MYKOLO ROMERIO UNIVERSITETO
TEISĖS FAKULTETO
BAUDŽIAMOSIOS TEISĖS KATEDRA

ASTA BENETYTĖ
(BAUDŽIAMOJI TEISĖ IR KRIMINOLOGIJA, 62401S111)

NUSIKALTIMŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI SAMPRATA IR BAUDŽIAMOJI ATSAKOMYBĖ UŽ JUOS. PROBLEMOS PAGAL LIETUVOS RESPUBLIKOS BAUDŽIAMĄJĮ KODEKSĄ

Magistro baigiamasis darbas

Darbo vadovas –
lekt. R. Marcinauskaitė

Konsultantas –
doc. dr. A. Gutauskas

Vilnius, 2008

TURINYS

ĮVADAS

2001 m. rugpjūčio 10 d. Lietuvos Respublikos Vyriausybės nutarime Nr. 984 „Dėl Lietuvos informacinės visuomenės plėtros strateginio plano patvirtinimo“ numatyta, jog informacinė visuomenė – atvira, išsilavinusi, nuolat besimokanti ir žiniomis savo veiklą grindžianti visuomenė, kurios nariai – paprasti Lietuvos gyventojai ir visų lygių vadovai – gali, moka ir nori visose savo veiklos srityse efektyviai taikyti šiuolaikinių informacinių technologijų priemones, naudotis savo šalies ir viso pasaulio kompiuterizuotais informacijos ištekliais, o valstybės ir savivaldos institucijos, įstaigos, pasitelkdamos šias priemones ir išteklius, priimti sprendimus, užtikrinti gyventojams prieinamą ir patikimą viešąją informaciją. Kuriant tokią informacinę visuomenę, šiuolaikinės informacinės technologijos plinta visose žmogaus veiklos srityse, todėl neišvengiamai informacinės technologijos yra naudojamos ne tik teisėtiems tikslams. Informacinės sistemos ir elektroniniai duomenys gali būti naudojami daryti baudžiamajame įstatyme numatytoms nusikalstamoms veikoms bei sudaryti naujas galimybes įvykdyti veikas, iki tol nežinomas teisinėje praktikoje.

Temos aktualumas. Pasirinktos temos „Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui samprata ir baudžiamoji atsakomybė už juos. Problemos pagal Lietuvos Respublikos baudžiamąjį kodeksą“ aktualumą lemia keletas aplinkybių. Pirma, nors nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui sudaro labai nedidelę bendrojo nusikalstamumo dalį, tačiau jų reikšmę tarp kitų nusikalstamų veikų lemia ypatingos baudžiamojo įstatymo saugomos vertybės (elektroninių duomenų ir informacinių sistemų saugumas) bei jomis padaroma didelė žala. Nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui padaroma žala ne tik elektroninių duomenų ir informacinių sistemų saugumui, bet tokių veikų padariniai gali pasiekti artimą nukentėjusiojo aplinką (pavyzdžiui, kaltininkas neteisėtai perėmė ir paskleidė elektroninius duomenis apie jo pažįstamo asmens vieno iš šeimos narių nepagydomą ligą), o tam tikrais atvejais ir valstybės valdymo, finansų, ūkio sistemas, strateginę reikšmę nacionaliniam saugumui turinčius objektus. Tai formuoja visuomenės, o kartu ir kiekvieno joje esančio individo, nesaugumo jausmą, naudojantis informacinių technologijų priemonėmis.

Antra, nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui yra ypač pavojingos tuo, kad oficiali teisėsaugos institucijų statistika neatskleidžia tikrosios padėties. 85 – 97 % tokių nusikalstamų veikų net neiškyla į viešumą, o iš tų, kurios iškyla, išaiškinamumo procentas neviršija net 40 %.[1] Tik 5 % nukentėjusiųjų nuo nusikalstamų veikų elektroninių

[1] Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Nusikalstamumas ir teisėsaugos institucijų veikla 2007. - Vilnius, 2008. P. 45.

duomenų ir informacinių sistemų saugumui oficialiai kreipėsi į teisėsaugos institucijas.[2] Trečia, didelis šių nusikalstamų veikų latentiškumas reikalauja milžiniškų laiko ir lėšų sąnaudų, siekiant visapusiškai išsiaiškinti tokias nusikalstamas veikas.

Ketvirta, nors fiziniai asmenys, padarę nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, *de lege lata* yra traukiami baudžiamojon atsakomybėn, tačiau *de lege ferenda* tai padaryti yra nelengva, kadangi Lietuvoje beveik nėra išsamios baudžiamosios teisinės doktrinos ir teismų praktikos, kuria būtų galima remtis, aiškinant ir taikant baudžiamojo įstatymo normas, nustatančias baudžiamosios atsakomybės už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui prielaidas. Todėl, mūsų manymu, viena iš aktualiausių Lietuvos baudžiamosios teisės teorijos ir praktinių temų ir yra konceptuali baudžiamosios atsakomybės už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui analizė.

Informacinių technologijų spartus vystymasis atskleidžia nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui itin aiškų ir detaliai sureglamentuotų baudžiamosios atsakomybės sąlygų būtinumą. Baudžiamoji atsakomybė už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui numatyta Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) XXX skyriuje esančiuose 196 – 198[2] straipsniuose, įtvirtinančiuose skirtingas nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtis, kurios ir yra asmens baudžiamosios atsakomybės pagrindas. Šiame tiriamajame darbe bus nagrinėjami nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui objektyvieji ir subjektyvieji požymiai, pagal kokius požymius šios veikos atribojamos nuo kitų nusikalstamų veikų, kokios kyla nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kvalifikavimo problemos. Dėl ribotos šio darbo apimties nagrinėjama tik fizinių asmenų baudžiamoji atsakomybė už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, neanalizuojant juridinių asmenų atsakomybės už šias nusikalstamas veikas. Tarptautiniai teisės aktai, reglamentuojantys baudžiamosios atsakomybės nustatymą ir taikymą už šias nusikalstamas veikas, taip pat detaliai nenagrinėjami, o apžvelgiami tik BK XXX skyriuje įtvirtintų nusikalstamų veikų sudėčių suderinamumo su jais aspektu. Šalia teorinių aspektų bus nagrinėjama ir teismų praktika, siekiant atskleisti BK XXX skyriuje numatytų straipsnių taikymą ir aiškinimą, nagrinėjant baudžiamąsias bylas dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui.

Tyrimo objektas – fizinių asmenų padaromos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui bei baudžiamoji atsakomybė už jas. **Tyrimo dalykas**

[2] Ten pat.

– nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtys kaip baudžiamosios atsakomybės pagrindas teoriniu aspektu ir teismų praktikoje.

Iškelta **hipotezė**, kad nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui teisinis reglamentavimas yra sudėtingas ir nepakankamas, keliantis teorinių ir praktinių problemų dėl tokių nusikalstamų veikų sampratos neaiškumo ir baudžiamųjų sąlygų už jas neišsamumo.

Tyrimo tikslas – atskleisti baudžiamosios atsakomybės už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui ypatumus, problemas ir pasitaikančias klaidas. Tikslui įgyvendinti numatyti tokie **uždaviniai**:

1. išanalizuoti mokslinę literatūrą, BK XXX skyriuje numatytus straipsnius ir teismų praktiką, susijusią su nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui samprata;

2. išnagrinėti BK XXX skyriuje ,,Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“ pateiktų nusikalstamų veikų sudėčių objektyviuosius ir subjektyviuosius požymius, atriboti nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui nuo kitų nusikalstamų veikų;

3. įvertinti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių trūkumus, išanalizuoti kvalifikavimo problemas;

4. įvertinti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kitimo tendencijas per 2004 - 2008-09-01[3] laikotarpį, jų santykį tiek su visomis užregistruotomis nusikalstamomis veikomis, tiek tarpusavio kiekybinius skirtumus;

Metodai: tiriamajame darbe naudoti lyginamasis, istorinis, sisteminės analizės, indukcinis – dedukcinis, loginis – analitinis ir kontent analizės metodai.

Lyginamuoju metodu buvo lyginamos įvairios mokslinės koncepcijos, baudžiamosios teisės ir kitų teisės šakų mokslininkų nuomonės. Istorinis metodas padėjo atskleisti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kriminalizavimo aktualumą, jų taikymo efektyvumą, trūkumus ir panašumus. Sisteminės analizės metodas leido nagrinėti tyrimo objektą kaip sistemos dalį ir baudžiamajame įstatyme įtvirtintų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtis ir kitas su baudžiamosios atsakomybės realizavimu susijusias nuostatas analizuoti kaip sistemą, atskleidžiant jos elementų tarpusavio ryšius. Indukcinis – dedukcinis metodas buvo taikomas, siekiant apibendrinti atskirų žinių duomenis, faktus bei formuluoti bendro pobūdžio teorines nuostatas, išvadas ir rekomendacijas. Loginiu – analitiniu metodu atskleidžiami nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui dispozicijų trūkumai ir kitos teisinio reglamentavimo problemos.

[3] Pateikiami duomenys per 2008 m. pirmus devynis mėnesius.

Kontent analizės metodu išanalizuota statistinė informacija[4] bei Lietuvos Respublikos teismų praktika[5], o tai atskleidžia pagrindines nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kvalifikavimo ir baudžiamosios atsakomybės už šias veikas realizavimo problemas.

Darbo struktūra. Darbą sudaro įvadas, 3 skyriai, išvados ir rekomendacijos, literatūros sąrašas, santrauka lietuvių ir anglų kalbomis.

[4] Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos statistika // http://www.vrm.lt/fileadmin/Image_Archive/IRD/Statistika/index2.phtml?id=198; prisijungimo laikas: 2008-09-15; Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Nusikalstamumas ir teisėsaugos institucijų veikla 2007. - Vilnius, 2008; Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Nusikalstamumas ir teisėsaugos institucijų veikla 2006. - Vilnius, 2007.

[5] Vilniaus miesto 1 apylinkės teismo, Vilniaus miesto 3 apylinkės teismo baudžiamosios bylos nuo 2003 m., kuriose buvo nagrinėjami nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui klausimai.

1. NUSIKALSTAMŲ VEIKŲ ELEKTRONINĖJE ERDVĖJE SAMPRATA BEI JŲ APIBRĖŽTUMO PROBLEMATIKA

1.1. Nusikalstamų veikų elektroninėje erdvėje doktrininė samprata ir jų apibrėžtumo problematika tarptautiniuose teisės aktuose

Tiek kontinentinės, tiek bendrosios teisės tradicijos šalių mokslinėje literatūroje yra minimos tokios sąvokos kaip „nusikalstama veika elektroninėje erdvėje“[6], „kompiuterinis nusikaltimas“[7], „nusikalstama veika, susijusi su kompiuteriais“[8]. Vieni mokslininkai šias sąvokas arba kai kurias iš jų tapatina (P. D. Bylenchuk, C. J. Magnin, I. Voronov), kiti – apibrėžia jas nevienodai (J. Bick, A. Graycar), nors bendrų požymių tikrai surasime. Taigi, kyla klausimas, ar šios sąvokos yra tapačios, ar jas reikia vartoti skirtingais atvejais ir skirtingose situacijose? Reikia pastebėti, kad jau keletą dešimtmečių vyksta diskusijos, rengiamos ne tik nacionalinio, bet ir tarptautinio lygmens konferencijos, seminarai, siekiant aptarti, išsiaiškinti ir surasti tinkamiausią kompiuterinio nusikaltimo definiciją, tačiau vieningo sutarimo ar tarptautiniu lygmeniu pripažįstamo šios sąvokos apibrėžimo vis dar nėra iki šiol.[9,10]

Jungtinių Amerikos Valstijų mokslininkas, vienas pirmųjų susidomėjęs šia problema, D. Parker kompiuterinio nusikaltimo sąvoką apibrėžė taip: „visos tyčinės veikos, vienaip ar kitaip susijusios su kompiuteriais, dėl kurių nukentėjusysis patyrė arba galėjo patirti žalą, o nusikalstamą veiką padaręs asmuo turėjo arba galėjo gauti iš to naudos”.[11] Manytina, kad ši sąvoka atitiko XX a. 7-ojo ir 8-ojo dešimtmečių poreikius, nes kompiuteriniu nusikaltimu buvo laikoma bet kokia nusikalstama veika, kuri yra tiesiogiai susijusi su kompiuteriu. Šiuo metu tokia definicija yra perteklinė, kadangi tiek kompiuterio vagystė, tiek neteisėtas elektroninių duomenų pasisavinimas patektų į tokios sampratos kompiuterinio nusikaltimo apibrėžimą.

Vokiečių mokslininkas D. von zur Muhlen mano, kad „kompiuterinis nusikaltimas yra baudžiamoji veika, kurios metu kompiuteris yra šios veikos instrumentas arba objektas”.[12] Jungtinių Amerikos Valstijų mokslinėje literatūroje pateikiamas toks kompiuterinio nusikaltimo apibrėžimas: „tai bet koks pažeidimas baudžiamosios teisės srityje, kuriam padaryti arba

[6] Bainbridge D. I. Introduction to Computer Law. - Harlow: Pearson, Longman, 2004. P. 194.
[7] Ten pat, P. 212.
[8] Civilka M. ir kt. Informacinių technologijų teisė. - Vilnius: NVO Teisės institutas, 2004. P. 258.
[9] Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study. http://law.scu.edu/international/File/Sieber_final.pdf; prisijungimo laikas: 2008-01-26.
[10] Wahlert G. Crime in Cyberspace: Trends in Computer Crime in Australia // Australian Institute of Criminology Conference „Internet Crime“. - Melbourne, 1998. http://www.aic.gov.au/conferences/internet/wahlert.pdf; prisijungimo laikas: 2007-12-07.
[11] Macdonald E., Rowland D. Information technology law. – London, 2005. P. 55.
[12] Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. - Vilnius: LTA Leidybos centras, 2000. P. 6.

išsiaiškinti panaudojamos informacinių technologijų žinios“.[13] Manytume, jog ši definicija taip pat yra perteklinė, nes į tokių nusikalstamų veikų ratą papuola ir tradicinės nusikalstamos veikos, kurioms išsiaiškinti naudojamos informacinių technologijų žinios. Rusijos Federacijos mokslininkai užima skirtingas pozicijas šiuo klausimu: vieni mano, kad tokios sąvokos kaip „kompiuteriniai nusikaltimai“ negali būti, nes tokiu principu tuomet reikėtų skirti ir kitas nusikalstamas veikas, pvz. peiliniai nužudymai (nužudymas, padarytas peiliu), kiti – jog tai yra nusikalstamos veikos, nukreiptos prieš kompiuterius.[14,15] Rusijos Federacijos baudžiamosios teisės daktaras M. Dutov kompiuterinio nusikaltimo sąvoką siaurina, teigdamas, kad tai yra tokios pavojingos veikos, kurių pasikėsinimo dalykas – kompiuterinė informacija, o saugomos vertybės – visuomeniniai santykiai, susiję su kompiuterine informacija.[16]

1983 m. Ekonominio bendradarbiavimo ir plėtros organizacija (OECD) sudarė ekspertų komitetą problemoms, susijusioms su pavojingomis veikomis elektroninėje erdvėje, spręsti, kuri pateikė tokį apibrėžimą - „bet koks neteisėtas, neetiškas arba nesankcionuotas elgesys, susijęs su automatiniu kompiuterinių duomenų apdorojimu ir siuntimu“.[17] Europos Tarybos Nusikaltimų tyrimo komitetas taipogi gvildeno diskusijas šia tema, tačiau, *a contrario*, nepateikė kompiuterinio nusikaltimo sąvokos, o tik suteikė tam tikrą laisvę valstybėms pačioms kriminalizuoti veikas šioje sferoje, atsižvelgiant į teisinės sistemos ypatumus, istorines tradicijas, kompiuterinį raštingumą, išsivystymą ir šios sferos veikų kriminalizavimo aktualumą.[18]

Dauguma mokslininkų, bandydami atskleisti nusikalstamų veikų elektroninėje erdvėje bei kompiuterinių nusikaltimų sąvokas, susidūrė su pernelyg plačios sampratos pateikimo problema, kas ir sąlygoja, jog šiomis nusikalstamomis veikomis gali būti laikoma labai didelė dalis nusikalstamų veikų, kuriose vienaip ar kitaip „figūruoja“ kompiuteris. Kaip matome, egzistuoja tam tikros problemos, dėl kurių yra sunku apibrėžti arba pateikti tikslią kompiuterinio nusikaltimo definiciją.

Manytume, jog baudžiamosios teisės požiūriu kompiuterinius nusikaltimus reikėtų suprasti kaip baudžiamojo įstatymo numatytas visuomenei pavojingas veikas, kurių saugomos vertybės – elektroninių duomenų ir informacinių sistemų saugumas, o dalykas – elektroniniai duomenys ir informacinės sistemos. Jau pati nusikalstamos veikos, susijusios su kompiuteriais,

---

[13] Hoffstadt B. M., Wong Yang D. Countering the Cyber-Crime Threat // American Criminal Law Review. 2006, Nr. 43(2). P. 78-80.

[14] Воронов Я. Понятие преступлений в сфере высоких технологий. http://www.crime-research.org/library/cyber pon.htm; prisijungimo laikas: 2007-11-09.

[15] Айков Д., Сейгер К. Компьютерные преступления: руководство по борьбе с компьютерными преступлениями. - Москва: Мир, 1999. P. 65.

[16] Дутов М. Ответственность за компьютерные преступления в Уголовном кодексе Украины. http://www.crime -research.org/library/dutov.htm; prisijungimo laikas: 2008-04-16.

[17] Sieber U. The International Handbook on Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy. – London: John Wiley & Sons Inc, 1996. P. 257.

[18] Convention on Cybercrime // http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; prisijungimo laikas: 2007-10-12.

sąvokos sintaksinė/gramatinė analizė suponuoja, jog nusikalstamą veiką, susijusią su kompiuteriais, turėtume suprasti plačiau nei kompiuterinį nusikaltimą. Socialinių mokslų daktaras D. Štitilis teigia, jog nusikalstamos veikos, susijusios su kompiuteriais, yra tokios baudžiamojo įstatymo numatytos visuomenei pavojingos veikos, kai nusikalstamos veikos dalykas – kompiuterinė informacija ir/arba kompiuteris panaudojamas kaip nusikalstamos veikos įvykdymo priemonė/būdas (plačioji samprata).[19] Tuomet nusikalstamos veikos, susijusios su kompiuteriais, saugomos vertybės gali būti ne tik elektroninių duomenų ir informacinių sistemų saugumas, bet ir nuosavybė, turtinės teisės ir turtiniai interesai, intelektinė ir pramoninė nuosavybė, asmens garbė ir orumas. Ši samprata atskleidžia būdų, įrankių ir pasikėsinimo į baudžiamojo įstatymo saugomų vertybių bendrumą.

Nusikalstamos veikos elektroninėje erdvėje sąvoka taip pat plačiai vartojama užsienio mokslininkų darbuose, tačiau vieningos sampratos, ką turėtume laikyti nusikalstama veika elektroninėje erdvėje taip pat nėra.[20] Jungtinių Amerikos Valstijų baudžiamosios teisės srityje praktikuojantis advokatas T. R. Broderick mano, kad nusikalstama veika elektroninėje erdvėje reikėtų laikyti visus pavojingus veiksmus, kurie susiję su įsikišimu į kompiuterinius tinklus/sistemas, pvz. žalingo turinio informacijos publikavimas internete, intelektinės ir pramoninės nuosavybės pažeidimai.[21] Jungtinių Amerikos Valstijų profesorius, specializuojantis informacinių technologijų ir interneto teisėje, J. Bick teigia, kad nusikalstamos veikos elektroninėje erdvėje yra visos pavojingos veikos, kurios įvykdomos internetu.[22]

Tačiau mokslinėje literatūroje daugiau kalbama apie nusikalstamų veikų elektroninėje erdvėje klasifikaciją nei apie pačią šių nusikalstamų veikų sampratą. Rusijos Federacijos ir Ukrainos šalių mokslininkai nusikalstamas veikas elektroninėje erdvėje skirsto į vidines nusikalstamas veikas, kurias padaro tam tikros įstaigos darbuotojai, ir išorines nusikalstamas veikas, kurios įvykdomos iš išorės, panaudojant nutolusias atakas.[23,24] Tokia klasifikacija - galima, tačiau ji neatskleidžia nusikalstamų veikų elektroninėje erdvėje esmės ir rūšių. Konvencija dėl elektroninių nusikaltimų, ją ratifikavusioms šalims (Albanija, Estija, Italija, Jungtinės Amerikos Valstijos, Latvija, Lietuva, Prancūzija, Suomija ir kt.) įsigaliojusi nuo 2004 m. liepos 1 d., pateikia tokią nusikalstamų veikų elektroninėje erdvėje klasifikaciją:

[19] Štitilis D. Neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimas // Informacijos mokslas. 2003, Nr. 26. P. 32.
[20] Ku R. S. R. ir kt. Cyberspace Law: Cases and Materials. - New York: Aspen law & Business, 2002. P. 142.
[21] Broderick T. R. Regulation of Information Technology in the European Union. - London: Springer, 2000. P. 79.
[22] Charney S., Alexander K. Computer Crime. http://www.crime-research.org/library/Alex.htm ; prisijungimo laikas: 2008-07-12.
[23] Мандиа К., Просис К. Защита от вторжений: расследование компьютерных преступлений. - Москва: Лори, 2005. P. 37.
[24] Hutchinson W., Warren M. Attitudes of Australian Information System Managers against Online Attackers // Information Management & Computer Security. 2001, Nr. 9/3. P. 108.

- nusikalstamos veikos, pažeidžiančios kompiuterinės informacijos ir kompiuterinių sistemų vientisumą, prieinamumą, saugumą (neteisėtas perėmimas, neteisėta prieiga, įsikišimas į kompiuterinės sistemos darbą);

- nusikalstamos veikos, susijusios su kompiuterių panaudojimu (sukčiavimas, panaudojant kompiuterį);

- nusikalstamos veikos, susijusios su turiniu (pornografinės medžiagos platinimas);

- nusikalstamos veikos, susijusios su autorių ir gretutinėmis teisėmis.[25,26]

Tokia nusikalstamų veikų elektroninėje erdvėje klasifikacija leidžia daryti išvadą bei kai kurie mokslininkai (C. J. Magnin, G. Wahlert) teigia, kad tiek nusikalstamos veikos elektroninėje erdvėje, tiek nusikalstamos veikos, susijusios su kompiuteriais, yra tapačios sąvokos ir skirtumų tarp jų beveik nėra.[27] Socialinių mokslų daktaras D. Štitilis pažymi, kad kai kurios nusikalstamos veikos, priskiriamos nusikalstamoms veikoms elektroninėje erdvėje (terorizmas, grasinimas, panaudojant elektroninę erdvę), mokslinėje literatūroje nėra laikomos nusikalstamomis veikomis, susijusiomis su kompiuteriais.[28] Vadovaujantis tokiu požiūriu, teigtina, jog nusikalstamų veikų elektroninėje erdvėje samprata yra šiek tiek platesnė nei nusikalstamų veikų, susijusių su kompiuteriais, nors praktikoje nei dėl tokio, nei dėl priešingo požiūrio (nusikalstamos veikos elektroninėje erdvėje ir nusikalstamos veikos, susijusios su kompiuteriais, yra tapačios sąvokos) problemų nekyla.[29]

Pažvelkime į 1 paveikslą, kuriame nusikalstamų veikų elektroninėje erdvėje, nusikalstamų veikų, susijusių su kompiuteriais, ir kompiuterinių nusikaltimų sampratų santykis dar papildomai detalizuojamas ir konkretizuojamas vaizdine priemone.

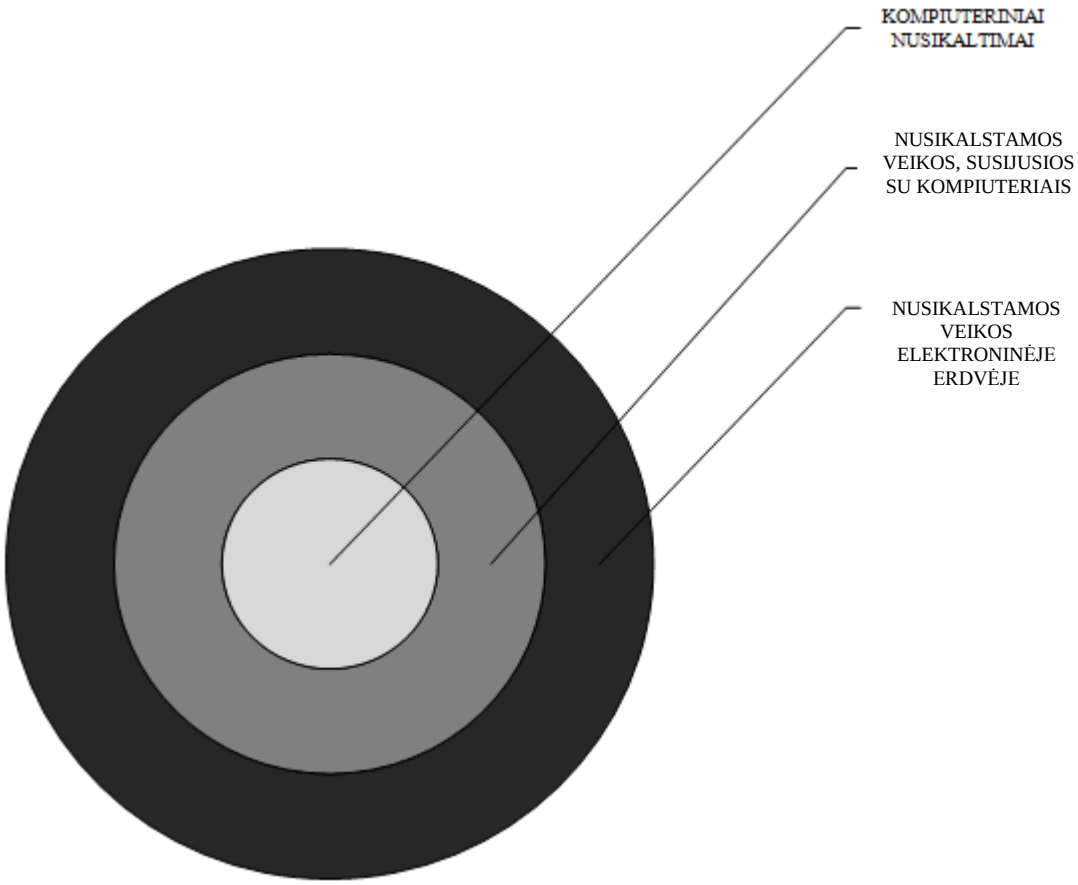
[25] Convention on Cybercrime // http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; prisijungimo laikas: 2007-10-12.

[26] Convention on Cybercrime. Explanatory Report // http://conventions.coe.int/Treaty/en/Report s/Html/185.htm; prisijungimo laikas: 2007-10-24.

[27] Magnin C. J. The 2001 Council of Europe Convention on Cyber-Crime: an Efficient Tool to Fight Crime in Cyber-Space? http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf; prisijungimo laikas: 2008-02-17.

[28] Česna R., Štitilis D. Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. - Vilnius: LTA Leidybos centras, 2000. P. 45.

[29] Brenner S. W., Goodman M. D. The Emerging Consensus on Criminal Conduct in Cyberspace. - Boston, 2005. P. 111.



1 pav. *Nusikalstamų veikų elektroninėje erdvėje, nusikalstamų veikų, susijusių su kompiuteriais, ir kompiuterinių nusikaltimų sampratų santykis*

Reziumuojant, 1 paveiksle pavaizduotas nusikalstamų veikų elektroninėje erdvėje, nusikalstamų veikų, susijusių su kompiuteriais, ir kompiuterinių nusikaltimų sampratų santykis. Remiantis tuo, kas buvo išdėstyta šiame poskyryje, nusikalstamos veikos elektroninėje erdvėje apima tiek nusikalstamas veikas, susijusias su kompiuteriais, tiek kompiuterinius nusikaltimus ir kai kurias kitas nusikalstamas veikas, kurios mokslinėje literatūroje nėra laikomos nusikalstamomis veikomis, susijusiomis su kompiuteriais. Nusikalstamos veikos elektroninėje erdvėje yra plačiausiai suprantama sąvoka. Kadangi nusikalstamos veikos, susijusios su kompiuteriais, yra tokios baudžiamojo įstatymo numatytos visuomenei pavojingos veikos, kai nusikalstamos veikos dalykas – elektroniniai duomenys, informacinės sistemos ir/arba kompiuteris panaudojamas kaip nusikalstamos veikos įvykdymo priemonė/būdas, tai ši samprata apima ir kompiuterinius nusikaltimus. Kompiuteriniai nusikaltimai yra baudžiamojo įstatymo numatytos visuomenei pavojingos veikos, kurių saugomos vertybės – elektroninių duomenų ir informacinių sistemų saugumas, tad šiame sampratų santykyje, pavaizduotame 1 pav., tai yra siauriausiai suprantama sąvoka.

