвязи. // http://www.crime.vl.ru/docs/stats/stat_197.htm (prisijungimo laikas: 2006-05-30).
38. Вехов В.Б. Компьютерные преступления: способы совершения, методика расследования. – Москва: Право и закон, 1996.
39. Гаврилин Ю.В., Пушкин А.В., Соцков Е.А. и др. Расследование неправомерного доступа к компьютерной информации. Учебное пособие. Изд-е второе, дополненное и переработанное / Под ред. д.ю.н. проф. Н.Г. Шурухнова. – Москва: Московский университет МВД России, 2004.

40. Голубев В. Компьютерная информация, как объект правоотношений // http://www.crime-research.ru/library/Golubev09_03.html (prisijungimo laikas: 2005-09-27).
41. Голубев В. Уголовно-правовые аспекты противодействия преступности в сфере использования электронно-вычислительных машин // http://www.crime-research.ru/library/Golubev1003.html (prisijungimo laikas: 2006-11-08).
42. Гостев А. Современные информационные угрозы, III квартал 2006 // http://www.crime-research.ru/articles/art15/ (prisijungimo laikas: 2006-11-20).
43. Карелина М.М. Преступления в сфере компьютерной информации // http://www.relcom.ru/Archive/1997/ComputerLaw/New_code.htm (prisijungimo laikas: 2006-11-10).
44. Карчевский Н.В. Компьютерные преступления: определение, объект и предмет // Доклад на V Международной конференции «Право и интернет: теория и практика»
45. http://www.ifap.ru/pi/05/karchev.htm (prisijungimo laikas: 2006-10-15).
46. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность //Юридический мир, Февраль 1998.
47. Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. // Уголовное право, 1998. №3.
48. Крылов В.В. Расследование преступлений в сфере информации. – Москва: Издательство «Городец», 1998.
49. Мелик Э. Компьютерные преступления // http://melik.narod.ru/index.html (prisijungimo laikas: 2004-09-18).
50. Пархомов В.А. К определению понятия "Информационное преступление" // Вестник ИГЭА, 2001. № 2. http://www.etasu.isea.ru/attorn/s5.htm (prisijungimo laikas: 2005-09-05).
51. Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева, А.В. Наумова. – Москва: Юристъ, 1997.
52. Dabartinės lietuvių kalbos žodynas. Interneto versija // http://www.autoinfa.lt/webdic/ (prisijungimo laikas: 2006-11-02).
53. Kompiuterinės leksikos aiškinamasis žodynas // http://aldona.mii.lt/pms/terminai/term/z2odynas.html (prisijungimo laikas: 2005-11-09).
54. Microsoft Lietuva // http://www.microsoft.com/lietuva/security/home/antivirus/virus101.mspx (prisijungimo laikas: 2006-11-12).

NUSIKALTIMŲ INFORMATIKAI SAMPRATOS PROBLEMA
SANTRAUKA

Pagrindinės sąvokos: nusikaltimų informatikai samprata, kompiuteriniai nusikaltimai, nusikaltimo informatikai objektas, nusikaltimo informatikai dalykas, kompiuterinė informacija, kompiuteriniai duomenys.

Darbe nagrinėjama nusikaltimų informatikai samprata, jos esminiai požymiai, analizuojamos vyraujančios nusikaltimų informatikai sampratos teisinėje literatūroje. Taip pat nagrinėjami nusikaltimai, numatyti Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje „Nusikaltimai informatikai“ nusikaltimų informatikai sampratos kontekste. Darbe autorius pateikia, jo požiūriu, priimtiniausią nusikaltimų informatikai sampratą ir nagrinėja šios sampratos galimą įtaką nusikaltimų informatikai reguliavimui Lietuvoje.