1.2. Kompiuterinių nusikaltimų teisinė samprata ir reglamentacija užsienio šalių baudžiamuosiuose įstatymuose[30]

Informacinių technologijų vystymasis įvairių valstybių įstatymų leidėjus skatina peržiūrėti esamas baudžiamąsias normas bei kurti naujas, įtvirtinančias visuomeninių informacinių santykių apsaugą. Daugelis valstybių savo baudžiamuosiuose įstatymuose yra kriminalizavusios neteisėtą poveikį kompiuterinei informacijai, tačiau vienos jų - tai įtvirtindamos specialiose baudžiamojo įstatymo normose (Prancūzijos Respublikos baudžiamojo kodekso 3 knygos 3 skyriuje ,,Neteisėtas prisijungimas prie automatinių duomenų apdorojimo sistemų“ ir 2 knygos 6 skyriaus ,,Nusikaltimai prieš asmenį“ 226-16 – 226-20 straipsniai, Vokietijos Federacinės Respublikos baudžiamojo kodekso 263a straipsnis, 303b straipsnis), kitos – tradicinėse.[31] Taip pat daugelio valstybių įstatymai numato baudžiamąją atsakomybę už neteisėtą kompiuterinės informacijos perėmimą, tačiau ne visų valstybių baudžiamuosiuose įstatymuose įtvirtinami visi galimi informacijos perėmimo būdai.[32] Belgijos Karalystė (baudžiamojo kodekso 550b straipsnis), Graikijos Respublika (baudžiamojo kodekso 370C§2 straipsnis, 370B straipsnis), Italijos Respublika (baudžiamojo kodekso 615^3 straipsnis, 615^4 straipsnis, 615^5 straipsnis) yra įtvirtinusios atskiras baudžiamąsias normas kompiuterinės informacijos perėmimui ir netaiko tradicinių baudžiamųjų normų, skirtų nuosavybei apsaugoti, nors daugelyje bendrosios teisės valstybių įstatymuose (Jungtinių Amerikos Valstijų Teksaso valstijos baudžiamojo kodekso 33.01 straipsnis, Kanados baudžiamojo kodekso 430 straipsnis) kompiuterinė informacija laikoma nuosavybe, dėl to ir taikomos tradicinės normos, numatančios baudžiamąją atsakomybę už vagystę.[33] Bendrosios teisės valstybėse (Kanados baudžiamojo kodekso 342.1 straipsnis, Jungtinių Amerikos Valstijų Kalifornijos valstijos baudžiamojo kodekso 1030 straipsnis, Jungtinės Karalystės ,,Neteisėto kompiuterių panaudojimo akto“ 1(1) - 1(2) straipsniai) pastebima tendencija kriminalizuoti neteisėtą prieigą prie kompiuterių, kai tuo tarpu kontinentinės teisės šalyse (Norvegijos Karalystės baudžiamojo kodekso 145 straipsnis, 151 b straipsnis, Vokietijos Federacinės Respublikos baudžiamojo kodekso 303a straipsnis)

[30] Šiame poskyryje ir kituose darbo skyriuose bus nagrinėjami klausimai, susiję su kompiuterinių nusikaltimų samprata siaurąja prasme.

[31] Čia ir toliau šiame darbe tradicinės baudžiamojo įstatymo normos – tos baudžiamojo įstatymo normos, kuriose kompiuteris ir/ar kita informacinių technologijų bei ryšio įranga nėra išskiriama kaip ypatingas nusikalstamos veikos padarymo būdas/priemonė ar aplinkybės, elektroniniai duomenys ir informacinės sistemos nėra išskiriamos kaip ypatinga baudžiamojo įstatyto saugoma vertybė, pvz., pornografinio turinio dalykų demonstravimas ar reklamavimas (BK 309 straipsnio 4 dalis) yra tradicinė baudžiamojo įstatymo norma mūsų tiriamojo darbo objekto atžvilgiu. Jei Lietuvos Respublikos įstatymų leidėjas atskira baudžiamąja norma įtvirtintų pornografinio turinio dalykų demonstravimą ar reklamavimą internete, tokiu atveju šią normą laikytume specialiąja.

[32] United Nations Manual on the Prevention and Control of Computer-Related Crime // International Review of Criminal Policy. 1994, No. 43/44. P. 117.

[33] Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study. http://law.scu.edu/international/File/Sieber_final.pdf; prisijungimo laikas: 2008-01-26.

tokios veikos yra laikomos pavojingomis, kai neteisėtai prisijungiama prie informacinės sistemos, pažeidžiant saugumo priemones.[34,35] Pirmasis įstatymas, kriminalizuojantis nusikalstamas veikas, susijusias su kompiuteriais, buvo priimtas Jungtinėse Amerikos Valstijose, ir dabar ši valstybė yra pirmaujanti tiek nusikalstamų veikų, susijusių su kompiuteriais, kriminalizavimo, tiek jų išaiškinamumo srityje.[36] Priešingai nei daugelis Europos ir Š. Amerikos valstybių, Baltarusija apskritai nėra kriminalizavusi jokių nusikalstamų veikų, susijusių su kompiuteriais.[37]

Sistemiškai analizuojant Rusijos Federacijos baudžiamąjį kodeksą, kompiuteriniai nusikaltimai suprantami kaip baudžiamajame įstatyme nustatytos pavojingos veikos, kurių saugomos vertybės – visuomeniniai informaciniai santykiai, o dalykas – kompiuterinė informacija. Toks požiūris atitinka siaurąją kompiuterinio nusikaltimo sampratą. Dabar galiojančiame Rusijos Federacijos baudžiamojo kodekso 28 skyriaus „Nusikaltimai kompiuterinės informacijos srityje“ 272 – 274 straipsniuose yra nustatyta baudžiamoji atsakomybė už šias pavojingas veikas: neteisėtą prieigą prie kompiuterinės informacijos, žalą darančių kompiuterinių programų kūrimą, naudojimą ir platinimą bei kompiuterių, jų sistemų ir informacinių tinklų taisyklių pažeidimą.[38]

Kroatijos baudžiamajame kodekse beveik nerasime atskirų straipsnių, skirtų kriminalizuoti kompiuterinius nusikaltimus - įstatymų leidėjas pasirinko kitą kelią: nurodė kvalifikuojančias sudėtis tradicinėse normose (neteisėtas asmens duomenų panaudojimas (133 straipsnis), žalos padarymas duomenims ir kitam asmeniui priklausančių duomenų panaudojimas (223 straipsnis), rasistinių, ksenofobiškų idėjų platinimas ir fašistinės, nacistinės ar kitokios totalitarinės ideologijos garbinimas (151a straipsnis), pornografinės medžiagos platinimas (196 straipsnis), išskyrus šį straipsnį – kompiuterinės informacijos ar kompiuterinės programos pakeitimas, ištrynimas ar sunaikinimas ir neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais (223a straipsnis).[39] Taigi Kroatijos įstatymų leidėjas visas nusikalstamas veikas, kurias galima įvykdyti elektroninėje erdvėje ar pasitelkiant kompiuterį ir informacines technologijas, laiko pavojingesnėmis nusikalstamomis veikomis nei tradicinės nusikalstamos veikos, todėl jos ir sudaro tradicinių nusikalstamų veikų kvalifikuojančias sudėtis.

[34] Ten pat.
[35] Broderick T. R. Regulation of Information Technology in the European Union. - London: Springer, 2000. P. 356.
[36] Eoghan C. Digital Evidence and Computer Crime. – New York: Academic Press, 2000. P. 258.
[37] Nykodym N., Taylor R. Control of Cyber Crime. The World‘s Current Legislative Efforts against Cyber Crime // Computer Law & Security Report. 2004, Nr. 20(5). P. 395.
[38] The Criminal Code of the Russian Federation // http://www.russian-criminal-code.com/PartII/SectionIX/Chapter28. html; prisijungimo laikas: 2008-09-26.
[39] The Criminal Code of the Republic of Croatia // http://www.vsrh.hr/CustomPages/Static/HR V/Files/Legislation_ _Criminal-Code.pdf; prisijungimo laikas: 2008-09-26.

Tiek senajame 1961 m., tiek naujajame, 2002 m. rugsėjo 1 d. įsigaliojusiame, Estijos baudžiamajame kodekse yra kriminalizuojamos nusikalstamos veikos elektroninėje erdvėje. Šios nusikalstamos veikos nėra išskirtos į vieną kodekso skyrių, tačiau jų galima rasti „Nusikaltimai nuosavybei“ (sabotažas, panaudojant kompiuterį (206 straipsnis), kompiuterinio tinklo sujungimų pažeidimas (207 straipsnis), kompiuterinių virusų platinimas (208 straipsnis), sukčiavimas, panaudojant kompiuterį (213 straipsnis), neteisėtas kompiuterio, kompiuterinės sistemos ar kompiuterinio tinklo naudojimas (217 straipsnis)), „Nusikaltimai intelektinei nuosavybei“ (disponavimas neteisėtai atgamintomis kompiuterinėmis programomis (222^1 straipsnis)), „Nusikaltimai viešajai tvarkai“ (slaptažodžių platinimas (284 straipsnis)) skyriuose.[40]

Pateikti ir išanalizuoti trijų valstybių įstatymų leidėjų skirtingi pasirinkimai, kaip baudžiamosiose normose įtvirtintos nusikalstamos veikos elektroninėje erdvėje, nusikalstamos veikos, susijusios su kompiuteriais ir kompiuteriniai nusikaltimai bei kaip jos pavadintos, leidžia daryti išvadą, jog vienas iš svarbiausių aspektų – numatyti baudžiamąją atsakomybę už šias nusikalstamas veikas, o tai, kaip jos yra įtvirtintos ir pavadintos baudžiamosiose normose, nėra taip svarbu – tai tik išreiškia skirtingų valstybių įstatymų leidėjų požiūrį į šių veikų pavojingumą ir jomis padaromų pavojingų padarinių reikšmę bei sunkumą. Net ir skirtingai vadinamas tokias nusikalstamas veikas įvairių valstybių baudžiamosiose normose galima suklasifikuoti pagal mūsų jau minėtą klasifikaciją (nusikalstamos veikos elektroninėje erdvėje, nusikalstamos veikos, susijusios su kompiuteriais, kompiuteriniai nusikaltimai), nes tai yra viena iš bendriausių, labiausiai paplitusių ir žinomų klasifikacijų mokslininkų darbuose. Kiekvienos valstybės įstatymų leidėjo bandymas „surasti“ ir įtvirtinti tos valstybės baudžiamųjų normų sistemai ir struktūrai priimtiną pavadinimą yra sveikintinas.

1.3. Kompiuterinių nusikaltimų teisinės sampratos raida Lietuvos Respublikos baudžiamajame kodekse

Sparčiai vystantis informacinėms technologijoms, didėjant prieinamumui prie globalios elektroninės erdvės, į valstybių ratą, kurios kriminalizuoja arba peržiūri savo baudžiamuosius įstatymus, susijusius su kompiuteriniais nusikaltimais, patenka ir Lietuva. Tokių veikų kriminalizavimas parodo, jog ir Lietuvos Respublikos įstatymų leidėjas šalia kitų valstybių kompiuterinius nusikaltimus laiko pavojingomis nusikalstamomis veikomis.

[40] Estijos baudžiamasis kodeksas // http://www.legislationline.org/upload/legislations/07/6a/4d16963509db70c09d23e52cb8df.htm; prisijungimo laikas 2008-07-14.

2003 m. gegužės 1 d. įsigaliojusiame naujajame BK[41] buvo atskiras skyrius „Nusikaltimai informatikai“, kuriame buvo kriminalizuotos šios nusikalstamos veikos: kompiuterinės informacijos sunaikinimas ar pakeitimas (196 straipsnis), kompiuterinės programos sunaikinimas ar pakeitimas (197 straipsnis) ir kompiuterinės informacijos pasisavinimas ir skleidimas (198 straipsnis). BK XXX skyriaus saugomos vertybės – informatika – buvo kritikuotinas, nes informatika – mokslas apie informaciją, jos perdavimą, kaupimą, saugojimą, apdorojimą.[42] Informatikos terminas apima ir teorinį, ir praktinį darbo su informacija pobūdį, taip pat ir kompiuterių taikymą. Be to, informatika - ne tik mokslas, bet ir mokyklinė disciplina (informacijos aprašymo ir algoritminių procesų pertvarkymo sisteminės studijos: jų teorija, analizė, projektavimas, realizavimas ir taikymas).[43] Taigi, Lietuvos Respublikos įstatymų leidėjas baudžiamajame įstatyme įtvirtino informatikos mokslą kaip tą vertybę arba gėrį, kurį tuo metu reikėjo apsaugoti. Tačiau, darant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, kėsinamasi į tokias baudžiamojo įstatymo saugomas vertybes kaip elektroninių duomenų ir informacinių sistemų saugumas ir nepažeidžiamas *per se* informatikos mokslas.

2004 m. sausio 29 d. įstatymu Nr. IX-1992 „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“ buvo padaryti XXX skyriaus „Nusikaltimai informatikai“ straipsnių pakeitimai bei skyrius papildytas 2 naujais straipsniais: neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo (198^1 straipsnis) ir neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti (198^2 straipsnis).[44] Šie pakeitimai iš dalies susiję su Lietuvos Respublikos 2003 m. birželio 23 d. Konvencijos dėl elektroninių nusikaltimų pasirašymu.[45] Kadangi baudžiamojoje teisėje turi būti tiesiogiai taikomi Lietuvos baudžiamieji įstatymai, tai Konvencijos dėl elektroninių nusikaltimų nuostatas reikėjo įgyvendinti nacionaliniuose baudžiamuosiuose įstatymuose.[46] Tik tarptautinės pastangos gali sukurti efektyvią nusikalstamų veikų elektroninėje erdvėje prevencijos ir kovos su jomis priemonių

[41] Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Lietuvos Respublikos baudžiamasis kodeksas (su pakeitimais ir papildymais iki 2008 m. birželio 12 d.) // Valstybės žinios. 2004, Nr. 25-760.

[42] Informacinių technologijų institutas. Lietuvos kompiuterininkų sąjunga. Pagrindinės informacijos technologijos sąvokos. – Vilnius: Žara, 2001. P. 26.

[43] Mitašiūnas A. Žvilgsnis iš informatikos varpinės // Mokslas ir gyvenimas. 1999, Nr. 9. P. 14.

[44] 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 198^1 straipsniais įstatymas // Valstybės žinios. 2000, Nr. 89-2741.

[45] Lietuvos Respublika Konvenciją dėl elektroninių nusikaltimų pasirašė 2003 m. birželio 23 d., ratifikavo – 2004 m. kovo 18 d., o konvencija įsigaliojo 2004 m. liepos 1 d.

[46] Lietuvos Respublikos Konstitucinio teismo išvada „Dėl Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 4, 5, 9, 14 straipsnių ir jos ketvirtojo protokolo 2 straipsnio atitikimo Lietuvos Respublikos Konstitucijai“ // Valstybės žinios. 1995, Nr. 9-199.

teisinio bendradarbiavimo schemą, o šios konvencijos pasirašymas ir ratifikavimas valstybę įpareigoja savo nacionalinę teisę suderinti su konvencinėmis nuostatomis, kriminalizuojant nusikalstamas veikas bei sutvarkant procesinių priemonių, skirtų konkrečių nusikalstamų veikų tyrimui, taikymą. Taip pat šiais pakeitimais buvo praplėstas straipsnių dispozicijoje esančių alternatyvių veikų sąrašas, įtraukti nauji veikų padarymo būdai.

Tiek Lietuvoje, tiek visame pasaulyje padaromų nusikalstamų veikų elektroninėje erdvėje skaičius nuolat auga, tobulėja nusikalstamų veikų padarymo būdai ir metodai, padaromi milžiniški nuostoliai. Tokios nusikalstamos veikos kelia vis didesnę grėsmę asmenų, įmonių privatumui bei nuosavybei, bankinės ir finansinės sistemos stabilumui, ūkio, valstybinių institucijų funkcionavimui, nacionalinio saugumo interesams. Nepakankamas ir netikslus šių nusikalstamų veikų reglamentavimas sąlygoja ribotas jų atskleidimo ir ištyrimo galimybes, atsakomybės nebuvimą už kai kurias nusikalstamų veikų padarymo formas, neadekvatų sankcijų griežtumą potencialiam nusikalstamų veikų pavojingumui. Todėl 2007 m. birželio 28 d. įstatymu Nr. X-1233[47] buvo pakeistas XXX skyriaus pavadinimas, kai kurių straipsnių terminija, įtrauktos kvalifikuotos ir privilegijuotos nusikalstamų veikų sudėtys, alternatyvios bausmės. Mūsų manymu, BK XXX skyriaus pavadinimas ,,Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“ tiksliau apibrėžia šio skyriaus straipsniuose įtvirtintų visuomeninių gėrių ir vertybių apsaugą – elektroninių duomenų ir informacinių sistemų saugumą. Informatikos objektas yra konkrečios informacinės sistemos: labiausiai čia domimasi sistemomis, kurios atlieka įvairius veiksmus su informacija (surenka, perduoda, tvarko, saugo), todėl tai daug tikslesnis skyriaus pavadinimas, o kartu ir baudžiamojo įstatymo saugomos vertybės, į kurias kėsinamasi, nei anksčiau buvusi – informatika. Toks skyriaus pavadinimas atitinka informacinių technologijų mokslų vartojamą šiuolaikinių technologijų terminiją ir esmę bei tarptautinių dokumentų nuostatas.

Tokia pakeitimų gausa susijusi ir su 2005 m. vasario 24 d. Tarybos pamatinio sprendimo 2005/222/TVR ,,Dėl atakų prieš informacines sistemas“ (toliau – Pamatinis sprendimas) nuostatų perkėlimu į nacionalinę teisę.[48] Europos Sąjungos sutarties 34 straipsnio 2 dalies b punkte numatyti teisės aktai – pamatiniai sprendimai – yra privalomi rezultatų, kuriuos reikia pasiekti, atžvilgiu, tačiau nacionalinėms valdžios institucijoms paliekama galimybė pasirinkti jų įgyvendinimo formą ir būdus. *Mutatis mutandis* buvo siekta suderinti BK nuostatas su

[47] Lietuvos Respublikos baudžiamojo kodekso 7, 38, 47, 63, 66, 70, 75, 82, 93, 129, 166, 167, 172, 178, 180, 181, 182, 183, 184, 185, 189, 194, 196, 197, 198, 198^1, 198^2, 199, 202, 213, 214, 215, 225, 227, 228, 231, 233, 235, 252, 256, 257, 262, 284, 285, 312 straipsnių, priedo pakeitimo ir papildymo, XXVI, XXX skyrių pavadinimų pakeitimo ir kodekso papildymo 256^1, 257^1 straipsniais įstatymas // http://www3.lrs.lt/pls/inter3/dokpaieska.showdocl?pid=301997; prisijungimo laikas: 2008-08-11.

[48] 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=COM:2005:0583:FIN:LT:HTML; prisijungimo laikas: 2008-08-27.

Konvencijos dėl elektroninių nusikaltimų nuostatomis ir vartojamomis sąvokomis, sugriežtinti baudžiamąją atsakomybę už poveikį strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui, ar finansų sistemai turinčiai informacinei sistemai, patikslinti kai kuriuos nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui padarymo būdus.

Lyginant BK XXX skyriuje numatytų pavojingų veikų straipsnių sankcijose numatytas bausmės rūšis ir sankcijų ribas su ankstesnėmis BK XXX skyriaus redakcijomis, pastebime, jog dabartinėje redakcijoje yra numatyta daugiau alternatyvių bausmės rūšių, praplėstos straipsnių sankcijose numatytos laisvės atėmimo bausmės ribos. Visi šie pakeitimai suteikia teismui didesnes galimybes individualizuoti bausmę.

Paradoksalu, tačiau BK terminas „kompiuterinis nusikaltimas“ nėra vartojamas, nors Lietuvos Respublikos įstatymų leidėjas kriminalizavo nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui. Nors šis terminas ir nėra įteisintas *de jure*, tačiau vartojamas *de facto* lietuvių mokslininkų darbuose (R. Petrausko, D. Štitilio, V. Kligio, R. Burdos, S. Gudmono, M. Kiškio). Kadangi baudžiamojo įstatymo saugomi gėriai yra BK specialiosios dalies normų suskirstymo į skyrius pagrindinis kriterijus, tai, vadovaujantis dabar galiojančio BK XXX skyriumi, teigtina, jog Lietuvos Respublikos įstatymų leidėjas įteisina kompiuterinio nusikaltimo siaurąja prasme sampratos aspektus.

Tačiau sistemiškai analizuojant BK, galime rasti ir tokių BK įtvirtintų nusikalstamų veikų sudėčių, kurios rodo, jog Lietuvos Respublikos įstatymų leidėjas įtvirtina ir kai kuriuos nusikalstamos veikos, susijusios su kompiuteriais, sampratos aspektus, nes šios nusikalstamos veikos gali būti padaromos, panaudojant kompiuterį ir kitas informacines telekomunikacijas bei technologijas: sukčiavimas (BK 182 straipsnis), literatūros, mokslo, meno ar kitokio kūrinio neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas (BK 192 straipsnis), neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas (BK 194 straipsnis), netikrų pinigų ar vertybinių popierių pagaminimas, laikymas arba realizavimas (BK 213 straipsnis), disponavimas pornografinio turinio dalykais (BK 309 straipsnis). Manytume, jog įstatymų leidėjas šioms nusikalstamoms veikoms, kuriose kompiuteris ir kitos informacinės telekomunikacijos ir technologijos gali būti panaudojamos kaip nusikalstamos veikos įvykdymo priemonės ar būdai, įtvirtinti pasirinko tradicines baudžiamojo įstatymo normas, neišskiriant šių nusikalstamų veikų į specialiąsias baudžiamojo įstatymo normas.

Apibendrinant, turime pasakyti, jog Lietuvos Respublikos įstatymų leidėjas, baudžiamajame kodekse kriminalizuodamas nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, įtvirtino kompiuterinio nusikaltimo siaurąja prasme sampratos aspektus. Nusikalstamomis veikomis, kuriose kompiuteris ir kitos informacinės technologijos

gali būti panaudojamos kaip nusikalstamos veikos įvykdymo priemonės ar būdai (BK 182, 192, 194, 213, 309 straipsniai ir kt.), įtvirtinami kai kurie nusikalstamų veikų, susijusių su kompiuteriais, sampratos aspektai tradicinėse baudžiamojo įstatymo normose, neišskiriant šių nusikalstamų veikų į specialiąsias baudžiamojo įstatymo normas.

2. LIETUVOS RESPUBLIKOS BAUDŽIAMAJAME KODEKSE NUMATYTŲ NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI SUDĖČIŲ IR JŲ OBJEKTYVIŲJŲ IR SUBJEKTYVIŲJŲ POŽYMIŲ ANALIZĖ

2.1. Lietuvos Respublikos baudžiamajame kodekse numatytų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių ypatumai

BK 2 straipsnio 4 dalyje įtvirtinta nuostata, jog pagal baudžiamąjį įstatymą atsako tik tas asmuo, kurio padaryta veika atitinka baudžiamojo įstatymo numatytą nusikaltimo arba baudžiamojo nusižengimo sudėtį.[49] Taigi nusikalstamos veikos sudėties įtvirtinimas baudžiamajame įstatyme yra pakankamas pagrindas įgyvendinti baudžiamąją atsakomybę.[50]

Lietuvos Respublikos įstatymų leidėjas BK 196 – 198^2 straipsniuose (neteisėtas poveikis elektroniniams duomenims, neteisėtas poveikis informacinei sistemai, neteisėtas elektroninių duomenų perėmimas ir panaudojimas, neteisėtas prisijungimas prie informacinės sistemos, neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis) įtvirtino nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtis, o baudžiamojo įstatymo pagrindinė saugoma vertybė išskiria šias veikas į atskirą BK XXX skyrių „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“. Šias nusikalstamų veikų sudėtis taip pat galima suskirstyti pagal tam tikrus kriterijus:

1. pagal pavojingumo laipsnį – pagrindinės sudėtys: BK 196 straipsnio 1 dalis, 197 straipsnio 1 dalis, 198 straipsnio 1 dalis, 198^1 straipsnio 1 dalis, 198^2 straipsnio 1 dalis, kvalifikuotos sudėtys: BK 196 straipsnio 2 dalis, 197 straipsnio 2 dalis, 198 straipsnio 2 dalis, 198^1 straipsnio 2 dalis, privilegijuotos sudėtys: BK 196 straipsnio 3 dalis, 197 straipsnio 3 dalis;

2. pagal pavojingų padarinių reikšmę nusikalstamos veikos sudėčiai ir asmens baudžiamajai atsakomybei – materialios sudėtys: BK 196, 197 straipsniai, formalios sudėtys: BK 198, 198^1, 198^2 straipsniai;

[49] Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Lietuvos Respublikos baudžiamasis kodeksas (su pakeitimais ir papildymais iki 2008 m. birželio 12 d.) // Valstybės žinios. 2004, Nr. 25-760.

[50] Piesliakas V. Lietuvos baudžiamoji teisė. Baudžiamasis įstatymas ir baudžiamosios atsakomybės pagrindai. Kn. 1. - Vilnius: Justitia, 2006. P. 182.

3. pagal nusikalstamų veikų rūšis (o nusikaltimus - dar ir pagal BK Specialiosios dalies straipsnio sankcijoje numatytą bausmės rūšį ir dydį) – baudžiamieji nusižengimai (BK 196 straipsnio 3 dalis, 197 straipsnio 3 dalis) ir nusikaltimai (nesunkūs (BK 198^1, 198^2 straipsniai), apysunkiai (BK 196 straipsnio 1 ir 2 dalys, 197 straipsnio 1 ir 2 dalys, 198 straipsnis));

4. pagal kaltės formą – kriminalizuotos tik tyčinės nusikalstamos veikos, kuriomis yra kėsinamasi į elektroninių duomenų ir informacinių sistemų saugumą: BK 196, 197, 198, 198^1, 198^2 straipsniai.

Priklausomai nuo padarinių sunkumo (didelė žala, nedidelė žala), nuo kaltės formos įstatymų leidėjas numato ir skirtingas sankcijas, t.y. skirtingas laisvės atėmimo bausmių ribas ir kitas bausmių rūšis. Į nusikalstamų veikų sudėtis įtraukti papildomi požymiai, didinantys nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui pavojingumą (kvalifikuotos sudėtys). Visos BK XXX skyriuje formuluojamos sankcijos yra santykinai apibrėžtos – greta laisvės atėmimo bausmės numatomos alternatyvios bausmės (BK 196, 197 straipsniai, 198 straipsnio 1 dalis, 198^1, 198^2 straipsniai) arba numatyta tik laisvės atėmimo bausmė (BK 198 straipsnio 2 dalis).

BK 196 – 198^2 straipsniuose dauguma įtvirtintų dispozicijų yra mišrios, turinčios aprašomųjų, nukreipiamųjų ir blanketinių dispozicijų požymių, pavyzdžiui, norint paaiškinti, kas yra nacionalinis saugumas, reikia vadovautis Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymu[51], norint išsiaiškinti, koks neviešų elektroninių duomenų stebėjimas, fiksavimas, perėmimas, įgijimas, laikymas yra teisėtas, o koks nusikalstamas, vienas iš teisės aktų, kuriuo reikia vadovautis, yra Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas[52].

Pagrindas išvadai apie nusikalstamos veikos sudėties buvimą kaltininko veikoje yra teisiškai reikšmingi nusikalstamų veikų sudėčių požymiai, o nesant tam tikro sudėties požymio, veika neužtraukia baudžiamosios atsakomybės. Taigi toliau bus detaliai aptariami nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių objektyvieji ir subjektyvieji požymiai, kurie yra nusikalstamų veikų kvalifikavimo pagal konkretų BK straipsnį pagrindas. Norėtume pažymėti, jog tiek priežastinio pavojingos veikos ir baudžiamajame įstatyme numatytų padarinių ryšio, tiek nusikalstamą veiką padariusį asmenį apibūdinančių požymių aspektai nebus nagrinėjami, kadangi jie nesukelia teorinių ir praktinių problemų.

[51] Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas // Valstybės žinios. 1997, Nr. 2-16.
[52] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 1996, Nr. 63-1479.

2.2. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių objektyviųjų požymių analizė

2.2.1. Baudžiamojo įstatymo, įtvirtinančio nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, saugomos vertybės

Kiekviena visuomenė savo gyvenimą valstybėje grindžia tam tikra vertybių sistema ir samprata. Baudžiamojo įstatymo saugomomis vertybėmis dažniausiai tampa vertingiausi ir labiausiai branginami gėriai. Baudžiamojo įstatymo saugomos vertybės – pagrindinis objektyvusis nusikalstamos veikos sudėties požymis, įrodinėtinas tiriant ir nagrinėjant visas nusikalstamas veikas. BK XXX skyriaus pavadinimo pakeitimas 2007 m. birželio 28 d. įstatymu Nr. X-1233[53], o tuo pačiu ir baudžiamojo įstatymo saugomų vertybių sukonkretinimas sveikintinas, nes 2003 m. gegužės 1 d. įsigaliojusiame naujajame BK XXX skyrius buvo pavadintas ,,Nusikaltimai informatikai“[54]. Tai kritikuotina, nes, *prima facie*, informatika yra suvokiama kaip mokslo šaka (visuma tam tikrų žinių), antra, labai abejotina, ar nusikalstamomis veikomis, nurodytomis BK XXX skyriuje, galima pasikėsinti į tam tikrą žinių visumą. Paradoksalu, tačiau, darant tokias nusikalstamas veikas, yra pasitelkiamos informatikos mokslo žinios ir laimėjimai.

Dabar galiojančiame BK XXX skyrius vadinamas ,,Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“, tad toks skyriaus pavadinimas atitinka informacinių technologijų mokslų vartojamą šiuolaikinių technologijų terminiją ir esmę. Kadangi BK XXX skyriuje yra įtvirtinti ne tik nusikaltimai, bet ir baudžiamieji nusižengimai, tad skyriaus pavadinimas yra netikslus – jį reikėtų keisti į ,,Nusikaltimai ir baudžiamieji nusižengimai elektroninių duomenų ir informacinių sistemų saugumui“.

BK XXX skyriaus saugoma vertybė - elektroninių duomenų ir informacinių sistemų saugumas, netrukdomai, nekliudomai, automatiškai apdorojant elektroninius duomenis ir valdant bei kontroliuojant informacines sistemas. Įstatymais garantuojamas elektroninių duomenų ir informacinių sistemų saugumas yra vertybė, į kurią kėsinamasi.[55] Baudžiamojo įstatymo saugomos vertybės yra BK specialiosios dalies normų suskirstymo į skyrius pagrindinis

[53] Lietuvos Respublikos baudžiamojo kodekso 7, 38, 47, 63, 66, 70, 75, 82, 93, 129, 166, 167, 172, 178, 180, 181, 182, 183, 184, 185, 189, 194, 196, 197, 198, 198^1, 198^2, 199, 202, 213, 214, 215, 225, 227, 228, 231, 233, 235, 252, 256, 257, 262, 284, 285, 312 straipsnių, priedo pakeitimo ir papildymo, XXVI, XXX skyrių pavadinimų pakeitimo ir kodekso papildymo 256^1, 257^1 straipsniais įstatymas // http://www3.lrs.lt/pls/inter3/dokpaieska.showdocl?pid=301997; prisijungimo laikas: 2008-08-11.