Darbe analizuojami nusikaltimų informatikai požymiai, iš kurių didesnes diskusijas sukelia nusikaltimo informatikai objektas ir dalykas. Vieni autoriai teigia, kad nusikaltimų informatikai objektas yra santykiai, susiję su informacijos ir informacijos resursų saugiu kūrimu, naudojimu ir platinimu, kitų nuomone nusikaltimų informatikai objektas yra informacija. Tačiau darbe autorius nepritaria tokiam požiūriui ir mano, kad priimtiniausia nuomonė dėl nusikaltimo informatikai objekto, apibūdinanti kaip visuomeninius santykius, susijusius su kompiuterinės informacijos saugumu. Autorius pateikia nuomonę, kad nusikaltimų informatikai dalykas kompiuterinė informacija dėl savo savybės nekisti pakitus ją sudarantiems kompiuteriniams duomenims ne visuomet atspindi nusikaltimų informatikai esmę. Dėl to, manytina, kad nusikaltimų informatikai dalyku turėtų būti įvardinti kompiuteriniai duomenys.

Autorius darbe analizuoja vyraujančias nusikaltimų informatikai sampratas kitų šalių, tame tarpe ir Rusijos bei Ukrainos teisinėje literatūroje. Darbe prieinama prie išvados, kad teisinėje literatūroje tebevyrauja kompiuterinių nusikaltimų sampratos siaurąja (būdinga Rusijos ir Ukrainos šalims) ir plačiąją prasmėmis (būdinga kitų užsienio šalių teisei).

Darbe taip pat nagrinėti Lietuvos Respublikos Baudžiamojo kodekso XXX skyriuje numatyti nusikaltimai nusikaltimų informatikai sampratos kontekste, jų atitikimas nusikaltimų

informatikai teisinei sampratai. Buvo padaryta išvada, kad XXX skyriuje aprašyti nusikaltimai tik iš dalies atitinka nusikaltimų informatikai sampratą.

Autorius mano, kad nusikaltimų informatikai sampratos problemą sudaro ne tiek vieningos teisinės nuomonės nebuvimas, kiek greitas ir dinamiškas nusikaltimų įvykdymo terpės kitimas. Todėl nusikaltimų informatikai sampratos problema liks aktuali, o pačios problemos sprendimas turėtų apsiriboti tik sampratos koregavimu ir pritaikymu esamam laikotarpiui. Autorius suformuluoja jo požiūriu, atsižvelgiant į darbe nagrinėtą medžiagą, esamam laikotarpiui priimtiniausią nusikaltimų informatikai sampratą ir išnagrinėja jos galimą įtaką nusikaltimų informatikai reguliavimui Lietuvoje.

THE PROBLEM OF THE CONCEPTION OF CRIMES AGAINST INFORMATICS

SUMMARY

Keywords*: conception of crimes against informatics, computer crimes, object of crimes against informatics, subject of crimes against informatics, computer information, computer data.*

The main topics were found out during this study are: the conception of crimes against informatics, the main indications and analyzing of conception of crimes against informatics according the law literature. The criminal activities named in Chapter XXX of Criminal Code of the Republic of Lithuania are also described in this study. According the author point of view, we proposes the most attractive conception of crimes against informatics and researching possible influence on regulation of such crimes type in Republic of Lithuania of it.

In this study the author analyzed indications of crime against informatics. The main causes of discussion are crime against informatics object and subject. There are different opinions about it. One of these opinions suggests that the object of that kind of crime is relationships, which are related to safe creation, use and broadcasting of information and information resources. Another opinion – object is information. The author of this study is disagree with such opinions and supposes that the most suitable opinion of conception of object have to describe the social relationships, related to security of computer information. He thinks that the subject of crime against informatics, computer information because of it feature to stay unchangeable even if computer data has been changed, inadequate the crime substance. The author suggests that the subject of crime against informatics is computer data.

The author analyzes different conceptions of crimes against informatics which are use in foreign countries, including Russian Federation and Ukraine law literature. During the research of present situation, we found out, that in the proper and broader concept of computer crime definitions in law literature is still in use.

The criminal activities named in Chapter XXX of Criminal Code of the Republic of Lithuania are also described in this study in context of the conception of crime against informatics. The author made a final conclusion that criminal activities named in Criminal Code are partly on the same way with it.

The problem of the conception of crime against informatics is not only in solid law opinion non existence. The main reason is changeable crime medium. It will be relevant. The solving of the problem has to be limited by the definition correction and adoption to the present legal state. The author proposes the most suitable conception of crime against information and

researching possible conception influence on regulation of such crimes type in Republic of Lithuania.