[54] Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Lietuvos Respublikos baudžiamasis kodeksas (su pakeitimais ir papildymais iki 2008 m. birželio 12 d.) // Valstybės žinios. 2004, Nr. 25-760.

[55] Sabaliauskas G. Informacijos saugumas internete: teisininkų ir informatikų problema // Justitia. 2001, Nr. 1. P. 28.

kriterijus.[56] Pagal pažeidžiamų baudžiamojo įstatymo saugomų vertybių svarbą Lietuvos Respublikos įstatymų leidėjas šias nusikalstamas veikas įtvirtino po nusikalstamų veikų nuosavybei, turtinėms teisėms ir turtiniams interesams, nusikaltimų intelektinei ir pramoninei nuosavybei, tad, manytume, jog Lietuvos Respublikos įstatymų leidėjas nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui gretina su tokiomis tradicinėmis nusikalstamomis veikomis kaip nusikalstamos veikos nuosavybei ir panašiai.

Elektroninių duomenų sąvoką reglamentuoja Lietuvos Respublikos elektroninio parašo įstatymas[57]: elektroniniai duomenys yra visi duomenys, kurie tvarkomi informacinių technologijų priemonėmis. Šis įstatymas elektroninių duomenų sąvoką sieja su atitinkamomis priemonėmis, tačiau pabrėžtina, jog informacinių technologijų priemonės apima ne tik siuntimui ir gavimui naudojamas priemones, bet ir kompiuteriu sukurtus duomenis, kurie nėra skirti perdavimui. Taigi elektroniniai duomenys - bet kokie materialiame (fiziniame) objekte esantys duomenys, kurie yra sukurti, saugomi ar perduodami informacinių technologijų ir telekomunikacijų priemonėmis, pavyzdžiui, kompiuterio kietajame diske, diskelyje, kompaktiniame diske, USB atmintinėje, skaitmeniniame vaizdo diske. Elektroniniai duomenys – bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti informacine sistema arba programa, pagal kurią informacinė sistema gali vykdyti tam tikrą funkciją. Tai gali būti labai įvairi informacija – apie asmenis, daiktus, faktus, įvykius, reiškinius ir procesus.

Elektroniniais duomenimis išreiškiama apdorojama informacija. Vieni autoriai teigia, jog skirtumas tarp informacijos ir duomenų sąvokų nėra griežtas, nes jomis vadinamas tas pats objektas, tik skirtingu abstrakcijos lygmeniu: „informacija“ – abstraktesniu, „duomenys“ – konkretesniu.[58] Teisėje „informacija“ dažniausiai yra nagrinėjama kaip teisinių santykių objektas, t. y. vertybė, kurią įgyja ir kuria pasinaudoti siekia teisinio santykio dalyviai, įgyvendindami savo teises.[59] Vis tik manytume, jog kompiuterinė informacija ir elektroniniai duomenys nėra tapačios sąvokos – galima tokia situacija, jog pakeitus duomenis, informacija gali išlikti nepakitusi, todėl skirtumas tarp informacijos ir duomenų yra akivaizdus.[60] Apibendrinant duomenis yra sukuriama informacija, kalbėdami apie duomenis, omenyje turime faktus, kalbėdami apie informaciją – faktų interpretavimą.

[56] Piesliakas V. Lietuvos baudžiamoji teisė. Baudžiamasis įstatymas ir baudžiamosios atsakomybės pagrindai. Kn. 1. - Vilnius: Justitia, 2006. P. 212.
[57] Lietuvos Respublikos elektroninio parašo įstatymas // Valstybės žinios. 2000, Nr. 61-1827.
[58] Johnson D., Post D. Law and Borders – the Rise of Law in Cyberspace // Stanford Law Review. 1996, Nr. 48. P. 38.
[59] Vaišvila A. Teisės teorija. Vilnius: Justitia, 2000. P. 234.
[60] Civilka M. ir kt. Informacinių technologijų teisė. - Vilnius: NVO Teisės institutas, 2004. P. 280.

Informacinės sistemos sąvoka yra įtvirtinta Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme[61]: informacinė sistema – techninių ir programinių priemonių visuma, naudojama informacijai kurti, siųsti, priimti, išsaugoti ar kitaip tvarkyti elektroniniu būdu. Informacinė sistema - 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.[62] Kai kurie autoriai informacinę sistemą supranta daug plačiau - prasmingą informaciją individams ir organizacijoms pateikianti ir kartu veikianti aparatūros ir programinės įrangos, žmonių, procedūrų ir duomenų visuma.[63] Tokios sampratos vartojimas yra grindžiamas tuo, jog pagal automatizacijos lygį visas informacines sistemas galima suskirstyti į: neautomatines (nėra naudojamos šiuolaikinės techninės priemonės ir visus darbus atlieka žmogus), pusiau automatines (naudojamos šiuolaikinės techninės priemonės, bet taip pat jose dalyvauja ir žmogus), automatines (atlieka visas informacijos apdorojimo operacijas be žmogaus įsikišimo, tai įvairūs robotai, pvz., interneto paieškos sistemos).[64]

Pabrėžtina, jog sąvoka informacinė sistema yra platesnė nei sąvoka kompiuteris, nes paprastai kompiuteris reiškia skaičiavimo mašiną, kai tuo tarpu jau dabar duomenys gali būti apdorojami ne tik kompiuteryje, bet ir, pavyzdžiui, mobiliajame telefone ir pan. Sąvoka informacinė sistema geriau atspindi technologijų pokyčius bei tuo pačiu apimtų naujai atsirandančius įrenginius ir technologijas.

Kuo sudėtingesnis informacijos surinkimas, kuo didesni jos kiekiai ir aktualesnis turinys, tuo didesnis yra informacinių sistemų poreikis, nes ,,popieriumi ir pieštuku“ jos suvaldyti paprasčiausiai nebeįmanoma.[65] Todėl šiuo metu vis daugiau informacijos apdorojimo užduočių yra automatizuojamos, panaudojant kompiuterizuotas informacines sistemas. Pusiau automatinės informacinės sistemos šiuo metu yra populiariausios, tad dažniausiai jos ir vadinamos informacinėmis sistemomis. Darytina išvada, jog Lietuvos Respublikos įstatymų leidėjas BK informacinės sistemos sąvoką vartoja kaip informacinės sistemos rūšį, t.y. informacinė sistema yra prilyginama pusiau automatinei/automatinei (kompiuterizuotai) informacinei sistemai, tad ir toliau šiame tiriamajame darbe bus naudojama informacinių sistemų sąvoka, ją suprantant kaip

[61] Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas // Valstybės žinios. 2006, Nr. 65-2380.
[62] 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=COM:2005:05 83:FIN:LT:HTML; prisijungimo laikas: 2008-08-27.
[63] Lindsay J. Information Systems – Fundamentals and Issues. - Kingston University, School of Information Systems, 2000. P. 117.
[64] Ten pat, P. 120.
[65] Steponavičienė G. Informacinės sistemos - galimybė sumažinti administravimo naštą. // Pranešimo tezės konferencijoje ,,Proliberalios reformos mokesčių naštai sumažinti“. - Vilnius, 1997.

kompiuterizuotą informacinę sistemą. Informacinės sistemos apdoroja duomenis, panaudodamos tarpusavyje susietų funkcijų (įvestis, saugojimas, apdorojimas ir išvestis) rinkinį - informacinės sistemos priima, saugo ir apdoroja duomenis, o rezultatus pateikia informacijos pavidalu.

Suma summarum, tiek elektroninių duomenų ir informacinės sistemos, tiek kitų BK XXX skyriuje vartojamų sąvokų išaiškinimas nėra būtinas pačiame BK. Nors šios sąvokos atrodo ir pakankamai aiškios, tačiau, jas interpretuojant ir vertinant padarytas veikas iš baudžiamosios teisės pozicijų, gali kilti problemų. Šias sąvokas detalizuoja kiti Lietuvos Respublikos teisės aktai[66], be to, dėl greito technologijų pokyčių ir vystymosi, sąvokos gali kisti, o tokiu atveju kaskart reiktų daryti BK pakeitimus, todėl šią problemą galėtų išspręsti blanketinių dispozicijų įtvirtinimas, kurios minėtų sąvokų konkretinimo nurodytų ieškoti tam tikruose teisės aktuose. Tačiau problema, jog tuose teisės aktuose vienodos sąvokos gali būti traktuojamos skirtingai, vis tik išlieka, todėl reikia siekti šių sąvokų unifikavimo arba vieno teisės akto priėmimo, kuriame būtų išaiškintos BK XXX skyriuje vartojamos sąvokos, panašiai kaip dabar galioja 2003 m. gegužės 23 d. Lietuvos Respublikos sveikatos apsaugos ministro, Lietuvos Respublikos teisingumo ministro ir Lietuvos Respublikos socialinės apsaugos ir darbo ministro įsakymas Nr. V-298/158/A1-86 „Dėl sveikatos sutrikdymo masto nustatymo taisyklių patvirtinimo“, detalizuojantis BK XVIII skyriuje „Nusikaltimai žmogaus sveikatai“ esančiuose straipsniuose numatytus sveikatos sutrikdymų požymius.[67]

2.2.2. Pavojinga veika kaip nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių objektyvusis požymis

Nusikalstamos veikos sudėtyse pavojinga veika yra vienas iš būtinų tiek nusikaltimo, tiek baudžiamojo nusižengimo požymių. Pavojinga veika yra nusikalstamos veikos sudėties objektyvusis požymis, kurį įstatymų leidėjas visada naudoja formuluodamas nusikalstamų veikų sudėtis.[68] Šį požymį reikia visada nustatyti ir įrodinėti bet kokioje nusikalstamos veikos sudėtyje. Nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui kaip pavojingas veikas apibūdina alternatyvūs veiksmai: neteisėtai sunaikino, sugadino, pašalino ar pakeitė ar

[66] Lietuvos Respublikos elektroninio parašo įstatymas // Valstybės žinios. 2000, Nr. 61-1827; Lietuvos Respublikos elektroninių ryšių įstatymas // Valstybės žinios. 2004, Nr. 69-2382; Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas // Valstybės žinios. 2006, Nr. 65-2380; Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas // http://www3.lrs .lt/pls/inter3/dokpaies ka.showdoc_l?p_id=314533; prisijungimo laikas: 2008-04-17.

[67] Lietuvos Respublikos Sveikatos apsaugos ministro, Lietuvos Respublikos Teisingumo ministro ir Lietuvos Respublikos Socialinės apsaugos ir darbo ministro įsakymas „Dėl sveikatos sutrikdymo masto nustatymo taisyklių patvirtinimo“ // http://www3.lrs.lt/pls/inter3/dokpaieska.s howdocl?p_id=211886&p_query=&p_tr2=; prisijungimo laikas: 2008-06-04.

[68] Piesliakas V. Lietuvos baudžiamoji teisė. Baudžiamasis įstatymas ir baudžiamosios atsakomybės pagrindai. Kn. 1. - Vilnius: Justitia, 2006. P. 230.

kitais būdais apribojo (BK 196 straipsnis); neteisėtai sutrikdė ar nutraukė (BK 197 straipsnis); neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo (BK 198 straipsnis); neteisėtai gamino, gabeno, pardavė ar kitaip platino arba tuo pačiu tikslu įgijo ar laikė (BK 198^2 straipsnis) bei BK 198^1 straipsnyje aprašyta viena pavojinga veika: neteisėtai prisijungė.

Pirmoji grupė nusikalstamų veikų sudėčių vadinama nusikalstamų veikų sudėtimis su alternatyviais veikos požymiais, taigi baudžiamajai atsakomybei kilti pakanka, jei padaryta bent viena veika, nurodyta straipsnio dispozicijoje, pvz., neteisėtas programinės įrangos, tiesiogiai skirtos daryti nusikalstamas veikas, įgijimas užtraukia baudžiamąją atsakomybę pagal BK 198^2 straipsnį. Kelių alternatyvių veikų, nurodytų straipsnio dispozicijoje, padarymas nesudaro nusikalstamų veikų pakartotinumo, ir veika kvalifikuojama kaip viena nusikalstama veika, pvz., neteisėtas neviešų elektroninių duomenų stebėjimas, perėmimas ir laikymas yra viena nusikalstama veika ir užtraukia atsakomybę pagal BK 198 straipsnį. Kai kurios aprašytos pavojingos veikos yra išsitęsusios laiko atžvilgiu, pvz., neviešų elektroninių duomenų laikymas (BK 198 straipsnis) ar programinės įrangos, slaptažodžių laikymas (BK 198^2 straipsnis). Tokia pavojinga veika vadinama trunkama nusikalstama veika, tačiau iš nusikalstamos veikos sudėties pozicijų tai yra viena nusikalstama veika.

Norint apsaugoti tinkamą elektroninių duomenų apdorojimą, išsaugotų elektroninių duomenų naudojimą, BK 196 straipsnyje yra numatyta baudžiamoji atsakomybė už neteisėtą poveikį elektroniniams duomenims. Elektroninių duomenų sunaikinimas – duomenų ištrynimas iš kompiuterio ar kitos laikmenos atminties, kai dėl tokių veiksmų jais nebeįmanoma naudotis pagal paskirtį arba jų atkurti. Sunaikinimo sąvoka yra sąlyginė, nes, ištrynus norimą bylą ar aplanką kompiuteryje, tie duomenys kurį laiką dar yra saugomi kompiuterio atmintyje. Norint visiškai sunaikinti kokius nors duomenis, saugomus kompiuteryje ar laikmenoje, vien pašalinti, ištrinti šių duomenų neužteks. Šalinant duomenis, jie nėra ištrinami diske, tad juos specialiomis programomis galima perskaityti tol, kol kiti duomenys nėra įrašomi būtent toje vietoje, kurioje buvo tie panaikinti duomenys. Norint visiškai sunaikinti duomenis taip, kad jų būtų apskritai nebeįmanoma atkurti, naudojamos tam tikros programos, o pats procesas vadinamas „wiping“ (visiškas sunaikinimas). Įdomi yra ta duomenų savybė, jog jei įmonė ar vartotojas sistemingai ir nuolatos daro tam tikrų duomenų kopijas, tai, sunaikinus tam tikrus duomenis, lieka jų kopijos, vadinasi, informacija neprarandama. Tokiu atveju sąvoka sunaikinimas nėra pats tinkamiausias terminas, kadangi tokia informacija niekada nebus sunaikinta – yra daromos jos kopijos. Šį aspektą iliustruoja toliau pateikiamos baudžiamosios bylos fragmentas.

Vilniaus miesto 3 apylinkės teismo baudžiamojoje byloje Nr. N-1-565-119/05 kaltinamasis 2004 m., pažeisdamas sistemos apsaugos priemones, neteisėtai prisijungė prie UAB

(duomenys neskelbtini) sukurto internetinio tinklapio ir pakeitė bei sunaikino kai kurią ten esančią įmonę reprezentuojančią informaciją. Tokiais savo veiksmais kaltinamasis neteisėtai prisijungė prie informacinės sistemos (BK 198[1] straipsnio 1 dalis) ir pakeitė ir sunaikino elektroninius duomenis (BK 196 straipsnio 1 dalis). Įmonės darbuotojai, pastebėję tokius pakeitimus tinklapyje, tinklapį administruojančiai UAB (duomenys neskelbtini) nusiuntė prašymą atkurti tinklapio turinį iš UAB (duomenys neskelbtini) daromos tinklapio rezervinės kopijos.

Darytina išvada, jog Lietuvos Respublikos įstatymų leidėjas į sunaikinimo sąvoką patalpino tokį elektroninių duomenų ištrynimą, kai po tokio veiksmo be jokių specialių duomenis atkuriančių programų tie duomenys nebėra prieinami vartotojui. Tokiai aukščiau paminėtai teismo pozicijai pritartina, kadangi taip yra apsaugomi paprasti informacinių technologijų vartotojai, kurie neturi tam tikrų specialių žinių, kaip sunaikintus duomenis būtų galima atkurti, skirtingai nuo informacinių technologijų specialistų. Nepaisant to, kad kai kurie informacinių technologijų vartotojai daro tam tikras elektroninių duomenų kopijas, tai vis tik nepanaikina pačios nusikalstamos veikos, numatytos BK 196 straipsnyje, pavojingumo.

Elektroninių duomenų sugadinimas – tai toks poveikis patiems duomenims arba laikmenai (fiziniam objektui), kurioje jie yra, kad jų turinys yra nebesuprantamas ir iškreiptas, tokiais duomenimis nebegalima naudotis pagal paskirtį. Kai asmuo sugadina laikmeną ar kitokį fizinį objektą, kuriame yra elektroniniai duomenys, kyla klausimas, kaip reikėtų vertinti tokius asmens veiksmus: kaip neteisėtą elektroninių duomenų sugadinimą (BK 196 straipsnis), kaip svetimo turto (t. y. laikmenos) sugadinimą (BK 187 straipsnis) ar kaip šių nusikalstamų veikų idealiąją sutaptį? Šiuo atveju yra svarbu išsiaiškinti asmens tyčios kryptingumą: jei asmuo siekė sugadinti elektroninius duomenis, pasirinkdamas elektroninių duomenų sugadinimo būdą – laikmenos, kurioje tokie elektroniniai duomenys yra, sugadinimą – asmens veiksmai bus kvalifikuojami kaip idealioji nusikalstamų veikų sutaptis pagal BK 196 ir 187 straipsnius. Jei asmuo dėl neatsargumo sunaikino ar sugadino laikmeną (fizinį objektą) ir dėl to buvo sugadinti elektroniniai duomenys, esantys laikmenoje, asmens veiksmai turėtų būti kvalifikuojami kaip turto sunaikinimas ar sugadinimas dėl neatsargumo (BK 188 straipsnis) ir elektroninių duomenų sugadinimas dėl neatsargumo, tačiau Lietuvos Respublikos įstatymų leidėjas BK 196 straipsnyje nėra įtvirtinęs tokios kaltės formos – neatsargumo. Todėl minėtu atveju asmuo būtų baudžiamas tik už svetimo turto sunaikinimą ar sugadinimą.

Elektroninių duomenų pašalinimas – duomenų perkėlimas į kitą informacinę/operacinę sistemą, iš pirminės sistemos duomenis ištrinant, tačiau juos išsaugant antrinėje sistemoje. Elektroninių duomenų pakeitimas – dalies duomenų turinio ištrynimas, kitų duomenų įrašymas ar kitoks poveikis turiniui, dėl ko duomenimis nebeįmanoma naudotis pagal paskirtį.

Vilniaus miesto 3 apylinkės teismo baudžiamojoje byloje Nr. N-1-565-119/05 kaltinamasis 2004 m., pažeisdamas sistemos apsaugos priemones, neteisėtai prisijungė prie UAB (duomenys neskelbtini) sukurto internetinio tinklapio ir pakeitė ten esančią įmonę reprezentuojančią informaciją. Tokiais savo veiksmais kaltinamasis neteisėtai prisijungė prie informacinės sistemos (BK 198[1] straipsnio 1 dalis) ir pakeitė elektroninius duomenis (BK 196 straipsnio 1 dalis).

Kitoje Vilniaus miesto 1 apylinkės teismo baudžiamojoje byloje Nr. 1-00857-276/2005 kaltinamasis ne mažiau kaip du kartus neteisėtai prisijungė prie (duomenys neskelbtini) internetinio forumo (URL: (duomenys neskelbtini)), apeidamas apsaugos sistemą (vartotojo vardą ir slaptažodį), bei valdė forumo turinį (pakeitė forumo pavadinimą, forumo temų pavadinimus, ištrynė kai kuriuos duomenis). Teismas tokius kaltinamojo veiksmus kvalifikavo pagal BK 198[1] straipsnio 1 dalį.

Vilniaus miesto 3 apylinkės teismo baudžiamojoje byloje Nr. N-1-565-119/05 veikos kvalifikuotos teisingai, tačiau, Vilniaus miesto 1 apylinkės teismo nuosprendis baudžiamojoje byloje Nr. 1-00857-276/2005 kritikuotinas, nes kaltinamasis, neteisėtai prisijungęs prie informacinės sistemos, pakeitė elektroninius duomenis, sunaikino kai kuriuos elektroninius duomenis, todėl jo veiksmai turėtų būti kvalifikuojami pagal BK 198[1] straipsnio 1 dalį ir BK 196 straipsnio 1 ar 3 dalį.

Naudojimosi elektroniniais duomenimis apribojimas – veiksmų atlikimas, kuriais ribojamas priėjimas prie elektroninių duomenų. Pavojinga veika ,,naudojimosi elektroniniais duomenimis apribojimas“ apima visus kitus nusikalstamus veiksmus, kurių neapima tokios pavojingos veikos kaip neteisėtas elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas, pakeitimas. Taip Lietuvos Respublikos įstatymų leidėjas įtvirtino nebaigtinį sąrašą nusikalstamų veiksmų, kuriais gali būti daromas neteisėtas poveikis elektroniniams duomenims. Tačiau naudojimosi duomenimis apribojimas ir duomenų sugadinimas yra du skirtingi dalykai, kadangi, kai asmuo apriboja naudojimąsi duomenimis, tai jis tiesiog neleidžia teisėtam duomenų vartotojui prieiti prie elektroninių duomenų, bet tokie duomenys nėra sugadinti.

Skirtingai nuo elektroninių duomenų sunaikinimo, kai apskritai sunaikintų duomenų nebeįmanoma perskaityti, pakeisti elektroniniai duomenys yra perskaitomi, tačiau dalies duomenų nebėra arba tie duomenys yra modifikuoti, t. y. kitokie nei pirminiai duomenys. Nors visur akcentuojama, jog elektroniniai duomenys yra pakeičiami arba sunaikinami negrįžtamai, elektroniniai duomenys praranda tam tikrus kokybinius požymius, tačiau informacinių ir telekomunikacinių technologijų priemonės šiandien yra taip pažengusios, kad techninių galimybių atkurti modifikuotus ar sunaikintus elektroninius duomenis vis tik yra – svarbu pabrėžti, kad net toks faktas, jog tokius elektroninius duomenis įmanoma atkurti į pradinį lygį,

buvusį dar prieš kaltininkui atliekant nusikalstamus veiksmus, nepanaikina nusikalstamą veiką padariusio asmens baudžiamosios atsakomybės.

Elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas, pakeitimas ar naudojimosi jais apribojimas yra pavojingos veikos, nes dabar daugumos fizinių ir juridinių asmenų veikla (valstybinės įstaigos, verslo subjektai) yra priklausoma nuo duomenų, saugomų elektronine forma.

BK 196 straipsnyje aprašytos veikos baigtumo momentas - toks nusikalstamą veiką padariusio asmens veiksmas, kuriuo kompiuteriniam įrenginiui duodama komanda sunaikinti, sugadinti, pašalinti ar pakeisti elektroninius duomenis ar apriboti naudojimąsi tokiais duomenimis. Visomis šiame straipsnyje nurodytomis veikomis kaltininkas neteisėtai siekia atimti arba apriboti galimybę vartotojams naudotis elektroniniais duomenimis pagal paskirtį. Nusikalstamą veiką padaręs asmuo, atlikdamas tokius neteisėtus veiksmus, pats elektroninių duomenų neįgyja, tik neteisėtai pašalina, sunaikina, sugadina, pakeičia ar apriboja naudojimąsi jais. Sistemiškai aiškinant, Lietuvos Respublikos įstatymų leidėjas vartodamas elektroninių duomenų sąvoką BK 196 straipsnyje, turi omenyje tiek viešų, tiek neviešų elektroninių duomenų pašalinimą, sunaikinimą, sugadinimą, pakeitimą ar apribojimą naudotis jais. Kai nusikalstamą veiką padaręs asmuo prieš sunaikindamas ar pakeisdamas neviešus elektroninius duomenis, dar ir neteisėtai atlieka jų kopijas, jo veika bus kvalifikuojama kaip realioji nusikalstamų veikų sutaptis pagal BK 196 ir 198 straipsnius.

Tiek informacinės sistemos darbo sutrikdymas, tiek jo nutraukimas yra pavojingos veikos, nes įvairios visuomenės gyvenimo sritys (ūkis, finansai, medicina ir pan.) yra vis daugiau priklausomos nuo informacinių sistemų, tad ir nedidelis šių sistemų darbo sutrikdymas gali sukelti tam tikrus padarinius žmogaus sveikatai, gyvybei ir pan.[69] BK 197 straipsnyje yra kriminalizuojamas trukdymas ar trikdymas teisėtai naudotis informacine sistema. Normaliu informacinės sistemos darbo funkcionavimu reikėtų laikyti operacijų, kurioms vykdyti skirta informacinė sistema, atlikimą.

Informacinės sistemos darbo sutrikdymas – tai tokie veiksmai, kurių metu arba po kurių informacinėje sistemoje neįmanoma atlikti tam tikrų funkcijų arba dalis darbo informacinėje sistemoje tampa nebeįmanomas, arba nors ir galima atlikti tam tikras funkcijas ir darbą toje informacinėje sistemoje, tačiau su dideliais ar sistemingais ir nuolatiniais trukdžiais (pavyzdžiui, informacinė sistema pateikia klaidingą informaciją ar išvis jos nepateikia). Informacinės sistemos darbo sutrikdymas gali pasireikšti labai įvairiais būdais: elektroninių duomenų įvedimu, pakeitimu, pašalinimu, naudojimosi apribojimu, paties įrenginio sunaikinimu ar sugadinimu,

[69] Bylenchuk P. D. Organized Transnational Computer Crime: the Global Problem of the Third Millenium. http://www.crime-research.org/library/Bileng.htm; prisijungimo laikas: 2007-12-11.

duomenis perduodančių jungčių, laidų pašalinimu ar sugadinimu, elektros tiekimo sutrikdymu, užverčiant informacinę sistemą dideliu kiekiu elektroninių duomenų ir pan. Tai gali sąlygoti tiek atskirų programų, duomenų bazių darbo sutrikdymą, tiek techninės įrangos ar tinklo funkcionavimo sutrikdymą. Štai 2008 m. liepos 21 d. buvo sutrikdytas interneto ryšys su Valstybinės mokesčių inspekcijos (toliau – VMI) internetiniu portalu bei elektroninio deklaravimo sistema, trikdžių priežastis - didžiulis vienu metu siunčiamų užklausų kiekis į VMI portalus. Keletą valandų VMI darbuotojai negalėjo naudotis informacinėmis sistemomis, kuriose yra sukaupti mokesčių mokėtojų duomenys bei kita svarbi informacija, mokesčių mokėtojai visiškai negalėjo naudotis elektroninio deklaravimo sistema.[70]

2000 m. Kalifornijos Aukščiausiasis Teismas nagrinėjo bylą Korporacija (duomenys neskelbtini) v. K. H., kurioje kaltinamasis, buvęs korporacijos (duomenys neskelbtini) darbuotojas, K. H. sistemingai siųsdavo daugybę elektroninių laiškų į kitų korporacijos (duomenys neskelbtini) darbuotojų elektroninio pašto dėžutes, o tai sąlygojo korporacijos (duomenys neskelbtini) centrinio kompiuterio ir tarnybinių stočių darbo sutrikdymą, dėl ko kiti korporacijos (duomenys neskelbtini) darbuotojai ne visada galėdavo naudotis savo elektroninio pašto dėžutėmis. Pats kaltinamasis tokią elektroninių laiškų ,,kampaniją" aiškino tuo, jog taip jis norėjo informuoti korporacijos (duomenys neskelbtini) darbuotojus apie tai, jog, jo manymu, korporacija (duomenys neskelbtini) vykdo diskriminuojančią įdarbinimo praktiką. K. H. buvo pripažintas kaltu ir nuteistas už korporacijos (duomenys neskelbtini) centrinio kompiuterio ir tarnybinių stočių darbo sutrikdymą.[71]

Šis pavyzdys iliustruoja, jog daugybės elektroninių laiškų siuntimas sutrikdė korporacijos centrinio kompiuterio ir tarnybinių stočių darbą, o tai pasireiškė tuo, jog korporacijos darbuotojai ne visada galėdavo naudotis elektroninio pašto dėžutėmis. Mūsų manymu, kaltinamojo veika kvalifikuota teisingai ir tokiai teismo pozicijai pritartina.

Informacinės sistemos darbo nutraukimas – tai tokie veiksmai, po kurių darbas informacinėje sistemoje tampa nebeįmanomas, informacine sistema nebeįmanoma naudotis. Mokslininkų tarpe ši nusikalstama veika dar kitaip gali būti vadinama arba prilyginama net elektroniniam terorizmui.[72]

BK 198 straipsnyje nurodytomis veikomis yra keliamas pavojus neviešų elektroninių duomenų saugumui (integruotumui, prieinamumui, konfidencialumui). Taip yra pažeidžiamas

[70] Savaitgalį bandyta sutrikdyti VMI interneto ryšį. Naujienos online. http://www.vtv.lt/naujienos/interneto-naujienos/savaitgali-bandyta-sutrikdyti-vmi-interneto-rysi.html; prisijungimo laikas: 2008-09-10.
[71] Byla Korporacija (duomenys neskelbtini) v. K. H. The Berkman Center for Internet & Society. http://cyber.law.harvard.edu /openlaw/intelvhamidi; prisijungimo laikas: 2008-09-11.
[72] Hinnen T. M. The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet // The Columbia Science and Technology Law Review. 2004, Nr. 5. P. 76.

Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnis[73], kuriuo siekiama apsaugoti duomenų komunikacijos privatumą, bei Lietuvos Respublikos Konstitucijos 22 straipsnis[74], garantuojantis asmens susirašinėjimo, pokalbių telefonu ir kitokio susižinojimo neliečiamumą. Neviešų elektroninių duomenų stebėjimas - asmuo tiesiogiai susipažįsta su tokiais elektroniniais duomenimis, tačiau jų nekopijuoja ar kaip nors kitaip nefiksuoja. Kai kurie autoriai teigia, jog nors asmuo nekopijuoja, o tik peržiūri tam tikrus duomenis, tai vis tik yra laikytina elektroninių duomenų kopijavimu.[75] Tai grindžiama tuo, jog, kai tam tikri duomenys pasirodo pažeidėjo kompiuterio monitoriuje, įvyksta duomenų perkėlimas. Tokiai nuomonei pritartina, tačiau BK prasme asmuo bus baudžiamas tik už neteisėtą tokių duomenų stebėjimą.

Neviešų elektroninių duomenų fiksavimas – tokie asmens veiksmai su neviešais elektroniniais duomenimis, kai yra daromos tokių duomenų kopijos arba pats asmuo suveda neteisėtai sužinotus neviešus elektroninius duomenis ir išsaugo materialiame (fiziniame) objekte, arba tokius duomenis užrašo popieriuje. Taigi neviešų elektroninių duomenų fiksavimas yra daug platesnė sąvoka nei tokių duomenų kopijavimas – taip Lietuvos Respublikos įstatymų leidėjas kriminalizuoja visas galimas veikas, kuriomis galima fiksuoti neviešus elektroninius duomenis ir jas ,,sutalpina“ į fiksavimo sąvoką. Šiandien informacinės technologijos yra taip pažengusios, kad leidžia greitai nukopijuoti labai didelį kiekį duomenų. Pritartina tokiai autorių nuomonei, kurie tokią veiką laiko savarankiška pavojinga veika, užtraukiančia baudžiamąją atsakomybę.[76]

Vilniaus miesto 1 apylinkės teismo baudžiamojoje byloje Nr. 1-538-463/2007 kaltinamieji, pasinaudodami programine įranga, kuri buvo skirta, veikiant vartotojui nežinant, nuotoliniame asmeniniame kompiuteryje registruoti klaviatūros paspaudimus, kopijuoti monitoriaus ekrane esančią informaciją apie asmenų kaip banko klientų vartotojų vardus ir identifikacinius kodus, ir tokiu būdu surinktą informaciją siuntė pagal užduotą šiai programai komandą į bendrininkų grupės narių kontroliuojamą ftp serverį (duomenys neskelbtini). Tokiais savo veiksmais kaltinamieji padarė nusikalstamas veikas, numatytas BK 25 straipsnio 2 dalyje ir BK 198 straipsnio 1 dalyje, t. y. neteisėtai fiksavo ir laikė neviešus elektroninius duomenis.

Manytume, jog tokiai teismų praktikai pritartina, veika kvalifikuota teisingai, nes kaltinamieji kopijavo neviešus elektroninius duomenis bei juos laikė jiems priklausančiame ftp serveryje.

---

[73] Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=19841&p_query=&p_tr2=; prisijungimo laikas: 2007-08-15.

[74] Lietuvos Respublikos Konstitucija // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=274999; prisijungimo laikas: 2007-09-10.

[75] Crimine economico e computer forenser. - Roma: Experta Edizioni, 2008. P. 96.

[76] Sieber U. Computerkriminalität und Strafrecht. - Köln: Carl Heymanns Verlag, 1980. P. 184.

Kaltininkas gali stebėti ir/arba fiksuoti neviešus elektroninius duomenis, nepažeisdamas informacinės sistemos, kurioje jie yra, apsaugos priemonių, pvz., ligoninės darbuotojai trumpam atsitraukus nuo kompiuterio ir išėjus iš patalpos, kaltininkas gali pasižiūrėti į kompiuterio ekrane esančius neviešus elektroninius duomenis. Manytume, jog Lietuvos Respublikos įstatymų leidėjas tikslingai į 198 straipsnyje numatytos nusikalstamos veikos sudėtį neįtraukė nusikalstamos veikos padarymo būdo – pažeidžiant informacinės sistemos apsaugos priemones, nes tokiu atveju liktų nekriminalizuota aukščiau paminėta veika.

Kaip ir daugelyje valstybių, taip ir Lietuvoje egzistuoja baudžiamosios normos, numatančios atsakomybę už tradicinę vagystę. Kalbant apie elektroninius duomenis, jie nėra tiesiogiai pagrobiami, o tik padaroma jų kopija, bet tie duomenys gali likti ir pas nukentėjusįjį, jei jie nėra sunaikinami. Turtui kaip vagystės dalykui yra keliami tokie reikalavimai: turto materialumas, kilnojamas turto pobūdis, ekonominė turto vertė, turto priklausomumas kitam asmeniui, daikto atskirtumas nuo gamtinės aplinkos arba žmogaus darbas, įdėtas į daikto sukūrimą.[77] Lietuvos Aukščiausiojo Teismo Teisėjų Senato 2005 m. birželio 23 d. nutarimo Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“, 4 punkte nurodyta, jog turtas pagal BK 178 ir 180 straipsnius – tai turintys vertę bei fizinius parametrus (gabaritus, svorį, skaičių, kiekį) daiktai (pvz., namų apyvokos daiktai, transporto ir gamybos priemonės, asmeniniai daiktai, pinigai ir vertybiniai popieriai). Materialumo požymio neatitinka tokie daiktai kaip ryšio paslaugos, televizijos signalas, interneto paslaugos ir informacija, todėl elektroniniai duomenys negali būti laikomi tradicinės vagystės dalyku.

Toks požiūris buvo išreikštas ir Jungtinės Karalystės Aukščiausiojo teismo byloje O. v. M., kurioje kaltinamasis, universiteto studentas, neteisėtai gavo būsimo egzamino užduočių kopijas.[78] *Jis buvo apkaltintas informacijos vagyste iš universiteto administracijos. Prokuroras teigė, jog informacija turi priklausomumo tam tikram asmeniui požymį ir, kai jos savininkas netenka informacijos dėl to, kad ji buvo pavogta, informacija per se tampa vagystės dalyku. Teismas, vadovaudamasis 1968 m. „Vagystės aktu“ pasisakė, jog šis aktas informacijos nelaiko materialu daiktu. Informacija yra nematerialus turtas.*

Tokiai teismo pozicijai pritartina, nes informacija neatitinka materialumo požymio, todėl kaltinamojo veika negali būti kvalifikuojama, remiantis Jungtinės Karalystės 1968 m. „Vagystės aktu“.

Neviešų elektroninių duomenų perėmimas – tokie asmens pavojingi veiksmai, kai duomenys yra perimami ir po to išsaugomi ar įrašomi duomenų siuntimo elektronine erdve

[77] Fedosiuk O. Nuosavybė ir turtas civiliniame ir baudžiamajame kodeksuose // Jurisprudencija. 2002, Nr. 28(20). P. 82.
[78] Ciro T. The Scarcity of Intellectual Property // The Journal of Information, Law and Technology. 2005, Nr. 1. P. 43.

proceso metu. Teisinėje literatūroje minima, jog tokia veika dažniausiai buvo tapatinama su telefoninių pokalbių perėmimu, bet technologijų ir komunikacijų pažanga lėmė, jog turi būti saugomi ir elektroniniai duomenys.[79] Galima tokia situacija, kai interneto vartotojas klaidingai įveda tinklapio adresą, tas tinklapis persiunčia vartotojo užklausą tinklapiui, kurį interneto vartotojas ir tikėjosi pasiekti. Tačiau šioje grandinėje jau atsiranda trečiasis asmuo, t. y. klaidingai suvesto adreso tinklapio administratoriai, kurie tokiu būdu gali „šnipinėti“, ką daro interneto vartotojas ir perimti duomenis. Dauguma internetinės bankininkystės sistemų naudoja protokolą HTTPS, kuriuo siunčiami duomenys yra užkoduojami taip, jog asmuo, neteisėtai perėmęs tokius duomenis, neturi galimybės juos iššifruoti.

Neviešų elektroninių duomenų įgijimas – tai veiksmai, kuriuos atlikęs asmuo gauna neviešus elektroninius duomenis. Tokiais veiksmais gali būti pirkimas, mainai, skolos atsiėmimas, dovanos gavimas ir kt. Nevieši elektroniniai duomenys yra taip pat neteisėtai įgyjami, kai kaltininkas pateikia suklastotą kokios nors institucijos ar įstaigos darbuotojo, kuris pagal savo vykdomas pareigas gali susipažinti ar gauti neviešus elektroninius duomenis, pažymėjimą ir taip neteisėtai įgyja neviešus elektroninius duomenis. Asmuo gali įgyti tokius duomenis per tarpininką arba tiesiogiai iš asmens, neteisėtai stebėjusio, fiksavusio ar perėmusio neviešus elektroninius duomenis. Taigi asmuo, neteisėtai įgijęs ar laikantis neviešus elektroninius duomenis, nors jis pats ir šių duomenų nestebėjo, nefiksavo, neperėmė, bus traukiamas baudžiamojon atsakomybėn pagal BK 198 straipsnį.

Neviešų elektroninių duomenų laikymas – neviešų elektroninių duomenų buvimas kaltininko žinioje, nepriklausomai nuo jų turėjimo laiko trukmės ar buvimo vietos (su savimi diskelyje, kompaktiniame diske, USB atmintinėje, kompiuterio kietajame diske ar kitose vietose). Paprastai laikomi tie nevieši elektroniniai duomenys, kuriuos kaltininkas perėmė ar įgijo, tačiau tam tikrais atvejais (pvz., esant bendrininkų grupei, kurioje yra du vykdytojai) neviešus elektroninius duomenis gali laikyti ir asmuo, kuris jų tiesiogiai savo veiksmais neperėmė ir neįgijo. Kai vienas bendrininkų grupės narys neteisėtai perėmė neviešus elektroninius duomenis, o kitas – neteisėtai juos laiko USB atmintinėje, tokie dviejų asmenų veiksmai bus kvalifikuojami pagal BK 25 straipsnio 2 dalį ir 198 straipsnio atitinkamą dalį.

Neviešų elektroninių duomenų pasisavinimas – tokie asmens veiksmai, kuriais nevieši elektroniniai duomenys pereina to asmens žinion. Pavyzdžiui, faktinis duomenų turėjimas savo kompiuteryje ar laikmenoje, t. y. asmuo šiuos duomenis išsisaugo savo kompiuteryje ar laikmenoje. Pasisavinimas reiškia faktinį elektroninių duomenų turėjimą materialiame (fiziniame) objekte, tačiau ši pavojinga veika neturi būti aiškinama kaip susipažinimas su elektroniniais duomenimis ir jos išsaugojimas nusikalstamą veiką padariusio asmens atmintyje.

[79] Computer law / edited by Angel J., Reed C. - Oxford: Oxford University Press, 2007. P. 162.

Nesvarbu, ar kaltininkas tokius duomenis ketina kaip nors panaudoti, ar ne, jis yra baudžiamas vien už tokios veikos atlikimą, t. y. už neviešų elektroninių duomenų pasisavinimą.

Vilniaus miesto 1 apylinkės teismo baudžiamojoje byloje Nr. 1-17-296/2008 2003 m. kaltinamasis nuotoliniu būdu neteisėtai pasidarė fizinių ir juridinių asmens elektroninių duomenų kopiją iš (duomenys neskelbtini) centrinės klientų duomenų bazės bei šią informaciją už atitinkamą mokestį parduodavo tretiesiems asmenims. Tokiais savo veiksmais kaltinamasis padarė BK 198 straipsnio 2 dalyje nurodytą nusikaltimą – neteisėtą didelę reikšmę valstybės valdymui ir ūkiui turinčių elektroninių duomenų pasisavinimą. Teisėjas, nagrinėjęs baudžiamąją bylą, nustatė, kad nusikaltimo padarymo metu baudžiamoji atsakomybė buvo numatyta tik už informacijos pasisavinimą, todėl kaltinamasis negali būti baudžiamas už informacijos platinimą.

Manytume, jog tokiai teismų praktikai pritartina, veika kvalifikuota teisingai, nes kaltininkas, pasidaręs neviešų elektroninių duomenų kopiją, taip juos pasisavino ir padarė BK 198 straipsnio 2 dalyje numatytą nusikaltimą.

Neviešų elektroninių duomenų pasisavinimas gali reikšti susipažinimą su pačiais neviešais elektroniniais duomenimis ir jų išsaugojimą materialiame (fiziniame) objekte, ir tam tikro materialaus daikto, kuriame yra užfiksuoti elektroniniai duomenys, įgijimą. Susipažinti su neviešais elektroniniais duomenimis galima ir jų tiesiogiai nestebint, pvz., kaltininkas, stebėjęs neviešus elektroninius duomenis, šių duomenų turinį papasakoja trečiajam asmeniui, o šis juos suveda į kompiuterį ir išsaugo. Manytume, jog tokie kaltininko – trečiojo asmens - veiksmai būtų kvalifikuojami ne kaip neteisėtas neviešų elektroninių duomenų stebėjimas, bet kaip neviešų elektroninių duomenų įgijimas ir/ar pasisavinimas, jei asmens tyčia buvo nukreipta įgyti ir/ar pasisavinti neviešus elektroninius duomenis.

Jei neteisėtai pasisavinti nevieši elektroniniai duomenys dar būtų ir sunaikinti, tai tokia veika būtų kvalifikuojama kaip BK 196 ir 198 straipsnių sutaptis. Pabrėžtina, jog prieiga prie tokių neviešų elektroninių duomenų gali būti tiek teisėta, tiek neteisėta, bet visais atvejais tokių duomenų perėmimas ar panaudojimas ne su pareigų ar darbo atlikimo susijusiais tikslais užtraukia baudžiamąją atsakomybę.

Neviešų elektroninių duomenų paskleidimas – tokių duomenų paleidimas į apyvartą, platinimas. Tokios pavojingos veikos baigtumo momentas – kai asmuo neteisėtai tokius neviešus elektroninius duomenis paskleidžia viešai, t. y. nuo to momento, kai su ja susipažinti gali ne tik teisėti tokių duomenų vartotojai, bet ir bent vienas tretysis asmuo, kuris įprastai tokios teisės susipažinti su tokiais neviešais elektroniniais duomenimis neturi. Duomenys gali būti paskleidžiami tiesiogiai trečiajam asmeniui ar per elektroninius forumus, naujienų grupes, interneto puslapius.

Neviešų elektroninių duomenų kitoks panaudojimas – tokie pavojingi asmens veiksmai su neviešais elektroniniais duomenimis, kurių neapima tokia pavojinga veika kaip neteisėtas neviešų elektroninių duomenų paskleidimas. Taip Lietuvos Respublikos įstatymų leidėjas įtvirtino nebaigtinį sąrašą nusikalstamų veiksmų, kuriais nevieši elektroniniai duomenys gali būti kitaip panaudojami. Kitokiu panaudojimu gali būti laikomas neviešų elektroninių duomenų naudojimas kitoms nusikalstamoms veikoms daryti, perdavimas kitiems asmenims, išmainant juos į kitus daiktus, dovanojant, apmokant skolą, atlyginant už darbą ar kitas paslaugas ir pan.

Atkreipkime dėmesį ir į BK 198 straipsnio pavadinimo ir straipsnio dalyse nurodytos veikos formuluotę. Taikant loginį analizės metodą bei sintaksiškai nagrinėjant, matome, kad straipsnio pavadinime kalbama apie „neteisėtą elektroninių duomenų perėmimą *ir* panaudojimą“, tuo tarpu straipsnio dispozicijoje minima „tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė *ar* kitaip panaudojo neviešus elektroninius duomenis“. Tai turi esminės įtakos, aiškinantis šio nusikaltimo objektyviuosius požymius, *ipso facto* tokių netikslumų BK negalima leisti. Be to, BK 198 straipsnio pavadinime yra minimi elektroniniai duomenys („Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“), kai tuo tarpu šiame straipsnyje įtvirtintų nusikalstamų veikų dispozicijose nurodyti ir šių nusikalstamų veikų dalykas yra nevieši elektroniniai duomenys. Tokie netikslumai taisytini ir 198 straipsnio pavadinimas keistinas į „ Neteisėtas *neviešų* elektroninių duomenų perėmimas *ar* panaudojimas“.

Sistemiškai analizuojant BK specialiosios dalies straipsnius, galima diskutuoti dėl 198 straipsnio ir 124, 125, 126, 295, 297 straipsnių – kol kas yra neaiškus šių nusikalstamų veikų atribojimas, be to, problema gali kilti ir derinant šių straipsnių sankcijas, pavyzdžiui, dokumento, kuriame yra valstybės paslaptis, sunaikinimas saugomas mažiau nei bet kokie nevieši elektroniniai duomenys.

Neteisėtas prisijungimas prie informacinės sistemos – veiksmai, kuriais asmuo prieina prie informacinės sistemos ar jos dalies, neturint tam teisės, be savininko leidimo. Tokia veika keliamas pavojus informacinių sistemų saugumui (konfidencialumui, integruotumui ir prieinamumui), pažeidžiamas asmenų privatumas. Neteisėtą prisijungimą prie informacinės sistemos galime palyginti su kita baudžiamojo įstatymo uždrausta veika – neteisėtu asmens būsto neliečiamumo pažeidimu. Šiuo nusikaltimu pažeidžiama žmogaus būsto neliečiamybė, kurią garantuoja Lietuvos Respublikos Konstitucijos 24 straipsnis[80]. Informacinių technologijų mokslo laimėjimai leidžia pažeisti asmens neliečiamybę kitais būdais – neteisėtai prieiti prie įstatymo saugomų asmens elektroninių duomenų, t. y. įvykdyti „elektroninį įsibrovimą“. Tai iliustruoja ir toliau pateikiamas fragmentas iš baudžiamosios bylos.

[80] Lietuvos Respublikos Konstitucija // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=274999; prisijungimo laikas: 2007-09-10.

Kaip jau buvo minėta Vilniaus miesto 3 apylinkės teismo baudžiamojoje byloje Nr. N-1-565-119/05, kaltinamasis, 2004 m., pažeisdamas sistemos apsaugos priemones, neteisėtai tris kartus prisijungdamas prie UAB (duomenys neskelbtini) sukurto internetinio tinklapio, padarė nusikalstamas veikas, numatytas BK 198[1] straipsnio 1 dalyje.

Neteisėto prisijungimo prie informacinės sistemos kaip pavojingos veikos kriminalizavimo aktualumas sparčiai auga ne tik pasaulyje (Vokietija, Norvegija, Ispanija), bet jau ir Lietuvoje. Ši veika yra kriminalizuota Lietuvos Respublikos įstatymų leidėjo BK ir yra nukreipta prieš programišių (angl. *hacker*) daromus veiksmus.[81,82] Tai yra viena iš dažniausiai padaromų nusikalstamų veikų pasaulyje, kurios tyrimų ir išaiškinimų skaičius yra atvirkščiai proporcingas tokių padaromų veikų skaičiui.[83]

Neteisėtas prisijungimas reiškia, jog asmuo neturi teisės prisijungti prie informacinės sistemos ir naudotis ten esančiais informacinės sistemos resursais. Asmuo, turintis teisę prisijungti prie tam tikrų informacinių sistemų, gali tą teisę turėti tiek dėl su darbe susijusių funkcijų vykdymu ar pareigų atlikimu, tiek užsiregistravęs kaip tam tikros informacinės sistemos vartotojas. Neteisėta prieiga gali būti suprantama tiek kaip pasinaudojimas informacinėje sistemoje esančiomis „skylėmis“, pvz., ugniasienių tam tikrais nustatymais, tiek generuojant ir atitaikant slaptažodžius bei prisijungimo kodus, pasinaudojant svetimu vartotojo vardu (tapatybės vagystė).[84] Nusikaltimo baigtumo momentas – kompiuterio komandos, kurią kaltininkas duoda kompiuteriui pradėti „įveikti“ informacinę sistemą, proceso pabaiga, t.y. tokia kompiuterio komandos proceso pabaiga, kuria kaltininkas prisijungia prie informacinės sistemos.

Akademikų visuomenėje vyrauja nuomonė, jog vien neteisėtas prisijungimas prie informacinės sistemos, įveikiant apsaugos priemones, nėra ta pavojinga veika, kurią reikėtų vadinti nusikalstama veika.[85] Ši nuomonė kritikuotina ir galima diskutuoti, ar šią veiką reiktų konstruoti ne kaip formaliosios, bet kaip materialiosios sudėties, nurodant padarytą žalos vertę, o vien už neteisėtą prisijungimą prie informacinės sistemos, įveikiant apsaugos priemones, reikėtų numatyti administracinę atsakomybę. Vokietijos informatikos ir kompiuterinių technologijų teisės profesorius U. Sieber mano, kad neteisėtas prisijungimas prie informacinės sistemos yra prasiskverbimas į tokias sistemas, susijęs su pasitenkinimu, kad įmanoma įveikti informacinės

[81] Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai // Jurisprudencija. 2003, Nr. 47(39). P. 24.
[82] Jordan T., Taylor P. A Sociology of Hackers // The Sociological Review. 1998, Nr. 2. P. 760.
[83] Computer-Related Crime. The Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 18-25 April 2005, Bangkok, Thailand. http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf; prisijungimo laikas: 2008-08-23.
[84] Desai M. S., Richards T. S. System Insecurity – Firewalls // Information Management & Computer Security. 2002, Nr. 10(3). P. 51.
[85] Grabosky P. Computer Crime: a Criminological Overview. – Sidney, 2000. P. 143.

sistemos apsaugos priemones.[86] Jis išskiria dvi situacijas: kai neteisėtai prisijungus prie informacinės sistemos, nepadaroma jokia žala, bet pažeidžiamas informacinės sistemos integralumas ir vientisumas ir kai, neteisėtai prisijungus prie informacinės sistemos, padaroma žala.

Pritariant šiai nuomonei, aišku tai, kad netgi vien neteisėtas prisijungimas prie informacinės sistemos, apeinant apsaugos priemones, turėtų būti laikomas jei ne baudžiamuoju nusižengimu ar nusikaltimu, tai bent jau administraciniu teisės pažeidimu. Konvencijoje dėl elektroninių nusikaltimų[87] yra numatyta, jog valstybės turi nustatyti baudžiamąją atsakomybę arba imtis kitų teisinių priemonių atsakomybei nustatyti, tad valstybėms narėms yra palikta teisė ne tik nustatyti baudžiamąją atsakomybę, bet ir tam tikras veikas įvardinti administracinės teisės pažeidimais. Tokiose valstybėse kaip Suomija, Didžioji Britanija yra numatyta baudžiamoji atsakomybė už neteisėtą prisijungimą, nepadarant žalos, o neteisėtas prisijungimas, kai tuo buvo padaryta žalos, traktuojamas kaip kvalifikuojantis požymis.[88]

Vien neteisėtas prisijungimas prie informacinės sistemos pažeidžia tos informacinės sistemos integralumą, vientisumą ir kelia grėsmę toje informacinėje sistemoje laikomų duomenų slaptumui ir konfidencialumui. Be to, visada išlieka galimybė, jog kaltininkas, neteisėtai prisijungęs prie informacinės sistemos, nespės ar negalės pasinaudoti ten esančiais šios sistemos resursais.

Jungtinės Karalystės apeliacinio teismo byloje R v. S. G. ir R. S. kaltinamieji S. G. ir R. S. neteisėtai prisijungė, prie (duomenys neskelbtini) telekomo informacinės sistemos ir paliko žinutę Jungtinės Karalystės princui ,,Laba diena, ponas Dukesai“.[89] Iš kaltinamųjų parodymų paaiškėjo, jog pagrindinis įsilaužimo tikslas buvo išryškinti saugumo ,,skyles“ (duomenys neskelbtini) telekomo tinkle.

Aukščiau pateiktas pavyzdys iliustruoja, jog praktikoje gali būti ir pasitaiko tokių situacijų, jog asmenys dėl vienų ar kitų priežasčių siekia tik neteisėtai prisijungti prie informacinės sistemos ir nesiekia pasinaudoti toje sistemoje esančiais elektroniniais duomenimis. Mūsų manymu, vien neteisėtas prisijungimas prie informacinės sistemos turi būti kriminalizuotas, kadangi tai pažeidžia informacinės sistemos integralumą, prieinamumą ir vientisumą.

[86] Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study. http://law.scu.edu/inter national /File/Sieber_final.pdf; prisijungimo laikas: 2008-01-26.
[87] Convention on Cybercrime // http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; prisijungimo laikas: 2007-10-12.
[88] Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study. http://law.scu.edu/inter national /File/Sieber_final.pdf; prisijungimo laikas: 2008-01-26.
[89] Byla R v. S. G. ir R. S. Discuss Law. http://www.swarb.co.uk/lawb/cpucmaRvGold.shtml; prisijungimo laikas: 2008-07-05.

Neteisėtas prisijungimas prie informacinės sistemos, pažeidžiant apsaugos priemones, yra labai dažnas kitų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui padarymo būdas. Asmuo, neteisėtai prisijungęs prie informacinės sistemos, turi galimybę stebėti, kopijuoti tam tikrus duomenis, kurie gali būti konfidencialūs, ištrinti ar pakeisti duomenis, sutrikdyti informacinės sistemos darbą. Tad jei asmuo neteisėtai prisijungė prie informacinės sistemos ir sunaikino dalį ten esančių elektroninių duomenų, tai jo veika bus kvalifikuojama kaip nusikalstamų veikų sutaptis pagal BK 196 ir 198[1] straipsnius. Jei asmuo neteisėtai prisijungė prie banko informacinės sistemos, ten atliko tam tikrų duomenų pakeitimus, dėl kurių jis gavo finansinės naudos, tai jo veika bus kvalifikuojama pagal BK 196, 198[1] ir 182 straipsnius.

Vilniaus miesto 1 apylinkės teismo baudžiamojoje byloje Nr. 1-538-463/2007 kaltinamieji neteisėtai prisijungė prie (duomenys neskelbtini) banko klientams teikiamų internetinės bankininkystės sąskaitų su neteisėtai gautais vartotojo vardais bei slaptažodžiais, atliko pinigų pavedimus ir vėliau juos išgrynino su neteisėtai gauta banko mokėjimo kortele. Kaltinamieji padarė nusikalstamas veikas, numatytas BK 198[1] straipsnio 1 dalyje, 182 straipsnio 1 dalyje ir 214 straipsnio 1 dalyje.

Kitoje, jau minėtoje, Vilniaus miesto 3 apylinkės teismo baudžiamojoje byloje Nr. N-1-565-119/05 kaltinamasis po to, kai, pažeisdamas sistemos apsaugos priemones, neteisėtai prisijungė prie UAB (duomenys neskelbtini) sukurto internetinio tinklapio, keletą kartų siuntė UAB (duomenys neskelbtini) elektroninius laiškus, reikalaudamas perduoti 1500 Lt ir nešiojamą kompiuterį, už tai, kad jis atskleis būdą, kaip įsibrovė į tinklapį. Kaltinamojo veiksmai buvo kvalifikuoti kaip neteisėtas prisijungimas prie informacinės sistemos (BK 198[1]straipsnio 1 dalis) ir turto prievartavimas (BK 181 straipsnio 1 dalis).

Tokiai teismų praktikai pritartina, kaltinamųjų veikos kvalifikuotos teisingai, nes kaltinamieji, prisijungę prie informacinės sistemos, siekė gauti ir finansinės naudos.

BK 198[2] straipsnis skirtas atskiru nusikaltimu įvardyti specifinių neteisėtų veikų, susijusių su įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, padarymą, siekiant įvykdyti kitas nusikalstamas veikas. Neteisėtas įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų gaminimas – toks procesas, kurio metu sukuriami įrenginiai ar programinė įranga, slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys. Gaminimas pripažįstamas baigtu, kai tokie įrenginiai, programinė įranga, slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys yra tinkami nusikalstamoms veikoms daryti. Išskirtinas programų – virusų sukūrimas, kadangi dažnai tokios virusinės programos veikia be žmogaus nurodymų ir padaro labai didelės žalos.[90]

[90] Computer Intrusions and Attacks // The Electronic Library. 1999, Nr. 17(2). P. 118.

Tačiau įstatymų leidėjas, turėdamas omenyje, jog ne tik virusai gali padaryti žalos, bet ir tokios programos kaip „Trojos arklys“ ir kitos, naudoja programinės įrangos sąvoką.

Neteisėtas įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų gabenimas – tai įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų buvimo, laikymo vietos pakeitimas, perkeliant juos didesniais nuotoliais (pavyzdžiui, iš miesto į kaimą, iš vieno miesto į kitą miestą, iš gatvės į gatvę ir pan.). Įrenginiai ar programinė įranga, taip pat slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys gali būti gabenami, vežant jas transporto priemone, nešant lagamine, kišenėse, krepšyje ir pan. Gabenimu neturėtų būti laikomas įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų perkėlimas iš vienos vietos į kitą toje pat patalpoje, iš vienos laikmenos į kitą, iš vieno pastato į kitą pastatą, toje pat namų valdoje, iš namo į kiemą ar lauką kaltininko sodyboje. Čia reikėtų paminėti ir tokią situaciją, kai, pvz., slaptažodžiai internetu yra persiunčiami kitam asmeniui. Siuntimas nuo gabenimo skiriasi tuo, jog siuntėjas medžiagų perkėlimo procese nedalyvauja. Tokios programinės įrangos, slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų siuntimas gali būti labai dažnas atvejis, nes visa tai gali būti perduodama internetu. Tokiu atveju kaltininkas, siunčiantis slaptažodžius internetu kitam asmeniui, liktų nenubaustas, todėl manytume, jog į BK 198[2] straipsnyje nurodyto nusikaltimo sudėtį reikėtų įtraukti ir tokią pavojingą veiką kaip įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų siuntimą.

Neteisėtas įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų pardavimas – tai yra įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų vienas iš platinimo būdų. Paprastai tai įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų perdavimas kitam asmeniui už tam tikrą pinigų sumą.

Neteisėtas įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų kitoks platinimas – tai įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų perdavimas kitiems asmenims, išleidimas į apyvartą, išmainant juos į kitus daiktus, dovanojant, apmokant skolą, atlyginant už darbą ar kitas paslaugas ir pan. Programinė įranga, slaptažodžiai, prisijungimo kodai ar kitokie duomenys gali būti platinami per kitus asmenis, naujienų grupėse, interneto puslapiuose, elektroniniuose forumuose ir kt.

Neteisėtas įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų įgijimas – tai tokie veiksmai, kuriuos atlikęs asmuo gauna programinę

įrangą, slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis. Tai gali būti pirkimas, mainai ir pan.

Neteisėtas įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų laikymas – įrenginių, programinės įrangos, slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų buvimas asmens žinioje, nepriklausomai nuo jų turėjimo laiko trukmės ar buvimo vietos (turėjimas su savimi laikmenose, kompiuteryje patalpoje, slėptuvėje ar kitose vietose). Paprastai laikomi tie slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys, kuriuos asmuo buvo pagaminęs ar įgijęs. Tam tikrais atvejais (pavyzdžiui, esant grupei iš anksto susitarusių asmenų) slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis gali laikyti ir asmuo, kuris jų negamino ir neįgijo.

Minėtoje Vilniaus miesto 1 apylinkės teismo baudžiamojoje byloje Nr. 1-538-463/2007 kaltinamieji neteisėtai laikė nusikalstamai veikai daryti pritaikytą asmeninį kompiuterį „Compaq“, kuris buvo skirtas įrašinėti programinę įrangą, skirtą nusikalstamoms veikoms daryti (veikiant vartotojui nežinant, nuotoliniame asmeniniame kompiuteryje registruoti klaviatūros paspaudimus, kopijuoti monitoriaus ekrane esančią informaciją apie asmenų kaip banko klientų vartotojų vardus ir identifikacinius kodus), į kompaktinius diskus. Kaltinamieji kompaktinius diskus su joje įrašyta programine įranga, tiesiogiai skirta nusikalstamoms veikoms daryti, pardavinėjo kitiems asmenims. Tokie kaltinamųjų veiksmai buvo kvalifikuoti pagal BK 25 straipsnio 2 dalį ir BK 198[2] straipsnio 1 dalį kaip neteisėtas įrenginių, tiesiogiai skirtų daryti nusikalstamas veikas, laikymas ir programinės įrangos, tiesiogiai skirtos daryti nusikalstamas veikas, pardavimas.

Tokiai teismo pozicijai pritartina, kaltinamųjų veikos kvalifikuotos teisingai, nes kaltinamieji savo žinioje turėjo kompiuterį ir jame instaliuotą programinę įrangą, skirtus nusikalstamoms veikoms daryti, bei pardavinėjo programinės įrangos kopijas, skirtas nusikalstamoms veikos daryti, tretiesiems asmenims.

BK 198[2] straipsnis negali būti aiškinamas kaip užtraukiantis baudžiamąją atsakomybę, kai šio straipsnio 1 dalyje minimas gaminimas, gabenimas, pardavimas, platinimas kitaip, įgijimas ar laikymas nėra skirtas daryti nusikalstamoms veikoms, o tik sankcionuotam informacinės sistemos tikrinimui, testavimui arba jos apsaugai.

Analizuojant BK 198[2] straipsnio dispoziciją, asmuo bus traukiamas baudžiamojon atsakomybėn tik tokiu atveju, jei jis gamino, gabeno, pardavė ar kitaip platino bent 2 įrenginius, slaptažodžius ar prisijungimo kodus, tiesiogiai skirtus nusikalstamoms veikoms daryti, nes minimo straipsnio dispozicijoje vartojama daugiskaita: „tas, kas neteisėtai gamino, gabeno, pardavė ar kitaip platino *įrenginius* ar *programinę įrangą*, taip pat *slaptažodžius, prisijungimo kodus* ar *kitokius panašius duomenis*, tiesiogiai skirtus daryti nusikalstamas veikas, arba tuo

pačiu tikslu juos įgijo ar laikė“.[91] Konvencijoje dėl elektroninių nusikaltimų nurodyta, jog valstybės gali reikalauti, kad baudžiamoji atsakomybė kiltų, tik turint keletą tokių dalykų. Ar Lietuvos Respublikos įstatymų leidėjas pasinaudojo šia konvencijoje įtvirtinta nuostata, ar tai tėra tik gramatinis netikslumas? Mūsų nuomone, Lietuvos Respublikos įstatymų leidėjas suvokė šios veikos pavojingumą analizuojant tokias situacijas, kai asmuo sistemingai, reguliariai daro tokias nusikalstamas veikas. Be to, jau pati veika (gamyba, gabenimas, pardavimas, platinimas kitaip, įgijimas, laikymas) suponuoja, jog užsiimama bent jau kelių įrenginių, programinės įrangos, slaptažodžių, prisijungimo kodų ir kitokių duomenų neteisėtu disponavimu, t. y. rodo veikos sistemingumą ir tęstinumą. Mokslininkų tarpe yra išreiškiama ir tokia nuomonė, kad šio straipsnio esmę sudaro ne kiekybinis veiksnys, tačiau įrenginių, programinės įrangos, slaptažodžių, prisijungimo kodų ir kitokių duomenų savybės.[92] Vis tik manytume, jog Lietuvos Respublikos įstatymų leidėjas pasinaudojo Konvencijoje dėl elektroninių nusikaltimų 6 straipsnio 1 dalies b punkte numatyta nuostata, jog valstybė gali reikalauti, kad baudžiamoji atsakomybė būtų užtraukiama, tik turint keletą tokių dalykų.

BK XXX skyriuje yra įtvirtintos tiek materialios nusikalstamų veikų sudėtys (BK 196, 197 straipsniai), tiek formalios sudėtys (BK 198, 198¹, 198² straipsniai). Taigi už tokias veikas kaip neteisėtas elektroninių duomenų perėmimas ir panaudojimas, neteisėtas prisijungimas prie informacinės sistemos ir neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis Lietuvos Respublikos įstatymų leidėjas numato baudžiamąją atsakomybę, nereikalaudamas jokių dėl tokios nusikalstamos veikos kilusių padarinių. Be abejo, gali būti ir taip, jog padariniai atsiras, tačiau iš esmės jie neturi įtakos kvalifikuojant nusikalstamą veiką, tačiau turi įtakos, skiriant bausmę.

Reziumuojant, BK XXX skyriuje įtvirtintas nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui kaip pavojingas veikas apibūdinantys nusikalstami veiksmai (neteisėtai sunaikino, sugadino, pašalino ar pakeitė ar kitais būdais apribojo (BK 196 straipsnis), neteisėtai sutrikdė ar nutraukė (BK 197 straipsnis), neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo (BK 198 straipsnis), neteisėtai prisijungė (BK 198^1 straipsnis), neteisėtai gamino, gabeno, pardavė ar kitaip platino arba tuo pačiu tikslu įgijo ar laikė (BK 198^2 straipsnis)) kelia teorinių ir teisinių praktinių problemų: doktrininis ir mokslinis šių pavojingų veikų aiškinimas yra nepakankamas. Be to, teismai netinkamai taiko baudžiamuosius įstatymus nusikalstamų veikų elektroninių duomenų ir informacinių sistemų

[91] Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Lietuvos Respublikos baudžiamasis kodeksas (su pakeitimais ir papildymais iki 2008 m. birželio 12 d.) // Valstybės žinios. 2004, Nr. 25-760.

[92] Forensic Computer Crime Investigation / edited by Johnson Th. A. – New York: CRC Press, Taylor & Francis, 2006. P. 88.

saugumui ir daro klaidas, neteisingai kvalifikuodami nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui padariusių asmenų pavojingas veikas.

2.2.3. Pavojingi padariniai kaip nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių objektyvusis požymis

Neteisėtas poveikis elektroniniams duomenims ir neteisėtas poveikis informacinei sistemai yra tokios nusikalstamos veikos, kurios pripažįstamos baigtinėmis, atsiradus nusikalstamos veikos sudėtyje numatytiems padariniams. Baudžiamojo įstatymo dispozicijoje minimi padariniai tampa įrodinėjimo dalyku baudžiamojoje byloje.

BK XXX skyriaus straipsnių dispozicijose numatyti tokie padariniai kaip didelė žala ir nedidelė žala. Šie padariniai yra vertinamieji nusikalstamos veikos sudėties požymiai ir jie dažnai aiškinami, pasinaudojant oficialiu įstatymo aiškinimu, tačiau, kalbant apie nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, nėra oficialaus Lietuvos Respublikos įstatymų leidėjo aiškinimo, ką reiškia didelė ar nedidelė žala.[93] Tokiu atveju mums reikia pasiremti įvairiais doktrininiais įstatymo aiškinimo šaltiniais. Kadangi Lietuvos Respublikos įstatymų leidėjas BK XXX skyriuje nedetalizavo galimų padarinių rūšies, tai didelė ar nedidelė žala apima ne tik turtinę, bet ir neturtinę (kitokią) žalą. Kai kurie mokslininkai teigia, jog, norint nustatyti, kas yra didelė ar nedidelė turtinė žala, padaryta nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui, reikia vadovautis BK 190 ir 212 straipsniuose esančiu išaiškinimu.[94] Baudžiamojoje teisėje draudžiama taikyti analogiją, todėl, manytume, kad šis požiūris nėra priimtinas, nes skiriasi BK XXX ir XXXI, XXVIII skyriuose saugomos vertybės. Teismui BK 212 straipsnis, nagrinėjant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, turėtų būti tik kaip orientacinio pobūdžio rekomendacija, sprendžiant, ar padaryta žala yra didelė, ar ne. Atsižvelgiant į BK struktūrą, nors ir netikslinga bei sudėtinga Lietuvos Respublikos įstatymų leidėjui būtų detalizuoti vertinamąjį didelės ar nedidelės žalos turinį, tačiau būtina užtikrinti didelės ar nedidelės žalos turinio kriterijų vienodumą baudžiamajame įstatyme. Teismams būtų paliekama daug laisvės įvertinti padarytą turtinę žalą ir nuspręsti dėl jos dydžio vertinimo, jei tokiais didelės ar nedidelės žalos turinio kriterijais laikytume tiesiogiai padarytos žalos dydį, kilusius nuostolius, nukentėjusiojo asmens turtinę padėtį, pvz., stambiai tarptautinei korporacijai tam tikrų elektroninių duomenų sunaikinimas gali reikšti nedidelę žalą, tačiau tokios pat vertės elektroninių duomenų sunaikinimas mažai, smulkiai įmonei gali reikšti net bankrotą.

[93] Sabaliauskas G. Informacijos saugumas internete: teisininkų ir informatikų problema // Justitia. 2001, Nr. 1. P. 29.
[94] Civilka M. ir kt. Informacinių technologijų teisė. - Vilnius: NVO Teisės institutas, 2004. P. 215.

Minėtoje Vilniaus miesto 3 apylinkės teismo baudžiamojoje byloje Nr. N-1-565-119/05 dėl neteisėtais kaltinamojo veiksmais sukeltų papildomų ir neplanuotų darbų įmonė patyrė 21 tūkst. Lt žalą – įmonė turėjo pirkti tinklapį sukūrusios įmonės paslaugas tinklapio sutvarkymui bei programinės įrangos patobulinimui. Teismas 21 tūkst. Lt žalą įvertino kaip didelę turtinę žalą.

Mūsų manymu, tokiai teismo pozicijai pritartina, nes įmonė, besireklamuojanti interneto tinklapyje, pagal finansinius rodiklius ir gaunamą pelną buvo nedidelė, patirtoms išlaidoms padengti prireikė banko paskolos.

Be to, nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui žala gali būti padaroma ne automatiniu (užverčiant informacinę sistemą dideliu kiekiu elektroninių duomenų), bet manualiniu (rankiniu) būdu – paties įrenginio sunaikinimu ar sugadinimu, duomenis perduodančių jungčių, laidų pašalinimu ar sugadinimu, elektros tiekimo sutrikdymu. 2005 m. lapkričio mėn. buvo pasikėsinta vandeniu užlieti Vilniaus greitosios medicinos pagalbos centro serverinės įrangą. Į serverinę patekęs vanduo galėjo sunaikinti telekomunikacinį mazgą, dėl ko būtų nebeveikęs telefonas 03, pacientai nebegalėtų prisiskambinti, būtų sunaikinti visi serveryje saugomi įrašai apie kvietimus ir kiti duomenys.[95]

Manytume, kad visais atvejais, kai nukentėjusiojo asmens patirta žala sudaro kitos BK numatytos nusikaltimo ar baudžiamojo nusižengimo sudėties objektyvųjį požymį, tai turėtų būti vertinama kaip didelė žala. Jei aukščiau aprašytoje situacijoje serverinės įranga būtų užlieta vandeniu, dėl ko būtų sutrikdytas informacinių sistemų darbas bei sunaikinti elektroniniai duomenys, nusikalstamas veikas padariusio asmens veiksmai galėtų būti kvalifikuojami kaip idealioji nusikaltimų sutaptis pagal 196 straipsnio 1 dalį, 197 straipsnio 1 dalį ir 187 straipsnio 1 dalį. Mūsų nuomone, vien situacijos aplinkybės leidžia daryti išvadą, jog tokiu atveju būtų padaryta didelė žala, o taip pat Vilniaus greitosios medicinos pagalbos centro patirta turtinė žala sudaro kitos BK numatytos nusikaltimo sudėties objektyvųjį požymį (BK 187 straipsnis).

Kyla klausimas, kaip reikėtų kvalifikuoti tokią veiką, kai tokia nusikalstama veika padaroma, nepadarant žalos. Vis tik kadangi nusikalstamų veikų sudėtis yra materiali, tokių neteisėtų veiksmų, nurodytų 196 ar 197 straipsnių dispozicijose, atlikimas, kai asmuo siekia padaryti žalos, tačiau nusikalstamos veikos sudėtyje aprašyti padariniai neatsiranda, leistų padarytą veiką kvalifikuoti kaip pasikėsinimą, inkriminuojant BK 22 straipsnio 1 dalį ir 196 ar 197 straipsnį. Jei asmuo neteisėtai pašalino elektroninius duomenis ir tokiais savo veiksmais siekė padaryti didelės žalos, bet padarė nedidelės žalos, tai jo veika kvalifikuotina kaip pasikėsinimas neteisėtai pašalinti elektroninius duomenis, padarant didelės žalos (BK 22

[95] Mėginta sutrikdyti Vilniaus greitosios medicinos pagalbos stoties darbą. http://sena.sam.lt/images/Dokumentai/Apzvalgos/tns%20media-intelligence%20informacija%20sam%2051115%20(tv,%20radijas).htm#0_5; prisijungimo laikas: 2008-09-01.

straipsnio 1 dalis ir 196 straipsnio 1 dalis). Jei asmuo neteisėtai sugadino elektroninius duomenis, siekdamas padaryti nedidelės žalos, bet tokiais savo veiksmais padarė didelės žalos, jo veika kvalifikuotina kaip baigtas neteisėtas elektroninių duomenų sugadinimas, padarant didelės žalos (BK 196 straipsnio 1 dalis).

Jungtinių Amerikos Valstijų Federalinių tyrimų biuro duomenimis, 2002 m. apklausus 250 didžiausių kompanijų pasaulyje, paaiškėjo, kad patirti nuostoliai dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui siekė net 300 mln. Jungtinių Amerikos Valstijų dolerių, ir šie nuostoliai kasmet vidutiniškai auga po 20%.[96] Kai kurie mokslininkai, atsižvelgiant į tokį šių nusikalstamų veikų specifiškumą, kompiuterinius nusikaltimus gretina su terorizmu.[97] Be to, nusikalstamų veikų elektroninių domenų ir informacinių sistemų saugumui specifiškumas pasireiškia dar ir tuo, jog šiomis veikomis gali būti padaroma ne tik turtinė, bet ir neturtinė žala. Neturtinės žalos dydį reikėtų vertinti, atsižvelgiant į žalos pasekmes, žalą padariusio asmens kaltę, nukentėjusio asmens teisių ir laisvių suvaržymo laipsnį, nukentėjusiųjų skaičių ir kitas aplinkybes, pvz., dėl informacinės sistemos darbo sutrikdymo gali pablogėti juridinio asmens reputacija, prarandami klientai, investuotojai ir pan. Teismui čia taip pat paliekama daug laisvės vertinti padarytą neturtinę žalą, atsižvelgiant į jos pasekmes, šią žalą padariusio asmens kaltę bei kitas turinčias reikšmės bylai aplinkybes, taip pat į sąžiningumo, teisingumo ir protingumo kriterijus.

Minėtoje Vilniaus miesto 1 apylinkės teismo baudžiamojoje byloje Nr. 1-17-296/2008 kaltinamasis, neteisėtai pasisavindamas didelę reikšmę valstybės valdymui ir ūkiui turinčius neviešus elektroninius duomenis iš (duomenys neskelbtini) centrinės duomenų bazės (BK 198 straipsnio 2 dalis), taip sumenkino (duomenys neskelbtini) kaip valstybės institucijos reputaciją. Jos atstovai buvo pareiškę 200 tūkst. Lt civilinį ieškinį neturtinės žalos atlyginimui. Teismas jį patenkino tik iš dalies – sumažino iki 20 tūkst. Lt.

Mūsų manymu, tokiai teismo pozicijai pritartina, nes teismas nuosprendyje įvertino aplinkybių visumą – tiek žalos pasekmes, žalą padariusio asmens kaltę, nukentėjusiojo asmens teisių ir laisvių suvaržymo bei reputacijos sumenkinimo laipsnį.

Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte[98] yra pasakyta, jog didelės žalos išaiškinimas paliekamas kiekvienos valstybės įstatymų leidėjo kompetencijai. Kadangi iškyla problema apibrėžti didelės ir nedidelės žalos vertę, turtinės ir neturtinės žalos turinį, manytume, kad čia turėtų pasisakyti teismai, formuodami teisminę praktiką, vertindami kiekvienos bylos konkrečias aplinkybes ir kazualiniais sprendimais užpildydami šio objektyviojo

[96] Trust and Privacy Online: Why Americans Want to Rewrite the Rules // The Internet Life Report. – Boston, 2000. P. 16.
[97] Icove D. ir kt. Computer Crime: Crimefighter‘s Handbook. – New York: O’Reilly Media Inc, 1995. P. 284.
[98] Convention on Cybercrime. Explanatory Report // http://conventions.coe.int/Treaty/en/Report s/Html/185.htm; prisijungimo laikas: 2007-10-24.

požymio turinį bei atskleisdami jo esmę. Turime būti pasiruošę, kad šių sąvokų turinys ir samprata baudžiamųjų įstatymų kontekste bus atskleista per ilgą laiką, nes menkas teisminės praktikos buvimas, nagrinėjant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, bei didelių finansinių lėšų poreikis, atskleidžiant tokias nusikalstamas veikas, stabdo aiškinimosi ir praktikos formavimo procesą. Detalumas ir aiškumas gali būti pasiektas tik tada, kai praktiniai šių nusikalstamų veikų aspektai atitinka teorinius aspektus.

Be to, BK 197 straipsnio 1 dalis ne visai atitinka Konvencijos dėl elektroninių nusikaltimų nuostatas.[99] Pagal BK 197 straipsnį reikalaujama, kad veika būtų padaroma didelė žala, tačiau Konvencijos dėl elektroninių nusikaltimų 5 straipsnis numato įpareigojimą nustatyti baudžiamąją atsakomybę už sąmoningą ir neteisėtą didelį kompiuterinės sistemos darbo trukdymą, t. y. nesieja baudžiamosios atsakomybės kilimo su nusikalstama veika sukeliamais padariniais. Taigi ši konvencija nenumato galimybės apriboti šių nuostatų taikymą, tik esant didelės žalos požymiui. Diskutuotina, kas yra didelis kompiuterinės sistemos darbo trukdymas ir ar didelis kompiuterinės sistemos darbo trukdymas visada sąlygoja žalą. Lietuvos Respublikos įstatymų leidėjas didelį informacinės sistemos darbo sutrikdymą ar nutraukimą sieja su pasekmėmis – didele žala. Taigi konvencijoje įtvirtintas didelis kompiuterinės sistemos darbo trukdymas Lietuvos Respublikos įstatymų leidėjo apibrėžiamas per informacinės sistemos darbo sutrikdymą ar nutraukimą, padarant didelės žalos.

Remiantis Pamatiniu sprendimu[100], kurį Lietuvos Respublikos įstatymų leidėjas įgyvendino BK XXX skyriaus nuostatomis, BK 196 ir 197 straipsniuose numatytos pasekmės neatitinka Pamatinio sprendimo 3 ir 4 straipsnių nuostatų, kadangi už neteisėtą įsikišimą į duomenis ar informacinę sistemą turi būti baudžiama „ir tais atvejais, kurie nėra reikšmingi“. Vadinasi, tuo yra siekiama, kad minėtus straipsnius perkeliantys nacionaliniai teisės aktai nebūtų taikomi mažareikšmėms veikoms, o ne nustatyti nusikalstamos veikos padarinius. Lietuvos Respublikos įstatymų leidėjas už nusikalstamas veikas, kurios nėra reikšmingos, tačiau dėl jų atsiranda žalos, BK 196 straipsnio 3 dalyje ir 197 straipsnio 3 dalyje numatė baudžiamąjį nusižengimą.

Be to, Pamatinio sprendimo 7 straipsnio 2 dalyje nurodyta, jog valstybės narės nusikalstamos veikos padarinius gali numatyti kaip veiką kvalifikuojančius požymius. Tačiau Konvencijoje dėl elektroninių nusikaltimų 4 straipsnyje nurodyta, jog valstybė gali pasilikti teisę reikalauti, kad nusikalstamos veikos poveikis duomenims sudėtyje turi būti nurodytos pasekmės - didelė žala. Todėl Lietuvos Respublikos įstatymų leidėjas turėtų pašalinti tokius prieštaravimus,

[99] Convention on Cybercrime // http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; prisijungimo laikas: 2007-10-12.

[100] 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=COM:2005:0583:FIN:LT:HTML; prisijungimo laikas: 2008-08-27.

sutinkamai tiek su Konvencijos dėl elektroninių nusikaltimų, tiek su Pamatinio sprendimo nuostatomis.

Reziumuojant, pasakytina, jog BK XXX skyriaus straipsnių dispozicijose numatytais padariniais (didelė žala, nedidelė žala) yra padaroma turtinė ir neturtinė žala. Kai nukentėjusiojo asmens patirta žala sudaro kitos BK numatytos nusikaltimo ar baudžiamojo nusižengimo sudėties objektyvųjį požymį, tai turėtų būti vertinama kaip didelė žala. Atsižvelgiant į BK struktūrą, nors ir netikslinga bei sudėtinga Lietuvos Respublikos įstatymų leidėjui būtų detalizuoti vertinamąjį didelės ar nedidelės žalos turinį, tačiau būtina užtikrinti didelės ar nedidelės žalos turinio kriterijų vienodumą baudžiamajame įstatyme, nes jų nesant, teismai bei ikiteisminio tyrimo institucijų pareigūnai didelės ar nedidelės žalos turinį gali komentuoti nevienodai. Tokiais kriterijais galėtų būti tiesiogiai padarytos žalos dydis, kilę nuostoliai, nukentėjusiojo asmens turtinė padėtis, reputacijos pabloginimo laipsnis, žalą padariusio asmens kaltė, nukentėjusio asmens teisių ir laisvių suvaržymo laipsnis, nukentėjusiųjų skaičius.

2.2.4. Nusikalstamos veikos dalykas kaip nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių objektyvusis požymis

Aptarėme nusikalstamos veikos sudėties pagrindinius objektyviuosius požymius, tačiau be šių požymių yra ir fakultatyvūs objektyvieji nusikalstamos veikos požymiai, kurie nulemia veikos nusikalstamumą ir baudžiamumą tik tada, jei yra aprašyti BK specialiosios dalies straipsnio dispozicijoje. Jei fakultatyviniai objektyvieji nusikalstamos veikos sudėties požymiai nenumatyti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui straipsnių dispozicijose, šie požymiai turi įtakos, skiriant bausmę ir individualizuojant baudžiamąją atsakomybę.

Nusikalstamos veikos dalykas yra baudžiamojo įstatymo saugomų vertybių materiali išraiška. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui dalykas – elektroniniai duomenys (BK 196, 198 straipsniai) arba informacinės sistemos (BK 197, 198[1] straipsniai). Juos veikiant yra pažeidžiamos baudžiamojo įstatymo saugomos vertybės – elektroninių duomenų ir informacinių sistemų saugumas. Šitaip nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui yra aiškiai atribojamos nuo nusikalstamų veikų nuosavybei, turtinėms teisėms ir turtiniams interesams, nes pačios kompiuterinės įrangos ar jos priedų vagystė, sugadinimas patenka į šių nusikalstamų veikų reglamentavimo dalyką. Tačiau tuo atveju, kai, esant tyčiai, pasisavinant ar sugadinant laikmeną, pasisavinami ar sunaikinami ir laikmenoje esantys elektroniniai duomenys, padaryta veika

kvalifikuojama pagal BK nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui ir nusikalstamų veikų nuosavybei sutaptis.

BK 198^2 straipsnyje nurodytas nusikalstamos veikos dalykas – įrenginiai, programinė įranga, slaptažodžiai ar kitokie panašūs duomenys, tiesiogiai skirti daryti nusikalstamoms veikoms.

Atkreiptinas dėmesys į BK 198 straipsnyje nurodytą susiaurintą nusikalstamos veikos dalyką – neviešus elektroninius duomenis. Kai kurie teisininkai teigia, jog viešų elektroninių duomenų vagystės kriminalizavimas būtų visiškai nelogiškas, nes viešos informacijos vagystė taip pat nėra kriminalizuota.[101] Taigi asmens veika bus laikoma nusikalstama tik tada, jei jis neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis. Kadangi neviešų elektroninių duomenų išaiškinimo nerasime BK XXX skyriuje, todėl, kad išsiaiškintume, kokie elektroniniai duomenys yra nevieši, turime vadovautis Lietuvos Respublikos Konstitucija[102], Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu[103], Lietuvos Respublikos civiliniu kodeksu[104], Lietuvos Respublikos elektroninio parašo įstatymu[105], Lietuvos Respublikos elektroninių ryšių įstatymu[106], Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu[107] bei kitais Lietuvos Respublikos įstatymais. Taigi matome, kad tai yra mišri, turinti blanketinės ir aprašomosios normos požymių, teisės norma.

Remiantis baudžiamojo proceso specialisto A. Panomariovo išskirtais pagrindiniais duomenų konfidencialumo kriterijais, galima formuluoti ir elektroninių duomenų, kaip vienos iš duomenų rūšių, neviešumo kriterijus.[108] Todėl elektroniniai duomenys gali būti laikomi nevieši, jei jie atitinka šiuos kriterijus: tam tikras apsaugos lygis (tokie elektroniniai duomenys yra saugomi teisės aktais), vertingumas, reikšmingumas (jį gali apspręsti konkretus asmuo, tam tikros socialinės asmenų grupės ar valstybė), prieigą prie tokių duomenų yra patikėta arba ją turi tik ribotas subjektų skaičius, duomenys turi būti tinkamai ir pakankamomis priemonėmis apsaugoti nuo jų atskleidimo (atitinkamų leidimų ar draudimų naudotis tam tikrais elektroniniais duomenimis įvedimas, teisinės atsakomybės už neteisėtą tam tikrų elektroninių duomenų atskleidimą arba už netinkamą naudojimąsi, disponavimą jais, maksimalių įslaptinimo terminų

[101] Federal Bureau of Investigation. Internet Crime Report 2006. http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf; prisijungimo laikas 2008-05-14.
[102] Lietuvos Respublikos Konstitucija // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_1?p_id=274999; prisijungimo laikas: 2007-09-10.
[103] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 1996, Nr. 63-1479.
[104] Lietuvos Respublikos civilinis kodeksas (su pakeitimais ir papildymais iki 2008 m. birželio 3 d.) // Valstybės žinios. 2000, Nr. 74-2262.
[105] Lietuvos Respublikos elektroninio parašo įstatymas // Valstybės žinios. 2000, Nr. 61-1827.
[106] Lietuvos Respublikos elektroninių ryšių įstatymas // Valstybės žinios. 2004, Nr. 69-2382.
[107] Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas // Valstybės žinios. 2004, Nr. 4-29.
[108] Panomariovas A. Viešai neskelbiama informacija (paslaptis) baudžiamajame procese: daktaro disertacija (socialiniai mokslai, teisė) / LTU. – V., 2001. P. 58.

nustatymas). Tokius neviešus elektroninius duomenis gali sudaryti asmens medicininiai, duomenų, privataus gyvenimo, susirašinėjimo, pokalbių telefonu, telegrafo ir kitokių pranešimų, mokesčių mokėtojo, ikiteisminio tyrimo, įvaikinimo, balsavimo duomenys, komercinės, banko, pramoninės, technologinės, įmonės, kredito unijų, profesinės, tarnybinės, valstybės ir karinės paslaptys.

BK 196 straipsnyje nuo neteisėto sunaikinimo, sugadinimo, pašalinimo, pakeitimo ar kitais būdais naudojimosi apribojimo yra saugomi tiek vieši, tiek nevieši elektroniniai duomenys, bet nuo neteisėto stebėjimo, fiksavimo, perėmimo, įgijimo, laikymo, pasisavinimo, paskleidimo ar kitaip panaudojimo yra saugomi tik nevieši elektroniniai duomenys (BK 198 straipsnis). Taigi teisės aktų nesaugomi elektroniniai duomenys yra tie, kurie neturi neviešiems elektroniniams duomenims keliamų, kaip teisės normų saugomai vertybei, būtinų požymių.

Kartu su pagrindinėmis nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtimis, numatančiomis minimalų kiekį nusikalstamos veikos požymių (BK 196 straipsnio 1 dalis, 197 straipsnio 1 dalis, 198 straipsnio 1 dalis, 198^1 straipsnio 1 dalis, 198^2 straipsnio 1 dalis), Lietuvos Respublikos įstatymų leidėjas numatė ir kvalifikuotas (BK 196 straipsnio 2 dalis, 197 straipsnio 2 dalis, 198 straipsnio 2 dalis, 198^1 straipsnio 2 dalis), ir privilegijuotas (BK 196 straipsnio 3 dalis, 197 straipsnio 3 dalis) nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtis. Kvalifikuotose nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui sudėtyse baudžiamasis įstatymas numato papildomus požymius, dėl kurių buvimo veika tampa pavojingesne ir todėl griežčiau baudžiama. BK 196 straipsnio 2 dalis, 197 straipsnio 2 dalis, 198 straipsnio 2 dalis, 198^1 straipsnio 2 dalis numato tuos pačius kvalifikuojančius požymius: pavojinga veika padaryta strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniams duomenims, informacinei sistemai, neviešiems elektroniniams duomenims. Kaltininkas pagal objektyvias įvykio aplinkybes turi suvokti kvalifikuojančio požymio egzistavimą, t. y. reikia įrodyti kaltininko psichinį santykį su tuo kvalifikuojančiu požymiu, pavyzdžiui, kaltininkas, sunaikindamas Ignalinos atominės elektrinės tam tikrus elektroninius duomenis, turi suvokti, jog tai yra objektyviai strateginę reikšmę nacionaliniam saugumui turinčios įmonės elektroniniai duomenys. Panašus požymis yra įtvirtintas ir Jungtinėse Amerikos Valstijose, kai baudžiama už tyčinę prieigą, neturint tam teisės prie Jungtinių Amerikos Valstijų departamento ar agentūros kompiuterio, jei kompiuteris skirtas išimtinai šioms institucijoms naudoti.[109]

[109] Beaupre D., Cassaday W. State and Local Law Enforcement Need to Combat Electronic Crimes. - National Institute of Justice, US Department of Justice, 2000. P. 173.

Vadovaujantis 1996 m. gruodžio 19 d. Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymu Nr. VIII-49, pagrindiniai nacionalinio saugumo objektai yra žmogaus ir piliečio teisės, laisvės bei asmens saugumas, tautos puoselėjamos vertybės, jos teisės ir laisvos raidos sąlygos, valstybės nepriklausomybė, konstitucinė santvarka, valstybės teritorijos vientisumas, aplinka ir kultūros paveldas ir visuomenės sveikata.[110] Strategiškai svarbūs nacionaliniam saugumui yra energetikos, transporto, informacinių technologijų ir telekomunikacijų, kitų aukštųjų technologijų, finansų ir kredito sektoriai. Strateginę reikšmę nacionaliniam saugumui turinčią infrastruktūrą detalizuoja 2002 m. spalio 10 d. Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas Nr. IX-1132[111], kuriame yra pateikiamas tokių įmonių baigtinis sąrašas, kurį galėtume suklasifikuoti taip:

- energetikos infrastruktūros įmonės (Ignalinos atominė elektrinė, Lietuvos naftos produktų agentūra, Kruonio hidroakumuliacinė elektrinė, Kauno hidroelektrinė, „Mažeikių nafta“, „Lietuvos dujos“ ir kt.);

- transporto infrastruktūros įmonės (Kauno oro uostas, Klaipėdos valstybinio jūrų uosto direkcija, tarptautinis Vilniaus oro uostas, „Kauno regiono keliai“, „Klaipėdos regiono keliai“, „Vidaus vandens kelių direkcija“, Klaipėdos valstybinio jūrų uosto hidrotechniniai įrenginiai, krantinės, navigacijos keliai ir kanalai, navigaciniai įrenginiai ir kiti infrastruktūros objektai, viešojo naudojimo geležinkeliai ir kt.);

- informacinių technologijų ir telekomunikacijų, kitų aukštųjų technologijų infrastruktūros įmonės (Lietuvos radijo ir televizijos centras, „Lietuvos telekomas“ ir kt.).

2004 m. spalio 15 d. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos vyriausybės direktoriaus įsakyme Nr. T-131 „Dėl valstybės informacinių sistemų kūrimo metodinių dokumentų patvirtinimo“ nurodyta, jog valstybės informacinė sistema – valstybės institucijai teisės aktų nustatytoms funkcijoms, išskyrus vidaus administravimą, atlikti reikiamos informacijos apdorojimo procesus (duomenų ir dokumentų tvarkymo, skaičiavimo, bendravimo nuotoliniu būdu) vykdanti sistema, kuri veikia informacinių technologijų pagrindu.[112]

Šiuo metu vienas iš pagrindinių kompiuterinių nusikaltėlių taikinių ne tik strateginę reikšmę nacionaliniam saugumui turinčių objektų informacinės sistemos, bet ir didelės reikšmės

[110] Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas // Valstybės žinios. 1997, Nr. 2-16.

[111] Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_1?p_id=314533; prisijungimo laikas: 2008-04-17.

[112] Lietuvos Respublikos Vyriausybės Informacinės visuomenės plėtros komiteto direktoriaus įsakymas „Dėl asmeninio kompiuterio vienetą sudarančių elementų sąrašo patvirtinimo“ // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=240019; prisijungimo laikas: 2008-05-03.

valstybės valdymui, ūkiui ar finansų sistemai turinčių objektų informacinės sistemos. Didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai turinčius objektus reikėtų suprasti daug plačiau nei strateginę reikšmę nacionaliniam saugumui turintys objektai. Valstybės valdymas yra daugiamatė, gana plati sąvoka, valstybės valdymo sistema - visuma valstybės valdžios institucijų, atliekančių tam tikras funkcijas, įgyvendinant valstybinę valdžią. Taigi siekiama sugriežtinti baudžiamąją atsakomybę ne tik už neteisėtą poveikį strateginę reikšmę nacionaliniam saugumui turinčių objektų informacinėms sistemoms ir elektroniniams duomenims, bet ir tokioms svarbioms valstybės valdymo, ūkio ar finansų sistemų informacinėms sistemoms kaip, pavyzdžiui, Valstybės registras, bankai, Valstybinės mokesčių inspekcijos duomenų bazės ir kitos valstybinės institucijos, savivaldybės įstaigos.

Jau minėtoje Vilniaus miesto 1 apylinkės teismo baudžiamojoje byloje Nr. 1-17-296/2008 aplinkybė, jog kaltinamasis neteisėtai pasidarė fizinių ir juridinių asmens elektroninių duomenų kopiją iš (duomenys neskelbtini) centrinės klientų duomenų bazės, buvo pripažinta nusikaltimą kvalifikuojančiu požymiu, nes (duomenys neskelbtini) centrinėje klientų duomenų bazėje saugomi nevieši elektroniniai duomenys yra didelę reikšmę valstybės valdymui ir ūkiui turintys elektroniniai duomenys.

Tokiai teismo pozicijai pritartina, teismas teisingai nustatė nusikalstamą veiką kvalifikuojantį požymį, kadangi nukentėjęs asmuo – valstybės institucija, disponuojanti fizinių ir juridinių asmenų duomenimis ir ypatingaisiais fizinių asmenų duomenimis.

Lietuvos Respublikos teisės aktuose strateginės reikšmės nacionaliniam saugumui ar didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniai duomenys yra apibrėžiami per atitinkamų institucijų, kurios turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansams, įvardijimą. Atrodytų, jog taip akcentuojama tam tikrų įmonių ar įstaigų svarba ir visos jose esančios informacinės sistemos, tačiau šį veiką kvalifikuojantį požymį reikėtų aiškinti taip: ne visos informacinės sistemos, esančios institucijose, įmonėse, įstaigose, kurios turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansams, yra turinčios strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai. Pavyzdžiui, elektroninių duomenų sunaikinimas Ignalinos AE buhalterinės apskaitos sistemoje užtraukia baudžiamąją atsakomybę pagal BK 196 straipsnio 1 ar 3 dalį, o ne pagal BK 196 straipsnio 2 dalį, kadangi buhalterinės apskaitos sistema nesudaro BK 196 straipsnio 2 dalyje nurodyto kvalifikuojančio požymio. Jeigu būtų sugadinti Ignalinos AE reaktoriaus - technologinių įrengimų kontrolės, valdymo ir apsaugos sistemoje esantys elektroniniai duomenys, tuomet tokia pavojinga veika būtų kvalifikuojama pagal BK 196

straipsnio 2 dalį. Kiekvienu atveju šis veiką kvalifikuojantis požymis turi būti atidžiai įvertinamas.

Apibendrinant, nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui dalykas – elektroniniai duomenys (BK 196, 198 straipsniai) arba informacinės sistemos (BK 197, 198[1] straipsniai). BK 198 straipsnyje nurodytas susiaurintas nusikalstamos veikos dalykas – nevieši elektroniniai duomenys. Nusikalstamų veikų dalykas BK 196 straipsnio 2 dalyje, 197 straipsnio 2 dalyje, 198 straipsnio 2 dalyje ir 198[1] straipsnio 2 dalyje - strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniai duomenys, informacinė sistema ir nevieši elektroniniai duomenys. BK 198[2] straipsnyje nurodytas nusikalstamos veikos dalykas – įrenginiai, programinė įranga, slaptažodžiai ar kitokie panašūs duomenys, tiesiogiai skirti daryti nusikalstamoms veikoms.

Kadangi BK 198[2] straipsnyje nurodyti įrenginiai, programinė įranga, slaptažodžiai, prisijungimo kodai ir kitokie duomenys, tiesiogiai skirti daryti nusikalstamoms veikoms, gali tapti kitų nusikalstamų veikų padarymo priemonėmis, bei kai kurie diskusiniai teoriniai klausimai, aptariami kitame poskyryje, siejasi su šiame straipsnyje nurodytu nusikalstamos veikos dalyku, todėl BK 198[2] straipsnyje nurodytos nusikalstamos veikos dalykas bus aptariamas kitame poskyryje, siekiant logiško ir nuoseklaus minčių dėstymo.

2.2.5. Nusikalstamos veikos padarymo priemonės kaip nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių objektyvusis požymis

Jei nusikalstamos veikos padarymo priemonė turi įtakos nusikalstamos veikos pavojingumui, įstatymų leidėjas įtraukia šį požymį į nusikalstamos veikos sudėtį. Atkreiptinas dėmesys, kad BK 198[2] straipsnyje nurodyti įrenginiai, programinė įranga, slaptažodžiai, prisijungimo kodai ir kitokie duomenys, tiesiogiai skirti daryti nusikalstamoms veikoms, yra nusikaltimo dalykas, tačiau tokie įrenginiai, programinė įranga, slaptažodžiai, prisijungimo kodai ir kitokie duomenys gali tapti kitų nusikalstamų veikų padarymo priemonėmis. Panaši situacija susidaro ir BK 196 straipsnyje – naudojimasis elektroniniais duomenimis yra apribojamas, pasitelkiant techninę ar programinę įrangą. Techninė ir programinė įranga čia yra nusikalstamos veikos padarymo priemonė. Apriboti naudojimąsi elektroniniais duomenimis galima, panaudojant tiek fizinę jėgą, tiek ir technines priemones, tad Lietuvos Respublikos įstatymų leidėjas kriminalizavo neteisėtą elektroninių duomenų naudojimosi apribojimą tiek technine ir programine įranga, tiek kitais būdais, pvz. fizinės jėgos panaudojimu.

Techninė įranga (aparatinė įranga, angl. *hardware*) – informacijos apdorojimo sistemos fizinių komponentų visuma arba tos visumos dalis.[113] Kompiuterių techninė įranga apima ir visas fizines kompiuterio dalis, bet ne programinę įrangą, valdančią šias dalis. Bet koks kompiuteris susideda iš šių dalių (techninės įrangos): procesoriaus (vykdo logines ir programos logikos valdymo komandas), atminties (joje saugoma vykdomoji programa - vykdomų procesoriaus komandų rinkinys - bei įvairūs jos vykdymo metu naudojami duomenys), duomenų magistralės (jomis perduodami duomenys tarp procesoriaus ir atminties), išorinių įrenginių, skirtų duomenų įvedimui ir išvedimui bei papildomai funkcijai – saugojimui (kietasis diskas, klaviatūra, pelė, monitorius, vaizdo plokštė, garso plokštė, mikroschemų rinkinys). 2004 m. rugpjūčio 23 d. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos vyriausybės direktoriaus įsakyme Nr. T-101 „Dėl asmeninio kompiuterio vienetą sudarančių elementų sąrašo patvirtinimo“ yra nurodyta, jog kompiuterio techninę įrangą sudaro sisteminis blokas (sisteminė plokštė, centrinis procesorius, operatyvioji atmintis, standusis diskas, maitinimo šaltinis, korpusas), monitorius, klaviatūra, pelė, papildomi kompiuterio elementai (spausdintuvas, skaitytuvas, internetinė vaizdo kamera, garso kolonėlės, ausinės, mikrofonas) išoriniai duomenų nuskaitymo ir įrašymo įrenginiai (optinių laikmenų nuskaitymo ir/arba įrašymo įrenginiai, lanksčiųjų diskelių nuskaitymo ir įrašymo įrenginys, išorinis standusis diskas, USB atmintinė), kita sisteminiame bloke talpinama ir veikianti aparatinė įranga, kurios prijungimo galimybės numatytos sisteminėje plokštėje.[114]

Logiškai ir sistemiškai analizuojant BK 196 ir 198^2 straipsnius, Lietuvos Respublikos įstatymų leidėjas techninei įrangai apibrėžti naudoja skirtingas sąvokas – techninė įranga (BK 196 straipsnis) ir įrenginiai (BK 198^2 straipsnis). Toks netikslumas yra kritikuotinas ir taisytinas, pasirenkant techninės įrangos sąvoką ir taip ją atskiriant nuo programinės įrangos. Taip pat nėra visiškai aišku, ar Lietuvos Respublikos įstatymų leidėjas šiomis sąvokomis įtvirtina tik kompiuterių techninę įrangą ar apskritai bet kokią techninę įrangą. Šiuolaikinės technologijos sudaro galimybes sugadinti ar pašalinti elektroninius duomenis, naudojantis net ir mobiliaisiais telefonais, tad, mūsų nuomone, ši techninės įrangos ar įrenginių sąvoka apima ne tik kompiuterių techninę įrangą, o bet kokią techninę įrangą, kuri sudaro galimybes padaryti nusikalstamas veikas, numatytas BK XXX skyriuje. Labai dažnas atvejis, kuomet elektroniniai duomenys yra perimami jų perdavimo metu tam tikrais kanalais – perdavimo metu tokie elektroniniai duomenys tampa labai pažeidžiami ir juos perimti yra daug lengviau nei neteisėtai prisijungti prie informacinės sistemos, pažeidžiant apsaugos priemones. Taigi Lietuvos Respublikos

[113] Informacinių technologijų institutas. Lietuvos kompiuterininkų sąjunga. Pagrindinės informacijos technologijos sąvokos. – Vilnius: Žara, 2001. P. 53.

[114] Lietuvos Respublikos Vyriausybės Informacinės visuomenės plėtros komiteto direktoriaus įsakymas „Dėl asmeninio kompiuterio vienetą sudarančių elementų sąrašo patvirtinimo“ // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=240019; prisijungimo laikas: 2008-05-03.

įstatymų leidėjas nekonkretina techninės įrangos sąvokos, nes, kaip jau buvo minėta, nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui padarymo priemonės ir įrankiai sparčiai tobulėja, panaudojamos naujai atsiradusios priemonės.

Norint dirbti kompiuteriu, nepakanka jį sukomplektuoti iš įvairių techninės įrangos komponentų. Kaip žmogus savo veikloje vadovaujasi protu, mokslo žiniomis ir sukaupta praktine patirtimi, taip ir kompiuteris dėl jame įdiegtų programų gali *per se*, be žmogaus įsikišimo, ir labai greitai atlikti daug veiksmų, pavyzdžiui, perrašyti duomenis iš vienos vietos į kitą, įjungti ar išjungti reikiamu momentu tam tikrus įtaisus.[115]

Programinė įranga (angl. *software*) – informacijos apdorojimo sistemos programų, procedūrų, taisyklių visuma arba tos visumos dalis kartu su atitinkama dokumentacija.[116] Programinė įranga yra intelektualus produktas ir tai nepriklauso nuo to, į kokią duomenų laikmeną ji yra įrašyta. Tai kompiuterio vykdomų instrukcijų seka, skirta tam tikriems veiksmams atlikti, tokia įranga kuriama, naudojant programavimo kalbas, o vėliau kompiliuojant ar interpretuojant parašytą kodą. Sąlyginai programinė įranga gali būti skirstoma į įmontuotąją (tai tokia programinė įranga, kuri paprastai yra neatsiejama nuo techninės įrangos, į kurią ji yra įdiegta), sisteminę (tokia įranga yra atsakinga už atskirų techninės įrangos komponentų kontrolę, integravimą ir valdymą, pavyzdžiui, operacinės sistemos, tvarkyklės, vartotojų identifikavimo sistemos) ir taikomąją (tokia įranga skirta specifinių užduočių sprendimui, tai gali būti viena programa ar susijusių programų paketas, pavyzdžiui, tekstų apdorojimo programinė įranga, duomenų bazių valdymo sistemos, grafinė programinė įranga, dokumentų valdymo (ir raštvedybos) programos, virusai). Programinė įranga, tiesiogiai skirta daryti nusikalstamas veikas, gali būti tam tikros programos, užkrėstos virusais, turinčios savybes vykdyti neteisėtus veiksmus, pavyzdžiui, buhalterinėse sistemose sumas apvalinti iki sveikojo skaičiaus, virusai, „Trojos arkliai“ (suteikia galimybes kontroliuoti kompiuterio darbą). Be to, tokios programos gali atlikti tokias funkcijas kaip pačios persikelti, patekti į kitas informacines sistemas, daugintis.

Daugeliui paprastų kompiuterių techninės ir programinės įrangos vartotojų aišku, kas yra techninė įranga, o kas – programinė, tačiau mokslininkų tarpe yra diskutuojama, jog riba tarp programinės ir techninės įrangos nėra visiškai aiški.[117] Nėra vieningo požiūrio, ar kompiuterio detalėse įmontuotoji programinė įranga yra programinė įranga, ar techninės įrangos dalis, nes tokia programinė įranga dažniausiai būna tiek susijusi su įrenginiu, kad techniškai jos neįmanoma atskirti – įrenginys be tokių programų dirbti negali. Tačiau tokios programos yra bevertės be įrenginių, kurioms jos skirtos. Dėl šių priežasčių tokia įmontuotoji programinė įranga

[115] Charney S., Alexander K. Computer Crime. http://www.crime-research.org/library/Alex.htm; prisijungimo laikas: 2008-07-12.
[116] Informacinių technologijų institutas. Lietuvos kompiuterininkų sąjunga. Pagrindinės informacijos technologijos sąvokos. – Vilnius: Žara, 2001. P. 32.
[117] Gringras C., Nathanson N. The Laws of the Internet. – New York: Butterworths, 1997. P. 117.

teisiškai dažniausiai priskiriama techninei, bet ne programinei įrangai. Tačiau apskritai visa programinė įranga yra bevertė be techninės įrangos, t.y. programinė įranga negali funkcionuoti ir būti pritaikoma pagal paskirtį, jei nėra techninės įrangos.

Elektroninių duomenų naudojimosi apribojimas kitais būdais reiškia, jog apribojimas yra atliekamas ne įrenginiais ar programine įranga, bet, pavyzdžiui, perpjovus laidą, kuriuo perduodami elektroniniai duomenys, paties įrenginio sunaikinimu ar sugadinimu, duomenis perduodančių jungčių, laidų pašalinimu ar sugadinimu, elektros tiekimo sutrikdymu ir pan. Įstatyme įtvirtinta kitų būdų sąvoka yra labai plati, tačiau tai pateisinama, nes sparčiai vystantis technologijoms atsiranda vis nauji duomenų naudojimosi apribojimo būdai, kurių neapima įrenginiai ar programinė įranga.

Programinę įrangą galima gaminti ir teisėtais tikslais – dažnas įvairių programų kūrėjas bando sukurti kitas atskiras programėles, kuriomis vėliau bus tikrinama, kiek sukurta pagrindinė programinė įranga yra patikima[118]. Manytume, kad tai labai sveikintinas dalykas, nes tik taip galime siekti tobulos apsaugos prasme programinės įrangos sukūrimo. Iš baudžiamosios teisės pozicijų tokio asmens netraukimą baudžiamojon atsakomybėn galima paaiškinti kaip BK 30 straipsnyje numatytą profesinių pareigų vykdymą. Viena Jungtinių Amerikos Valstijų informacinių technologijų bendrovė net paskelbė konkursą savo darbuotojams: tam, kas atras esančias programinėje įrangoje „skyles“, už tai bus sumokamas piniginis atlygis.[119]

Slaptažodis - tai simbolių eilutė, kuri leidžia vartotojams įeiti į kompiuterį ir pasiekti bylas, programas ir kitus šaltinius. Slaptažodžiai padeda užtikrinti, kad kiti asmenys neprieitų prie kompiuterio, jei tai jiems neleistina. Slaptažodžiai gali būti sudaryti iš raidžių (didžiųjų mažųjų), skaičių, simbolių ir pan. Slaptažodžiai, kaip ir asmens vardas, pavardė, asmens kodas, yra asmeniniai vartotojo duomenys. Prisijungimo kodas yra apibrėžiamas panašiai ir iš esmės tai yra dvi tapačios sąvokos, tačiau kai kurie autoriai šias dvi sąvokas skiria, teigdami, jog slaptažodžiu dažniausiai laikoma simbolių eilutė, kurią dažniausiai sugalvoja pats vartotojas, ir jį vartoja atitinkamą laiko tarpą prisijungti prie kompiuterio, bylų, aplankų ar programų. Prisijungimo kodas taip pat yra simbolių eilutė, tik ji dažniausiai yra suteikiama pačios informacinės sistemos, programos ir naudojama pirmąkart prisijungti prie programų, bylų, kitų informacinių sistemų ir pan. Saugumo sumetimais prisijungimo kodai galioja tik pirmą kartą, jungiantis prie sistemos, o vėliau sistema reikalauja sugalvoti slaptažodį. Mūsų manymu, tokia nuomonė kritikuotina, o tai, kaip pavadinsime simbolių eilutę - slaptažodžiu ar prisijungimo kodu - yra tik susitarimo reikalas. Iš esmės simbolių eilutei suteikti skirtingi pavadinimai jos turinio ir paskirties nekeičia.

[118] Icove D. J. Collaring the Cybercrook: an Investigator‘s View // Spectrum. 1997, Nr. 34(6). P. 98.
[119] Lessig L. Code and Other Laws of Cyberspace, Version 2.0. - Basic Books, 2006. P. 126.

Apibendrinant, reikia pasakyti, kad Lietuvos Respublikos įstatymų leidėjas nusikalstamos veikos padarymo priemones įtvirtina BK 196 straipsnyje – naudojimasis elektroniniais duomenimis yra apribojamas, pasitelkiant techninę, programinę įrangą ar kitais būdais. Siūlytina įtvirtinti techninės įrangos sąvoką, taip ją atskiriant nuo programinės įrangos, ir tokiu būdu pašalinant BK XXX skyriuje vartojamų skirtingų, tačiau turinio prasme tapačių sąvokų (techninė įranga ir įrenginiai) netikslumus. Be to, mūsų manymu, Lietuvos Respublikos įstatymų leidėjas nekonkretina pačios techninės įrangos sąvokos, nes tai gali būti tiek kompiuterių techninė įranga, tiek bet kokia kita techninė įranga, kuri sudaro galimybes padaryti nusikalstamas veikas, numatytas BK XXX skyriuje. Taip yra todėl, kad sparčiai vystantis informacinėms technologijoms, atsiranda vis naujesnės nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui padarymo priemonės, todėl jas konkretinti ar nustatyti tokių priemonių baigtinį sąrašą baudžiamajame įstatyme būtų netikslinga.

2.2.6. Nusikalstamos veikos padarymo būdai kaip nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių objektyvusis požymis

Nusikalstamos veikos padarymo būdas yra pavojingos veikos raiškos būdas ar jos padarymo metodas.[120] Teisinėje literatūroje yra daug nuomonių, susijusių su nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui įvykdymo būdais.[121] Vystantis technikai ir technologijoms, tų būdų daugėja, tad būtų netikslinga sudarinėti tam tikrą sąrašą, o tik paminėsime keletą iš jų. Neviešus elektroninius duomenis galima perimti tiesiogiai (tam tikrais įrenginiais jungiantis prie kompiuterio komunikacinių linijų), elektromagnetiniu būdu (pasinaudojant emisijos efektu, kai į aplinką išspinduliuojamos radijo bangos, atsirandančios elektroninių prietaisų darbo metu), pasiklausymo įrenginiais (blakės). Neteisėtai prisijungti prie informacinės sistemos galima pasinaudojant teisėto vartotojo kompiuteriu, prisijungiant prie teisėto vartotojo linijos, pasinaudojant informacinėje sistemoje esančiomis silpnomis vietomis (skylėmis) arba klaidomis, gaunant teisėtų vartotojų prisijungimo prie tos sistemos identifikacinius kodus, informacinės sistemos laikino gedimo metu. Elektroniniai duomenys gali būti pakeičiami, pakeičiant programos kodą ar funkciją, įvedant tokias programas, kurios atlieka naujas, neplanuotas funkcijas, virusais, kurių standartinis algoritmas yra „padaryk tą, paskui pereik prie to ir atlik tą“. Informacinės sistemos darbą galima sutrikdyti sistemai išsiuntus labai didelį kiekį žinučių – taip jau buvo sutrikdyta *CNN, Yahoo* informacinių sistemų veikla.[122]

[120] Piesliakas V. Lietuvos baudžiamoji teisė. Baudžiamasis įstatymas ir baudžiamosios atsakomybės pagrindai. Kn. 1. - Vilnius: Justitia, 2006. P. 297.
[121] Burda R., Gudmonas S. Modernios technologijos – modernūs nusikaltimai // Justitia. 1998, Nr. 4. P. 11.
[122] Robinson J. K. Internet as the Scene of Crime // International Computer Crime Conference. - Oslo, 2000.

Neviešus elektroninius duomenis galima paskleisti, juos platinant kompiuteriniais tinklais ar kitokiu būdu perduodant tretiesiems asmenims. Be to, nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui gali būti įvykdomos, pasitelkus kelis būdus.

Visose BK XXX skyriaus nusikalstamų veikų dispozicijose yra įtvirtintas jų padarymo būdas – neteisėtai. Žodis ,,neteisėtai“ nurodo elektroninių duomenų sugadinimo arba prisijungimo prie informacinės sistemos būdą. Visais šiais atvejais nusikalstamos veikos padarymo būdas tampa įrodinėtina bylos aplinkybė. Neteisėta – tai toks priėjimas ar įsikišimas, kuriam nesuteikė leidimo sistemos ar jos dalies savininkas, kitas teisės turėtojas arba kurio neleidžia nacionalinės teisės aktai. Neteisėta reiškia be duomenų savininko ar įgalioto asmens sutikimo, leidimo, viršijant tam asmeniui nustatytas teises arba jomis piktnaudžiaujant.

Asmuo turi būtinai įveikti tam tikras informacinės sistemos apsaugos priemones, kad neteisėtai prisijungtų prie informacinės sistemos. Darytina išvada, kad ta informacinė sistema, kuri prieinama kaltininkui, turi būti būtinai apsaugota apsaugos priemonėmis.[123] Tik tokiu atveju nusikalstamą veiką padariusio asmens veiksmai bus kvalifikuojami pagal BK 198^1 straipsnį. Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje numatyta, jog valstybė gali reikalauti, kad toks nusikaltimas būtų padarytas pažeidžiant apsaugos priemones, tačiau kaip reikėtų kvalifikuoti tokį asmens veiksmą, kai jis, pasinaudodamas tuo, jog informacinė sistema nėra apsaugota apsaugos priemonėmis, prie jos prisijungia? Štai asmuo B leidžia prisijungti prie jo spausdintuvo bet kam, nustatydamas spausdintuvo režimą į ,,share“ (dalytis), vadinasi, pats asmuo B supranta, kad leidžia jo spausdintuvu naudotis bet kokiam asmeniui, galinčiam prisijungti prie jo spausdintuvo, be to, taip paneigiamas ir pats neteisėtumas, jungiantis prie spausdintuvo. Problema čia kyla tame, jog asmuo B gali nežinoti, jog tam tikra jo naudojama informacinė sistema nėra apsaugota apsaugos priemonėmis. Vis tik manytume, jog tai yra BK 198^1 straipsnyje įtvirtintos nusikaltimo sudėties trūkumas, nes apskritai nereikėtų detalizuoti šio nusikaltimo padarymo būdo.

Apsaugos priemonės neapsiriboja vien tik antivirusinės programinės įrangos naudojimu ar stiprių slaptažodžių parinkimu. Tai gali būti konfidencialumo apsaugos priemonės - informacinių sistemų vartotojų prieigos teisių valdymas, duomenų šifravimas, speciali duomenų ištrynimo iš kompiuterio kietojo disko programinė įranga; ugniasienės, antivirusinė programinė įranga, loginės prieigos kontrolės sistemos. Dauguma informacinių sistemų neleidžia automatiškai naudotis jose esančiais resursais be tam tikrų tos sistemos vartotojo nustatymų atlikimo, tačiau ne visada tokios sistemos būna tobulos. Praėjus mėnesiui nuo ,,Firefox“ sistemos

[123] Petrauskas R., Štitilis D. Lietuvos Respublikos baudžiamasis kodeksas Nusikaltimų elektroninėje erdvėje konvencijos kontekste // Jurisprudencija. 2002, Nr. 24(16). P. 80.

pasirodymo rinkoje, patys vartotojai aptiko tam tikras „skyles“, todėl sistemų kūrėjai stengiasi kaip įmanoma greičiau patobulinti tokią sistemą ir ragina ją atnaujinti.[124]

Apibendrinant, dėl technikos ir technologijų vystymosi nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui įvykdymo būdų daugėja. Visose BK XXX skyriaus nusikalstamų veikų dispozicijose yra įtvirtintas jų padarymo būdas – neteisėtai, o tai reiškia be savininko ar įgalioto asmens sutikimo, leidimo, viršijant tam asmeniui nustatytas teises arba jomis piktnaudžiaujant. BK 198^1 straipsnyje numatytas neteisėto prisijungimo prie informacinės sistemos būdas – pažeidžiant informacinės sistemos apsaugos priemones, todėl ta informacinė sistema, kuri prieinama kaltininkui, turi būti būtinai apsaugota apsaugos priemonėmis, norint tokiam asmeniui inkriminuoti BK 198^1 straipsnį.

2.3. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėčių subjektyviųjų požymių analizė

Subjektyvieji nusikalstamos veikos sudėties požymiai turi būti įrodinėjami kiekvienoje baudžiamojoje byloje. Remiantis BK 2 straipsnio 3 dalimi, baudžiamoji atsakomybė be kaltės yra negalima.

Kaltė yra pagrindinis subjektyvusis nusikalstamos veikos sudėties požymis, kurį visada reikia įrodinėti baudžiamojoje byloje. Kaltė – pavojingą veiką padariusio asmens psichinis santykis su objektyviaisiais nusikalstamos veikos sudėties požymiais.[125] Nustatyti kaltę nagrinėjamose nusikalstamose veikose gali būti sudėtinga dėl to, jog kaltininkas gali neigti savo kaltę arba kaltės formą.

Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui gali būti padaromos tik tyčia, pavyzdžiui, asmuo, neteisėtai pakeisdamas elektroninius duomenis, suvokia pavojingą veikos pobūdį, numato, kad, pakeisdamas elektroninius duomenis, padarys didelės žalos, ir nori tokių padarinių – didelės žalos. Tyčia gali būti tiesioginė, kai kaltininkas supranta, kad jis savo veika kėsinasi į elektroninių duomenų ir informacinių sistemų saugumą, numato, kad dėl tokio jo veikimo gali atsirasti baudžiamajame įstatyme nurodyti padariniai ir jų nori (materiali sudėtis) arba kai kaltininkas supranta, kad jis savo veika kėsinasi į elektroninių duomenų ir informacinių sistemų saugumą ir nori taip veikti (formali sudėtis). Nusikalstamos veikos, nurodytos BK XXX skyriuje, gali būti padaromos tik tiesiogine tyčia, pavyzdžiui, asmuo neteisėtai prisijungdamas prie informacinės sistemos, pažeidžiant informacinės sistemos

[124] Chiliarchaki P., Dowland P. S., Furnell S. M. Security Analysers: Administrator Assistants or Hacker Helpers? // Information Management & Computer Security. 2001, Nr. 9/2. P. 98.
[125] Piesliakas V. Lietuvos baudžiamoji teisė. Baudžiamasis įstatymas ir baudžiamosios atsakomybės pagrindai. Kn. 1. - Vilnius: Justitia, 2006. P. 337.

apsaugos priemones, suvokia tokios veikos pavojingą pobūdį ir nori taip veikti, neteisėtai prisijungti prie informacinės sistemos, pažeidžiant informacinės sistemos apsaugos priemones.

Kalbant apie tiesioginę tyčią materialiose nusikalstamų veikų sudėtyse, kaltininkas gali numatyti konkrečius pavojingos veikos padarinius arba jų nekonkretinti. Pagal tai tyčia skirstoma į apibrėžtą ir neapibrėžtą. Kaltininkas, pasinaudodamas programine įranga, apribojo naudojimąsi elektroniniais duomenimis ir siekė padarinių. Jo veika gali būti kvalifikuojama:

1. kaip pasikėsinimas padaryti didelės/nedidelės žalos, neteisėtai apribojant naudojimąsi elektroniniais duomenimis, jei jis tokių padarinių siekė (BK 22 straipsnio 1 dalis, 196 straipsnio 1 dalis ar 3 dalis) arba pagal realiai kilusius padarinius, jei jam pavyko realizuoti viską, ką jis buvo numatęs. Kaltininkas čia veikė apibrėžta tyčia;

2. pagal realiai kilusius padarinius (BK 196 straipsnio 1 ar 3 dalis), jei kaltininkas veikė neapibrėžta tyčia ir norėjo bet kokių padarinių.

Jei kaltininkas siekė apibrėžtų padarinių, t. y. didelės ar nedidelės žalos, tačiau jie nekilo dėl nuo jos valios nepriklausančių aplinkybių, tai jo veika bus kvalifikuojama kaip pasikėsinimas padaryti atitinkamą veiką arba pagal realiai kilusius padarinius. Jeigu kaltininkas veikė neapibrėžta tyčia ir jam buvo priimtini bet kokie kilsiantys padariniai, tai veika kvalifikuojama pagal kilusius padarinius. Nustatant tyčios kryptingumą, reikia įvertinti tiek kaltininko subjektyvų veikos aplinkybių suvokimą, tiek ir veikos objektyviuosius požymius, kurie atskleidžia, kiek kaltininkas suvokė ir detalizavo galinčius kilti padarinius ir ko jis savo veiksmais siekė.

Kai kurie autoriai teigia, kad nusikalstamos veikos, nurodytos BK 196 ir 197 straipsniuose, gali būti padaromos tiek tiesiogine, tiek netiesiogine tyčia.[126] Esant netiesioginei tyčiai, kaltininkas yra abejingas padarinių atžvilgiu. Mūsų manymu, BK 196 ir 197 straipsniuose nurodytas nusikalstamas veikas galima padaryti tik tiesiogine tyčia, nes labai sunku rasti net ir teorinių teiginių apie materialiųjų sudėčių nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, padaromas netiesiogine tyčia – kaltininkas bet kokiu atveju numato, kad neišvengiamai atsiras tam tikri padariniai.[127] Detaliau panagrinėkime pateiktą pavyzdį.

Kaltininkas, norėdamas atkeršyti bankui, kurio darbuotojas jį nemandagiai aptarnavo, nusprendžia sutrikdyti banko informacinės sistemos darbą. Sumanytą tikslą galima pasiekti keliais būdais: sumanymą galima įgyvendinti banko darbo metu, t. y. dieną, kai banko darbuotojai, aptarnaudami klientus, naudojasi banko informacine sistema, tačiau yra rizika, jog

[126] Adduci M. Cybercrime: riflessioni sulla produzione normativa in Italia. http://www.cybercrimes.it/articoli/ci_prodnorm.php; prisijungimo laikas: 2007-12-08.
[127] Computer Security Institute. Computer Crime and Security Survey 2000. http://www.gocsi.com/prelea000321.htm; prisijungimo laikas: 2008-07-05.

informacinės sistemos darbo sutrikdymą greitai pastebės darbuotojai. Daug mažesnė rizika tokį sumanymą įgyvendinti banko nedarbo metu, vėlai vakare arba naktį, kai banko informacinė sistema yra daug mažiau apkrauta ir ja naudojasi mažai vartotojų. Taigi, kaltininkas savo sumanymą įgyvendina vėlyvą vakarą, tačiau paaiškėja, jog būtent tuo metu banko informacinėse sistemose vykdomi pinigų pervedimai į užsienio bankus, o dėl tokio informacinės sistemos darbo sutrikdymo, pinigai į užsienio bankus nebuvo pervesti, atsirado daugybė nepatenkintų klientų ir pan. Kaltininkas teigia nenorėjęs sukelti bankui didelės žalos, o tik norėjęs „pamokyti“ banką, kad kitąkart banko darbuotojai su juo elgtųsi mandagiau. Netiesioginės tyčios atveju kaltininkas turi būti absoliučiai abejingas kilusių padarinių atžvilgiu, o esant neapibrėžtai tyčiai asmuo suvokia pavojingą veikos pobūdį ir numato padarinius, jų nori, tačiau jų nedetalizuoja. Iš pateiktos situacijos matome, jog kaltininko veika neišvengiamai sukels BK numatytus padarinius. Taigi čia galima kalbėti tik apie tiesioginės neapibrėžtos tyčios buvimą kaltininko veikoje, nes, nors kaltininkas ir teigia, kad padarinių nenorėjo, tačiau pagal bylos aplinkybes jų kilimas buvo neišvengiamas ar labai tikėtinas, tačiau kaltininkas jų nedetalizavo. Kaltininko veika bus kvalifikuojama pagal BK 197 straipsnio 1 dalį.

Fakultatyvūs subjektyvieji nusikalstamos veikos sudėties požymiai yra nusikalstamos veikos padarymo motyvas ir tikslas. Šiuos požymius įrodinėti reikia tik tada, kai jie yra aprašyti BK specialiosios dalies straipsnio dispozicijoje. Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui dažniausiai padaromos dėl savanaudiškų paskatų (siekiama gauti turtinės naudos sau ar kitiems asmenims), chuliganiškų užmojų (žmogaus ir visuomenės negerbimas, moralės ir elgesio normų nepaisymas, niekinamo požiūrio demonstravimas, dėl mažareikšmės dingsties), tačiau Lietuvos Respublikos įstatymų leidėjas BK XXX skyriaus straipsnių dispozicijose neaprašė šių veikų motyvų, tad motyvai, kvalifikuojant tokias nusikalstamas veikas, reikšmės neturi.

Kalbant apie neteisėtą prisijungimą prie informacinės sistemos (BK 198 straipsnis), labai dažnai asmenys tiesiog įsilaužia į tam tikras informacines sistemas, kad parodytų savo galimybes kolegoms, draugams arba tos sistemos teisėtiems vartotojams, jog jų naudojama sistema yra nesaugi arba nėra visiškai saugi.[128] Kaip rodo pasaulinė statistika, su tokiu tikslu dažniausiai laužiasi paaugliai arba asmenys iki 18 m., bet, manytume, kad pagrindiniu tikslu įsilaužti į informacines sistemas reikėtų laikyti suinteresuotumą gauti arba prieiti prie tam tikrų duomenų, juos sunaikinti arba pakeisti visiškai ar iš dalies.[129] Daugumoje analizuotų baudžiamųjų bylų, kuriose buvo kaltinami asmenys, padarę nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, kaltinamieji buvo jau sulaukę pilnametystės.

[128] Rupp T., Smith A. Issues in Cybersecurity: Understanding the Potential Risks Associated with Hackers/Crackers // Information Management & Computer Security. 2002, Nr. 10/4. P. 180.
[129] Klimas T. Šiuolaikinis nusikalstamumas. - Kaunas: VDU, 2002. P. 76.

Lietuvoje stebint nusikalstamas veikas padariusių asmenų amžiaus kitimo tendenciją ir spartų informacinių technologijų plitimą, galime tikėtis, jog nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui darys jaunesni nei 18 m. asmenys.[130,131] Vadovaujantis BK 13 straipsnio 1 dalimi, už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui atsako asmuo, kuriam iki nusikaltimo ar baudžiamojo nusižengimo padarymo buvo suėję 16 metų.[132]

Nusikalstamos veikos padarymo tikslas – asmens siekiai, susiję su nusikalstamos veikos padarymu, priežastys, dėl ko jis nusprendė padaryti nusikalstamą veiką.[133] Tik vienintelėje BK XXX skyriaus 198^2 straipsnio dispozicijoje yra nurodytas nusikalstamos veikos padarymo tikslas – daryti nusikalstamas veikas, t. y. asmuo neteisėtai gamino, gabeno, pardavė ar kitaip platino įrenginius ar programinę įrangą, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis, tiesiogiai skirtus daryti nusikalstamas veikas, arba tuo pačiu tikslu juos įgijo ar laikė. Neįrodžius tokio asmens tikslo, šios nusikalstamos veikos sudėties asmens veikoje nėra.

Yra nuomonių, jog programinę įrangą, kuri skirta neteisėtai prisijungti prie informacinės sistemos ar neteisėtai gauti elektroninius duomenis, yra labai sunku atskirti nuo tų atvejų, kai siekiama teisėtų tikslų, tad baudžiamosios normos, kriminalizuojančios neteisėtą disponavimą įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis gali būti netaikomos praktikoje.[134] Manytume, jog teisėtos programinės įrangos atskyrimas nuo neteisėtos yra atitinkamų specialistų darbo dalis, todėl tai neturi turėti įtakos tokios veikos kriminalizavimui. Jau 1992 m. Tarptautinėje baudžiamosios teisės apžvalgoje ir 1994 m. Kriminalinės policijos tarptautinėje apžvalgoje dėl kompiuterinių nusikaltimų buvo pasisakyta, kad neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais turi patekti į kriminalizuotinų veikų sąrašą.[135,136]

Mūsų nuomone, jei BK 198^2 straipsnyje nurodytos nusikalstamos veikos sudėtyje nebūtų įtvirtintas nusikalstamos veikos padarymo tikslas, tuomet į šios nusikalstamos veikos sudėtį

---

[130] Asmenys, įtariami (kaltinami) nusikalstamų veikų padarymu. Nepilnamečiai (14-17 m. amžiaus). http://www.nplc.lt/stat/asm/asm5.htm; prisijungimo laikas: 2008-06-14.

[131] Yar M. Computer Hacking: Just Another Case of Juvenile Delinquency? // The Howard Journal. 2005, Nr. 44(4). P. 393.

[132] Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Lietuvos Respublikos baudžiamasis kodeksas (su pakeitimais ir papildymais iki 2008 m. birželio 12 d.) // Valstybės žinios. 2004, Nr. 25-760.

[133] Piesliakas V. Lietuvos baudžiamoji teisė. Baudžiamasis įstatymas ir baudžiamosios atsakomybės pagrindai. Kn. 1. - Vilnius: Justitia, 2006. P. 412.

[134] Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study. http://law.scu.edu/international/File/Sieber_final.pdf; prisijungimo laikas: 2008-01-26.

[135] United Nations Manual on the Prevention and Control of Computer-Related Crime // International Review of Criminal Policy. 1994, No. 43/44. P. 28.

[136] Wahlert G. Crime in Cyberspace: Trends in Computer Crime in Australia // Australian Institute of Criminology Conference „Internet Crime“. - Melbourne, 1998. http://www.aic.gov.au/conferences/internet/wahlert.pdf; prisijungimo laikas: 2007-12-07.

papultų ir tokie teisėti asmenų veiksmai, kai jie teisėtai gamina, gabena, parduoda ar kitaip platina įrenginius ar programinę įrangą, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis, arba tuo pačiu tikslu juos įsigyja ar laiko. Už teisėtus veiksmus asmenys negali būti traukiami baudžiamojon atsakomybėn, tad BK 198^2 straipsnyje įtvirtintas nusikalstamos veikos padarymo tikslas atskiria teisėtą disponavimą įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis nuo neteisėto.

Nors Konvencija dėl elektroninių nusikaltimų numato, jog valstybė gali nustatyti baudžiamąją atsakomybę už neteisėtą įtaisų naudojimą tokioms nusikalstamoms veikoms atlikti kaip neteisėta prieiga, neteisėta perimtis, neteisėtas poveikis duomenims ir informacinei sistemai, tačiau Lietuvos Respublikos įstatymų leidėjas numatė baudžiamąją atsakomybę už neteisėtą disponavimą įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais ne tik BK XXX skyriuje nurodytoms veikoms padaryti (196, 197, 198, 198^1 straipsniai), bet ir nusikalstamoms veikoms, numatytoms BK 166, 167, 182, 210, 295 straipsniuose, daryti bei kitoms nusikalstamoms veikoms.

Kalbant apie BK 198^1 straipsnyje kriminalizuota nusikalstamą veiką, praktikoje labai paplitusios tokios situacijos, kai kiekvienas, savo jėgas ir žinias siekiantis išbandyti asmuo, bando neteisėtai prisijungti prie informacinės sistemos, pažeidžiant jos apsaugos priemones. Taigi, toks asmuo būtų baudžiamas už nusikalstamos veikos padarymą. Remiantis Konvencijos dėl elektroninių nusikaltimų 2 straipsniu, kuriame numatyta, kad valstybė gali reikalauti, kad toks nusikaltimas būtų padarytas, pažeidžiant apsaugos priemones, ketinant gauti kompiuterinius duomenis ar turint kitą nesąžiningą ketinimą.[137] Kaip jau buvo aptarta anksčiau, vien neteisėtas prisijungimas prie informacinės sistemos pažeidžia tos informacinės sistemos integralumą ir vientisumą bei toje informacinėje sistemoje laikomų duomenų slaptumą bei konfidencialumą, todėl nėra tikslinga BK 198^1 straipsnyje numatyti neteisėto prisijungimo prie informacinės sistemos tikslą – siekimą gauti elektroninius duomenis.

Prieiname išvados, jog atsakomybės už mažai pavojingas veikas klausimas gali būti sprendžiamas, atsižvelgiant į bausmių skyrimo taisykles ar atleidimo nuo baudžiamosios atsakomybės institutą. Norėtume pridurti, jog, remiantis 2000 m. gruodžio 21 d. Lietuvos Aukščiausiojo Teismo Senato nutarimo Nr. 29 „Dėl teismų praktikos veikas pripažįstant mažareikšmėmis“ 7 punktu, kuriame teigiama, kad „jeigu įstatymų leidėjas baudžiamajai atsakomybei kilti yra nustatęs tam tikrą vertinamąjį nusikaltimo sudėties požymį (žymi žala, didelė žala, ypatingas įžūlumas ir pan.), tai veikoje ar jos pasekmėse nustačius šį požymį, jo specifikos pagrindu pripažinti veiką mažareikšme negalima“. Taigi tokiems savo jėgas ir žinias

[137] Convention on Cybercrime. Explanatory Report // http://conventions.coe.int/Treaty/en/Reports/Html/185.htm; prisijungimo laikas: 2007-10-24.

siekiantiems išbandyti asmenims, kurie padaro BK XXX skyriuje numatytas nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, kurių sudėtyse yra įtvirtinti pavojingos veikos padariniai – žala, nebus taikomas BK 37 straipsnis – atleidimas nuo baudžiamosios atsakomybės dėl nusikaltimo mažareikšmiškumo. Be to, BK Be to, BK 37 straipsnis negali būti taikomas ir kai baudžiamasis įstatymas už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui (BK 196 straipsnio 3 dalis ir 197 straipsnio 3 dalis) numato baudžiamąjį nusižengimą.

3. LIETUVOS RESPUBLIKOS BAUDŽIAMAJAME KODEKSE NUMATYTŲ NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI PAGRINDINIAI STATISTIKOS RODIKLIAI IR JŲ ANALIZĖ

Elektroninių duomenų ir informacinių sistemų saugumas – viena iš svarbiausių informacinės visuomenės vertybių. Dėl vis didėjančios informacinių technologijų ir, ypač interneto skvarbos, anksčiau tik užsienio valstybėms aktualios nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui problemos atėjo ir į Lietuvą. Tokias nusikalstamas veikas, turint omenyje jomis padaromą didelę žalą, nusikalstamų veikų įvykdymo vietas bei kitus ypatumus, galima vadinti ir XXI amžiaus „rykšte“.

Lietuvos Respublikos įstatymų leidėjas tokias vertybes kaip nuosavybė, turtinės teisės ir turtiniai interesai, intelektinė ir pramoninė nuosavybė gretina su tokia vertybe kaip elektroninių duomenų ir informacinių sistemų saugumas. Visuomenė, kurioje žmogus patiria nesaugumo jausmą, baimę dėl to, kad naudojasi informacinių technologijų mokslų laimėjimais (internetinių banko sąskaitų valdymas, asmens elektroniniai duomenys valstybės institucijose), rodo, jog valstybė nesugeba pakankamai ir tinkamai užtikrinti elektroninių duomenų ir informacinių sistemų funkcionavimo galimybes, o tuo pačiu ir visuomenės saugumo.

Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui pasižymi labai dideliu latentiškumu. Labai didelė dalis šių nusikalstamų veikų dėl subjektyvių ir objektyvių priežasčių dažnai lieka nepastebėtos, ir todėl neatskleistos. Dalis šių nusikalstamų veikų lieka nepastebėtos dėl sistemų administratorių nepakankamo žinių kiekio apie kompiuterinių sistemų administravimo ypatumus bei jų saugumo užtikrinimą ar kompiuterių vartotojų aplaidumo, kompiuterinio raštingumo nepakankamumo. Kita dalis nusikalstamų veikų lieka neatskleistos dėl įvairių subjektyvių aplinkybių, dėl kurių apie nusikalstamas veikas nenorima pranešti atitinkamoms teisėsaugos institucijoms: verslo ir komercinių įmonių baimė prarasti klientus, investuotojus, visuomenės pasitikėjimą, nes tokios nusikalstamos veikos

atskleidimo faktas leidžia interpretuoti, jog įmonės informacinių tinklų apsauga yra nepakankama arba ten dirba nekvalifikuoti informacinių technologijų specialistai, nenoras atskleisti tam tikrą informaciją apie įmonės veiklą, kurią gali panaudoti konkurentai savo labui, ar noras išvengti viešumo.[138]

Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui yra lydimos ir kitų nusikalstamų veikų – sukčiavimo (BK 182 straipsnis)[139], literatūros, mokslo, meno ar kitokio kūrinio neteisėto atgaminimo, neteisėtų kopijų platinimo, gabenimo ar laikymo (BK 192 straipsnis), informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimo arba pakeitimo (BK 193 straipsnis), neteisėto autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimo (BK 194 straipsnis), disponavimo pornografinio turinio dalykais (BK 309 straipsnis) ir pan.

Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui yra „patogios“ tuo, jog dažnai duoda labai didelį pelną. Ekspertai teigia, kad pelnas iš tokių nusikalstamų veikų viršija pelną, gaunamą iš prekybos narkotikais.[140] Be to, tokiomis nusikalstamomis veikomis įprastai padaroma didelė žala. Jungtinių Amerikos Valstijų Federalinių tyrimų biuro duomenimis, dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui vien amerikiečių verslo bendrovės patiria daugiau kaip 67 mlrd. dolerių nuostolių.[141] Per pastaruosius dvejus metus (2005 – 2007) amerikiečiai patyrė 8 mlrd. dolerių nuostolių dėl virusų platinimo. Lietuvos bankai apie kompiuterių įsilaužėlių padarytus nuostolius neskelbia.

Dar vienas labai svarbus ir ypatingas nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui požymis – nusikalstamos veikos įvykdymo vieta. Tokios nusikalstamos veikos daromos elektroninėje erdvėje, kuri neturi geografinių sienų, nustatančių atskirų šalių jurisdikcijos galiojimo ribas.[142] Jei nusikalstama veika elektroninių duomenų ir informacinių sistemų saugumui padaroma, naudojantis internetu - vadinasi, per kelias valstybes - gali susiklostyti tokia situacija, kai asmuo, būdamas valstybėje, kurioje tokios nusikalstamos veikos nėra kriminalizuotos, įvykdęs tokią veiką, gali likti nenubaustas. Taip pat tokiu atveju negalima ir ekstradicija, jei toje valstybėje tokio pobūdžio veika nelaikoma nusikalstama ir nėra kriminalizuota. Be to, kaltininkas, esantis ir veikiantis Lietuvos Respublikos baudžiamosios

[138] Criminalità informatica: cos'è realmente e dove si trova? http://innovatorining.com/group/intmetecrimineinnovazionenelleindagini; prisijungimo laikas: 2008-08-24.
[139] Fletcher N. Challenges for Regulating Financial Fraud in Cyberspace // Journal of Financial Crime. 2007, Nr. 14(2). P. 202.
[140] Hoofnagle C. J. Identity Theft: Making The Known Unknowns Known // Harvard Journal of Law and Technology. 2007, Nr. 21(1). P. 118.
[141] Federal Bureau of Investigation. Internet Crime Report 2006. http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf; prisijungimo laikas 2008-05-14.
[142] Exon S. N. Personal Jurisdiction: Lost in Cyberspace? // Computer Law Review and Technology Journal. 2003, Nr. 8. P. 75.

jurisdikcijos teritorijoje, gali bandyti neteisėtai prisijungti prie duomenų bazių, esančių Kinijos, Jungtinių Amerikos Valstijų ar kitų valstybių baudžiamosios jurisdikcijos teritorijose, todėl apie tai galime ir nesužinoti. Iškyla atskirų valstybių, skirtingai reglamentuojančių nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui baudžiamosios atsakomybės klausimus, įstatymų derinimo ir baudžiamosios jurisdikcijos kolizijų problemos. Tik jas išsprendus, bus galima nusikalstamą veiką elektroninių duomenų ir informacinių sistemų saugumui padariusį asmenį patraukti baudžiamojon (ar administracinėn) atsakomybėn, nepriklausomai nuo to, kurios valstybės baudžiamosios jurisdikcijos teritorijoje jis veikė ir kur atsirado nusikalstamos veikos padariniai.

Dėl aukščiau paminėtų ir anksčiau šiame tiriamajame darbe aptartų priežasčių yra tikslinga pateikti ir išanalizuoti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui statistinius rodiklius ir jų kaitos tendencijas.

Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui kol kas sudaro labai mažą bendro nusikalstamumo dalį (iki 0,2%).[143] Žinant apie labai didelį šių nusikalstamų veikų latentiškumą, šie duomenys yra itin svarbūs, darant prognostines nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kitimo tendencijas. Toliau atskleisime visų užregistruotų nusikalstamų veikų ir užregistruotų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui per tam tikrą laiko tarpą tarpusavio ryšį bei kitimo tendencijas, lyginsime užregistruotų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui ir išaiškintų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui dalis. Pasirinkta analizuoti duomenis laikotarpyje nuo 2004 m. iki 2008 m. rugsėjo mėn., remiantis Statistikos departamento prie Lietuvos Respublikos Vyriausybės ir Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos pateikiama statistine informacija apie nusikalstamas veikas, įvykdytas Lietuvos Respublikos teritorijoje.

Iš 1 lentelėje pateiktų duomenų matyti, jog vidutiniškai nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui sudaro 0,06% bendro nusikalstamų veikų skaičiaus ir tai yra labai mažas skaičius bendrame registruotų nusikalstamų veikų skaičiuje. Tačiau, kaip buvo minėta, nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui yra labai latentiškos, todėl šio skaičiaus kitimas negali būti laikomas nusikalstamumo apskritai, įskaitant ir latentinę dalį, kitimo indikatoriumi.[144]

[143] Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Nusikalstamumas ir teisėsaugos insttiucijų veikla 2006. - Vilnius, 2007. P. 15.
[144] Babachinaitė G. Socialiniai pokyčiai ir nusikalstamumas. Teisinės valstybės link // Jurisprudencija. 2000, Nr. 15(7). P. 130.

***1 lentelė**. Užregistruotos visos nusikalstamos veikos ir nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui (2004 – 2008-09-01)*[145]

Metai	Užregistruotos visos nusikalstamos veikos	Užregistruotos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui	Užregistruotos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui, %
2004	93419	15	0,016
2005	89815	18	0,02
2006	82155	20	0,024
2007	73741	50	0,07
2008	52002	84	0,16

Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui skaičiaus kitimo tendencijos per 5 metų (2004 – 2008-09-01) laikotarpį neatspindi visų užregistruotų nusikalstamų veikų per tą patį laikotarpį kitimo tendencijas: nuosekliai ir tolygiai augant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui skaičiui, visų užregistruotų nusikalstamų veikų skaičius mažėja. 2004 m. užregistruotos 15 nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui ir 93419 nusikalstamų veikų iš viso, kai 2007 m. užregistruotos 50 nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui ir 73741 nusikalstamos veikos iš viso - visų užregistruotų nusikalstamų veikų per šį laikotarpį sumažėjo 1,27 karto. Pastebimas didelis nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui šuolis nuo 2006 m. iki 2007 m. ir nuo 2007 m. iki 2008-09-01. Tai galima paaiškinti suaktyvėjusia Lietuvos Kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo skyriaus suaktyvėjusia veikla, ikiteisminio tyrimo pareigūnams bei ekspertams rengtais specialiais kursais ir mokymais, teikiančiais teisinį, kriminalistinį, organizacinį bei techninį pasiruošimą tirti nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui.[146]

Be to, apskritai didėjančią šių nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tendenciją galima paaiškinti visuotine kompiuterizacija, interneto technologijų plėtra šiuolaikiniame visuomenės gyvenime, prie plataus interneto tinklo kartu su eiliniais vartotojais prisijungia ir nusikalstamo pasaulio atstovai.

Per nagrinėjamą laikotarpį išanalizavus visų užregistruotų nusikalstamų veikų ir nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tarpusavio ryšį,

[145] Pateikiami duomenys per 2008 m. pirmus devynis mėnesius.
[146] Leichteris E. Kompiuteriniai nusikaltimai // Naujoji komunikacija. 1999, Nr. 19. P. 34.

pažvelkime į nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui vidinę struktūrą ir į užregistruotų ir ištirtų šių nusikalstamų veikų santykį (2 lentelė).

***2 lentelė**. Užregistruotos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui (2004 – 2008-09-01)*[147]

Metai	BK 196 straipsnis	BK 197 straipsnis	BK 198 straipsnis	BK 198[1] straipsnis	BK 198[2] straipsnis
2004	4	2	7	1	1
2005	1	-	6	10	1
2006	2	2	10	6	-
2007	3	3	11	30	2
2008	n	n	n	n	n
Iš viso	10	7	34	47	4

n – nėra duomenų.

Per nagrinėjamą laikotarpį skirtingų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui vidinė struktūra labai skyrėsi kiekybiškai. Daugiausia užregistruota nusikalstamų veikų, susijusių su neteisėtu prisijungimu prie informacinės sistemos (BK 198[1] straipsnis) ir neteisėtu elektroninių duomenų perėmimu ir panaudojimu (BK 198 straipsnis), mažiausiai užregistruota nusikalstamų veikų, susijusių su neteisėtu disponavimu įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis (BK 198[2] straipsnis) ir neteisėtu poveikiu informacinei sistemai (BK 197 straipsnis).

Nagrinėjant atskirų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kitimo tendencijas per pasirinktą laikotarpį, pastebimas žymus nusikalstamų veikų, susijusių su neteisėtu elektroninių duomenų perėmimu ir panaudojimu (BK 198 straipsnis) bei su neteisėtu prisijungimu prie informacinės sistemos (BK 198[1] straipsnis) didėjimas. Skirtingai nuo šių nusikalstamų veikų, pastebima svyruojanti tokių nusikalstamų veikų kaip neteisėtas poveikis elektroniniams duomenims (BK 196 straipsnis), neteisėtas poveikis informacinei sistemai (BK 197 straipsnis) ir neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis (BK 198[2] straipsnis) kitimo tendencija. Pavyzdžiui, 2004 m. buvo užregistruotos 4 nusikalstamos veikos, susijusios su neteisėtu poveikiu elektroniniams duomenims, 2005 m. – tik 1, o 2006 m. – jau 2 tokios nusikalstamos veikos; 2005 m. buvo užregistruota 1 nusikalstama veika, susijusi su neteisėtu disponavimu įrenginiais,

[147] Tas pats.

programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, 2006 m. – nei vienos, o 2007 m. – jau 2 tokios nusikalstamos veikos.

Analizuojant užregistruotų ir ištirtų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui santykį per pasirinktą laikotarpį, kiekvienais metais stebima šių nusikalstamų veikų išaiškinamumo didėjimo tendencija: jei 2004 m. buvo išaiškinama tik 26,7% visų užregistruotų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui, tai 2008 m. išaiškinamumo lygis šoktelėjo iki 77,4% visų užregistruotų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui (3 lentelė). Tokį aukštą nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui išaiškinamumo lygį reikėtų paaiškinti didėjančiu kvalifikuotų ikiteisminio tyrimo pareigūnų, turinčių specialiųjų informacinių technologijų žinių, skaičiumi, pakitusiu teisėsaugos pareigūnų požiūriu į tokių nusikalstamų veikų pavojingumą bei tiek ikiteisminio tyrimo pareigūnų, tiek ekspertų ir informacinių technologijų specialistų bendradarbiavimo didėjimu.[148] Deja, informacijos apie atskirų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui išaiškinamumą nepavyko rasti.

***3 lentelė**. Užregistruotos ir ištirtos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui (2004 – 2008-09-01)*[149]

Metai	Užregistruotos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui	Ištirtos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui	Ištirtos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui %
2004	15	4	26,7
2005	18	9	50
2006	20	8	40
2007	50	35	70
2008	84	65	77,4
Iš viso	187	121	64,7

Plačiau kalbant apie nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui atskleidimą ir išaiškinimą, pažymėtina, jog tyrimas reikalauja ne tiek teisinio, kiek kriminalistinio, organizacinio bei techninio pasiruošimo. Aiškinantis padarytas nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui dar tik ikiteisminiame tyrimo

[148] Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos statistika. http://www.vrm.lt/fileadmin/Image_Archive/IRD/Statistika/index2.phtml?id=198; prisijungimo laikas: 2008-09-15.
[149] Tas pats.

etape, ikiteisminio tyrimo pareigūnas susiduria su tokiais šių nusikalstamų veikų specifiniais požymiais kaip nusikalstamos veikos padarymo vieta, kuri nėra materiali, o dažniausiai tai yra tarnybinės stotys, kuriose galima aptikti nusikalstamą veiką padariusio asmens pėdsakų (prisijungimo adresai (IP), slapukai (cookies)[150]), kurie suteikia vertingos informacijos apie nusikalstamą veiką padariusį asmenį. Nors prisijungimo – IP - adresas visuomet yra unikalus, kurį kiekvienam vartotojui suteikia interneto paslaugų tiekėjas, tačiau pasaulyje plintant belaidėms technologijoms ir atsirandant galimybei prisijungti prie pasaulinio tinklo iš bet kurio taško, kuriame yra įdiegta ši technologija, tampa dar sudėtingiau nustatyti tikruosius nusikalstamas veikas padariusius asmenis. Tuomet tai galima padaryti tik pagal vartotojo unikalų tinklo plokštės MAC (Media Access Control) adresą.[151]

Šiandien mūsų ikiteisminio tyrimo pareigūnams, tiriantiems tokias veikas, stinga lėšų bei laiko, galingos techninės įrangos, specialių programavimo žinių. Taigi dažniausiai net nerandama materialių nusikalstamų veikų pėdsakų – elektroninės erdvės specifika lemia, kad visi galimi pėdsakai bus elektroniniame pavidale. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tyrimas reikalauja ypatingų informacinių technologijų, ypač programavimo ir tinklų administravimo, žinių, todėl į tokių veikų tyrimą turėtų įsitraukti ne tik kriminalistai, bet ir informacinių technologijų specialistai. Kadangi patys ikiteisminio tyrimo pareigūnai dažnai neturi pakankamai žinių apie nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui specifiką, todėl jų bendradarbiavimas su specialistais yra itin pageidautinas, kuris vienais atvejais turėtų būti – epizodinis, kitais – nuolatinis.

Manytume, jog, kol pareigūnai, tiriantys nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, neturės geros techninės bazės ir žinių, tol nesiformuos ir teisminė praktika.

Analizuojant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tyrimo rezultatus, procesas dėl šių nusikalstamų veikų dažniausiai būdavo užbaigiamas teismo baudžiamuoju įsakymu (BPK 418 straipsnis) (4 lentelė). Baudžiamojo proceso užbaigimas teismo baudžiamuoju įsakymu galimas tik dėl tokių nusikalstamų veikų, už kurių padarymą gali būti skiriama tik bauda arba ši bausmė yra numatyta kaip alternatyvinė, ir tik tada, kai bylos aplinkybės yra pakankamai aiškios, kai kaltininkas atlygina ar pašalina padarytą žalą, jeigu žala buvo padaryta, arba įsipareigoja tokią žalą atlyginti ar pašalinti, kaltininkas sutinka su proceso užbaigimu teismo baudžiamuoju įsakymu. Tai rodo, jog užbaigti procesą teismo baudžiamuoju įsakymu dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui yra

[150] Electronic Privacy Information Center. Cookies. http://epic.org/privacy/cookies/default.html; prisijungimo laikas: 2008-04-11.
[151] Cybercrime and Jurisdiction: a Global Survey / edited by Koops B. J., Brenner S. W. - The Hague: T. M. C. Asser Press, 2006.

sudarytos visos sąlygos, nes daugelyje BK XXX skyriuje numatytų nusikalstamų veikų sankcijose bauda yra numatyta kaip alternatyvi bausmė.

***4 lentelė**. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tyrimo rezultatai (2004 – 2008-09-01)*[152]

Metai	Užregistruotos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui	BPK 220 straipsnis	BPK 418 straipsnis	BPK 426 straipsnis	Nutraukta BPK 3 straipsnio pagrindu	Nutraukta BPK 212 straipsnio pagrindu
2004	15	-	4	-	2	1
2005	18	2	3	-	4	-
2006	20	1	5	-	2	-
2007	50	1	33	-	1	-
2008	84	1	-	-	5	10
Iš viso	187	5	45	-	14	11

Be to, kaltininkui sutikti su tokia baudžiamojo proceso užbaigimo forma yra naudinga *ipso facto* - teismo baudžiamuoju įsakymu jam gali būti paskirta švelnesnė bausmė (o praktikoje dažniausiai taip ir yra)[153] už bausmę, kuri galėtų būti paskirta įprasta tvarka priimant apkaltinamąjį nuosprendį, o tai ypač aktualu nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui atvejais, nes daugelyje šių nusikalstamų veikų sankcijose, be baudos, yra numatytos ir kitos bausmės. Be to, kaltinamasis taip gali išvengti nepageidaujamo viešumo, kadangi nevyksta teismo posėdis. Pabrėžtina, jog galimybė užbaigti procesą dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui teismo baudžiamuoju įsakymu ir išvengti viešumo yra labai svarbi ir nukentėjusioms nuo tokių nusikalstamų veikų įmonėms ir organizacijoms, kadangi tai gali paskatinti jų aktyvumą, pranešant apie šių nusikalstamų veikų įvykdymą ir kartu nesibaiminant prarasti klientus dėl nesaugių informacinių sistemų ar kad tam tikrą informaciją apie įmonės veiklą gali panaudoti konkurentai savo labui.

Per analizuojamą laikotarpį iš visų užregistruotų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui, tik dėl 5 nusikalstamų veikų baudžiamasis procesas vyko įprasta tvarka, t. y. byla perduodama nagrinėti teisme (BPK 220 straipsnis). Tai galima

[152] Pateikiami duomenys per 2008 m. pirmus devynis mėnesius.
[153] Jurgaitis R. Baudžiamojo įsakymo procesas: proceso be įprastojo nagrinėjimo teisme ypatumai ir įtariamojo (kaltinamojo) procesinės garantijos // Jurisprudencija. 2008, Nr. 6(108). P. 71.

paaiškinti tuo, jog baudžiamąjį procesą dėl daugumos tokių nusikalstamų veikų galima užbaigti teismo baudžiamuoju įsakymu, esant visoms formaliosioms ir vertinamosios sąlygoms. Taigi nagrinėjant užregistruotų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kitimo tendencijas per pasirinktą laikotarpį pastebimas proceso dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui užbaigimo teismo baudžiamuoju įsakymu tendencijos didėjimas.

Nei vienas baudžiamasis procesas iš visų užregistruotų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui per nagrinėjamą laikotarpį nebuvo baigtas pagreitinto proceso tvarka (BPK 426 straipsnis). Skirtingai nuo baudžiamojo proceso užbaigimo teismo baudžiamuoju įsakymu, pagreitintame baudžiamajame procese yra sutrumpinta ikiteisminio tyrimo stadija. Kadangi nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui išaiškinimas vis tik reikalauja laiko ir atitinkamų resursų, tad ir galimybės procesą dėl tokių nusikalstamų veikų užbaigimo pagreitinta tvarka yra labai mažos. Dėl 25 užregistruotų nusikalstamų veikų per nagrinėjamą laikotarpį baudžiamasis procesas buvo nutrauktas BPK 3 straipsnio pagrindais arba ikiteisminis tyrimas buvo nutrauktas BPK 212 straipsnio pagrindais.

Apibendrinant pateiktus ir šiame skyriuje išanalizuotus Statistikos departamento prie Lietuvos Respublikos Vyriausybės ir Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos duomenis apie nusikalstamas veikas, įvykdytas Lietuvos Respublikos teritorijoje 2004 m. - 2008 m. rugsėjo mėn. laikotarpiu, galima pasakyti, jog nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui sudaro labai mažą bendro nusikalstamumo dalį (iki 0,2%), tačiau pastebimas didelis nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui šuolis nuo 2006 m. iki 2007 m. ir nuo 2007 m. iki 2008-09-01. Kadangi nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui yra labai latentinės, tai šie duomenys yra itin svarbūs, darant prognostines nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kitimo tendencijas.

IŠVADOS IR REKOMENDACIJOS

1. Šio darbo įvade iškelta hipotezė pasitvirtino: nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui teisinis reglamentavimas yra sudėtingas ir nepakankamas. Patraukti baudžiamojon atsakomybėn asmenis, padariusius nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, *de lege lata* yra įmanoma, tačiau *de lege ferenda* nelengva, nes Lietuvoje beveik nėra išsamios baudžiamosios teisinės doktrinos ir teismų praktikos, kuria būtų galima remtis, aiškinant ir taikant baudžiamojo įstatymo normas, nustatančias baudžiamosios atsakomybės už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui prielaidas.

2. Remiantis tarptautiniais teisės aktais ir moksline literatūra, dažniausiai pateikiama ir universaliausiai vartojama ši nusikalstamų veikų elektroninėje erdvėje klasifikacija: nusikalstamos veikos elektroninėje erdvėje (plačiausiai suprantama sąvoka, apimanti tiek nusikalstamas veikas, susijusias su kompiuteriais, tiek kompiuterinius nusikaltimus ir kai kurias kitas nusikalstamas veikas, kurios nėra laikomos nusikalstamomis veikomis, susijusiomis su kompiuteriais, pvz., terorizmas), nusikalstamos veikos, susijusios su kompiuteriais (nusikaltimo dalykas – kompiuterinė informacija ir/arba kompiuteris panaudojamas kaip nusikalstamos veikos įvykdymo priemonė/būdas, ši sąvoka apima kompiuterinius nusikaltimus) ir kompiuteriniai nusikaltimai (siauriausiai suprantama sąvoka).

3. Įvairių valstybių įstatymų leidėjai nusikalstamas veikas elektroninėje erdvėje kriminalizuoja skirtingais būdais: specialiose ar tradicinėse baudžiamojo įstatymo normose, išskirdami šias nusikalstamas veikas į atskirą skyrių, numatydami šias veikas kaip tradicinių nusikalstamų veikų kvalifikuojančias sudėtis. Tai išreiškia skirtingų valstybių įstatymų leidėjų požiūrį į šių veikų pavojingumą ir jomis padaromų pavojingų padarinių reikšmę bei sunkumą. Skirtingai įvairių valstybių įstatymų leidėjų baudžiamosiose normose vadinamos šios nusikalstamos veikos vis tik patenka į jau minėtą universaliausią klasifikaciją, todėl kiekvienos valstybės įstatymų leidėjo bandymas „surasti“ ir įtvirtinti tos valstybės baudžiamųjų normų sistemai ir struktūrai priimtiną pavadinimą yra sveikintinas.

4. Lietuvos Respublikos įstatymų leidėjas, baudžiamajame kodekse kriminalizuodamas nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, įtvirtino kompiuterinio nusikaltimo siaurąja prasme sampratos aspektus. Nusikalstamomis veikomis, kuriose kompiuteris ir kitos informacinės technologijos gali būti panaudojamos kaip nusikalstamos veikos įvykdymo priemonės ar būdai (BK 182, 192, 194, 213, 309 straipsniai ir kt.), įtvirtinami kai kurie nusikalstamų veikų, susijusių su kompiuteriais, sampratos aspektai

tradicinėse baudžiamojo įstatymo normose, neišskiriant šių nusikalstamų veikų į specialiąsias baudžiamojo įstatymo normas.

5. BK XXX skyrius vadinasi „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“ - toks skyriaus pavadinimas atitinka informacinių technologijų mokslų vartojamą šiuolaikinių technologijų terminiją ir esmę. BK XXX skyriuje yra įtvirtinti ne tik nusikaltimai, bet ir baudžiamieji nusižengimai, tad skyriaus pavadinimas yra netikslus – jį siūlytina keisti į „Nusikaltimai ir baudžiamieji nusižengimai elektroninių duomenų ir informacinių sistemų saugumui“. BK XXX skyriaus saugoma vertybė - elektroninių duomenų ir informacinių sistemų saugumas, netrukdomai, nekliudomai, automatiškai apdorojant elektroninius duomenis ir valdant bei kontroliuojant informacines sistemas. Įstatymais garantuojamas elektroninių duomenų ir informacinių sistemų saugumas yra vertybė, į kurią kėsinamasi.

6. Elektroniniai duomenys - bet kokie materialiame (fiziniame) objekte esantys duomenys, kurie yra sukurti, saugomi ar perduodami informacinių technologijų ir telekomunikacijų priemonėmis. Informacinė sistema - 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.

7. Elektroninių duomenų ir informacinės sistemos, tiek kitų BK XXX skyriuje vartojamų sąvokų išaiškinimas nėra būtinas pačiame BK. Šias sąvokas detalizuoja kiti Lietuvos Respublikos teisės aktai, be to, dėl greito technologijų pokyčių ir vystymosi, sąvokos gali kisti, o tokiu atveju kaskart reiktų daryti BK pakeitimus, todėl šią problemą galėtų išspręsti blanketinių dispozicijų įtvirtinimas, kurios minėtų sąvokų konkretinimo nurodytų ieškoti tam tikruose teisės aktuose. Tačiau problema, jog tuose teisės aktuose vienodos sąvokos gali būti traktuojamos skirtingai, vis tik išlieka, todėl reikia siekti šių sąvokų unifikavimo arba vieno teisės akto priėmimo, kuriame būtų išaiškintos BK XXX skyriuje vartojamos sąvokos.

8. BK 198 straipsnio pavadinime įtvirtinamas „neteisėtas elektroninių duomenų perėmimas *ir* panaudojimas“, kai straipsnio dispozicijoje minima „tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė *ar* kitaip panaudojo neviešus elektroninius duomenis“. Tai turi esminės įtakos, aiškinantis šio nusikaltimo objektyviuosius požymius, *ipso facto* tokių netikslumų BK negalima leisti, todėl rekomenduotume šį straipsnį patikslinti. BK 198 straipsnio pavadinime yra minimi elektroniniai duomenys („Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“), kai tuo tarpu šiame straipsnyje įtvirtintų nusikalstamų veikų dispozicijose nurodyti ir šių nusikalstamų veikų dalykas yra nevieši elektroniniai duomenys.

Tokie netikslumai taisytini ir 198 straipsnio pavadinimas keistinas į „Neteisėtas *neviešų* elektroninių duomenų perėmimas *ar* panaudojimas“.

9. BK XXX skyriuje įtvirtintas nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui kaip pavojingas veikas apibūdinantys nusikalstami veiksmai (neteisėtai sunaikino, sugadino, pašalino ar pakeitė ar kitais būdais apribojo (BK 196 straipsnis), neteisėtai sutrikdė ar nutraukė (BK 197 straipsnis), neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo (BK 198 straipsnis), neteisėtai prisijungė (BK 198^1 straipsnis), neteisėtai gamino, gabeno, pardavė ar kitaip platino arba tuo pačiu tikslu įgijo ar laikė (BK 198^2 straipsnis)) kelia teisinių teorinių ir praktinių problemų: doktrininis ir mokslinis šių pavojingų veikų aiškinimas yra nepakankamas. Teismai netinkamai taiko baudžiamuosius įstatymus nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui ir daro klaidas, neteisingai kvalifikuodami nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui padariusių asmenų pavojingas veikas.

10. BK XXX skyriaus straipsnių dispozicijose numatytais padariniais (didelė žala, nedidelė žala) yra padaroma turtinė ir neturtinė žala. Kai nukentėjusiojo asmens patirta žala sudaro kitos BK numatytos nusikaltimo ar baudžiamojo nusižengimo sudėties objektyvųjį požymį, tai turėtų būti vertinama kaip didelė žala. Atsižvelgiant į BK struktūrą, nors ir netikslinga bei sudėtinga Lietuvos Respublikos įstatymų leidėjui būtų detalizuoti vertinamąjį didelės ar nedidelės žalos turinį, tačiau būtina užtikrinti didelės ar nedidelės žalos turinio kriterijų vienodumą baudžiamajame įstatyme, nes jų nesant, teismai bei ikiteisminio tyrimo institucijų pareigūnai didelės ar nedidelės žalos turinį gali komentuoti nevienodai. Tokiais kriterijais galėtų būti tiesiogiai padarytos žalos dydis, kilę nuostoliai, nukentėjusiojo asmens turtinė padėtis, reputacijos pabloginimo laipsnis, žalą padariusio asmens kaltė, nukentėjusio asmens teisių ir laisvių suvaržymo laipsnis, nukentėjusiųjų skaičius.

11. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui dalykas – elektroniniai duomenys (BK 196, 198 straipsniai) arba informacinės sistemos (BK 197, 198^1 straipsniai). BK 198 straipsnyje nurodytas susiaurintas nusikalstamos veikos dalykas – nevieši elektroniniai duomenys. Nusikalstamų veikų dalykas BK 196 straipsnio 2 dalyje, 197 straipsnio 2 dalyje, 198 straipsnio 2 dalyje ir 198^1 straipsnio 2 dalyje - strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniai duomenys, informacinė sistema ir nevieši elektroniniai duomenys. BK 198^2 straipsnyje nurodytas nusikalstamos veikos dalykas – įrenginiai, programinė įranga, slaptažodžiai ar kitokie panašūs duomenys, tiesiogiai skirti daryti nusikalstamoms veikoms.

12. Lietuvos Respublikos įstatymų leidėjas techninei įrangai apibrėžti naudoja skirtingas sąvokas – techninė įranga (BK 196 straipsnis) ir įrenginiai (BK 198^2 straipsnis). Siūlytina

įtvirtinti techninės įrangos sąvoką, taip ją atskiriant nuo programinės įrangos, ir tokiu būdu pašalinant BK XXX skyriuje vartojamų skirtingų, tačiau turinio prasme tapačių sąvokų (techninė įranga ir įrenginiai) netikslumus. Lietuvos Respublikos įstatymų leidėjas nekonkretina pačios techninės įrangos sąvokos, nes tai gali būti tiek kompiuterių techninė įranga, tiek bet kokia kita techninė įranga, kuri sudaro galimybes padaryti nusikalstamas veikas, numatytas BK XXX skyriuje. Taip yra todėl, kad sparčiai vystantis informacinėms technologijoms, atsiranda vis naujesnės nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui padarymo priemonės, todėl jas konkretinti ar nustatyti tokių priemonių baigtinį sąrašą baudžiamajame įstatyme būtų netikslinga.

13. Dėl technikos ir technologijų vystymosi nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui įvykdymo būdų daugėja. Visose BK XXX skyriaus nusikalstamų veikų dispozicijose yra įtvirtintas jų padarymo būdas – neteisėtai, o tai reiškia be savininko ar įgalioto asmens sutikimo, leidimo, viršijant tam asmeniui nustatytas teises arba jomis piktnaudžiaujant. BK 198^1 straipsnyje numatytas neteisėto prisijungimo prie informacinės sistemos būdas – pažeidžiant informacinės sistemos apsaugos priemones, todėl ta informacinė sistema, kuri prieinama kaltininkui, turi būti būtinai apsaugota apsaugos priemonėmis, norint tokiam asmeniui inkriminuoti BK 198^1 straipsnį.

14. Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui kol kas sudaro labai mažą bendro nusikalstamumo dalį (iki 0,2%). Pastebimas didelis nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui šuolis nuo 2006 m. iki 2007 m. ir nuo 2007 m. iki 2008-09-01. Žinant apie labai didelį šių nusikalstamų veikų latentiškumą, šie duomenys yra itin svarbūs, darant prognostines nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kitimo tendencijas.

LITERATŪROS SĄRAŠAS

I. Teisės aktai

1. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0890:EN:HTML; prisijungimo laikas: 2007-12-15.

2. Convention on Cybercrime // http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; prisijungimo laikas: 2007-10-12.

3. Convention on Cybercrime. Explanatory Report // http://conventions.coe.int/Treaty/en/Reports/Html/185.htm; prisijungimo laikas: 2007-10-24.

4. Estijos baudžiamasis kodeksas // http://www.legislationline.org/upload/legislations/07/6a/4d16963509db70c09d23e52cb8df.htm; prisijungimo laikas 2008-07-14.

5. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=19841&p_query=&p_tr2=; prisijungimo laikas: 2007-08-15.

6. Lietuvos Aukščiausiojo Teismo Teisėjų Senato nutarimas Nr. 29 „Dėl teismų praktikos veikas pripažįstant mažareikšmėmis“ // Teismų praktika. 2000, Nr. 14.

7. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 1996, Nr. 63-1479.

8. Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Lietuvos Respublikos baudžiamasis kodeksas (su pakeitimais ir papildymais iki 2008 m. birželio 12 d.) // Valstybės žinios. 2004, Nr. 25-760.

9. Lietuvos Respublikos baudžiamojo kodekso 7, 38, 47, 63, 66, 70, 75, 82, 93, 129, 166, 167, 172, 178, 180, 181, 182, 183, 184, 185, 189, 194, 196, 197, 198, 198^1, 198^2, 199, 202, 213, 214, 215, 225, 227, 228, 231, 233, 235, 252, 256, 257, 262, 284, 285, 312 straipsnių, priedo pakeitimo ir papildymo, XXVI, XXX skyrių pavadinimų pakeitimo ir kodekso papildymo 256^1, 257^1 straipsniais įstatymas // http://www3.lrs.lt/pls/inter3/dokpaieska.showdocl?pid=301997; prisijungimo laikas: 2008-08-11.

10. 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 198^1 straipsniais įstatymas // Valstybės žinios. 2000, Nr. 89-2741.

11. Lietuvos Respublikos civilinis kodeksas (su pakeitimais ir papildymais iki 2008 m. birželio 3 d.) // Valstybės žinios. 2000, Nr. 74-2262.

12. Lietuvos Respublikos elektroninio parašo įstatymas // Valstybės žinios. 2000, Nr. 61-1827.

13. Lietuvos Respublikos elektroninių ryšių įstatymas // Valstybės žinios. 2004, Nr. 69-2382.
14. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas // Valstybės žinios. 2006, Nr. 65-2380.
15. Lietuvos Respublikos Konstitucija // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_1?p_id=274999; prisijungimo laikas: 2007-09-10.
16. Lietuvos Respublikos Konstitucinio teismo išvada ,,Dėl Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 4, 5, 9, 14 straipsnių ir jos ketvirtojo protokolo 2 straipsnio atitikimo Lietuvos Respublikos Konstitucijai“ // Valstybės žinios. 1995, Nr. 9-199.
17. Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas // Valstybės žinios. 1997, Nr. 2-16.
18. Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas // http://www3.lrs .lt/pls/inter3/dokpaies ka.showdoc_l?p_id=314533; prisijungimo laikas: 2008-04-17.
19. Lietuvos Respublikos Sveikatos apsaugos ministro, Lietuvos Respublikos Teisingumo ministro ir Lietuvos Respublikos Socialinės apsaugos ir darbo ministro įsakymas ,,Dėl sveikatos sutrikdymo masto nustatymo taisyklių patvirtinimo“ // http://www3.lrs.lt/pls/inter3/dokpaieska.showdocl?p_id=211886&p_query=&p_tr2=; prisijungimo laikas: 2008-06-04.
20. Lietuvos Respublikos Vyriausybės Informacinės visuomenės plėtros komiteto direktoriaus įsakymas ,,Dėl asmeninio kompiuterio vienetą sudarančių elementų sąrašo patvirtinimo“ // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=240019; prisijungimo laikas: 2008-05-03.
21. The Criminal Code of the Republic of Croatia // http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation__Criminal-Code.pdf; prisijungimo laikas: 2008-09-26.
22. The Criminal Code of the Russian Federation // http://www.russian-criminal-code.com/PartII/SectionIX/Chapter28.html; prisijungimo laikas: 2008-09-26.
23. 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=COM:2005:0583:FIN:LT:HTML; prisijungimo laikas: 2008-08-27.

II. Specialioji literatūra

24. Abramavičius A. ir kt. Baudžiamoji teisė: bendroji dalis. – Vilnius: Eugrimas, 2001.
25. Adduci M. Cybercrime: riflessioni sulla produzione normativa in Italia. http://www.cybercrimes.it/articoli/ci_prodnorm.php; prisijungimo laikas: 2007-12-08.
26. Bainbridge D. I. Introduction to Computer Law. - Harlow: Pearson, Longman, 2004.
27. Beaupre D., Cassaday W. State and Local Law Enforcement Need to Combat Electronic Crimes. - National Institute of Justice, US Department of Justice, 2000.

28. Berzin P. Bank Computer Crimes Classification. http://www.crime-research.org/library/Berzin_ eng.htm; prisijungimo laikas: 2007-11-20.
29. Bylenchuk P. D. Organized Transnational Computer Crime: the Global Problem of the Third Millenium. http://www.crime-research.org/library/Bileng.htm; prisijungimo laikas: 2007-12-11.
30. Brenner S. W., Goodman M. D. The Emerging Consensus on Criminal Conduct in Cyberspace. - Boston, 2005.
31. Broderick T. R. Regulation of Information Technology in the European Union. - London: Springer, 2000.
32. Charney S., Alexander K. Computer Crime. http://www.crime-research.org/library/Alex.htm ; prisijungimo laikas: 2008-07-12.
33. Civilka M. ir kt. Informacinių technologijų teisė. - Vilnius: NVO Teisės institutas, 2004.
34. Cybercrime and Jurisdiction: a Global Survey / edited by Koops B. J., Brenner S. W. - The Hague: T. M. C. Asser Press, 2006.
35. Computer law / edited by Angel J., Reed C. - Oxford: Oxford University Press, 2007.
36. Computer-Related Crime. The Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 18-25 April 2005, Bangkok, Thailand. http://www.unis.unvienna.org/pdf/05-82111 _ E_6_pr_SFS.pdf; prisijungimo laikas: 2008-08-23.
37. Computer Security Institute. Computer Crime and Security Survey 2000. http://www.gocsi.com/prelea000321.htm; prisijungimo laikas: 2008-07-05.
38. Convention on Cybercrime. Status as of: 25/9/2008. http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=9/25/2008&CL=ENG; prisijungimo laikas: 2008-11-01.
39. Electronic Privacy Information Center. Cookies. http://epic.org/privacy/cookies/default.html ; prisijungimo laikas: 2008-04-11.
40. Criminalità informatica: cos'è realmente e dove si trova? http://innovatorining.com/group/intmetecrimineinnovazionenelleindagini; prisijungimo laikas: 2008-08-24.
41. Crimine economico e computer forenser. - Roma: Experta Edizioni, 2008.
42. Čėsna R., Štitilis D. Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. - Vilnius: LTA Leidybos centras, 2000.
43. Eoghan C. Digital Evidence and Computer Crime. – New York: Academic Press, 2000.
44. Federal Bureau of Investigation. Internet Crime Report 2006. http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf; prisijungimo laikas 2008-05-14.
45. Forensic Computer Crime Investigation / edited by Johnson Th. A. – New York: CRC Press, Taylor & Francis, 2006.

46. Golubev V. Computer Crime Fighting Problems. http://www.crime-research.org/library/Golte.htm; prisijungimo laikas: 2008-01-22.
47. Golubev V. The Computer Information as the Proof on Criminal Case. http://www.crime-research.org/library/Gol_temE2.htm; prisijungimo laikas: 2008-01-20.
48. Grabosky P. Computer Crime: a Criminological Overview. – Sidney, 2000.
49. Gringras C., Nathanson N. The Laws of the Internet. – New York: Butterworths, 1997.
50. Handbook of Computer Crime Investigation: Forensic Tools and Technology / edited by Casey E. - San Diego: Elsevier Academic Press, 2004.
51. Icove D. ir kt. Computer Crime: Crimefighter‘s Handbook. – New York: O’Reilly Media Inc, 1995.
52. Information Technology law group. European Computer Law. - New York: Transnational Publishers, 1995.
53. Informacinių technologijų institutas. Lietuvos kompiuterininkų sąjunga. Pagrindinės informacijos technologijos sąvokos. – Vilnius: Žara, 2001.
54. Keras A., Petrauskas R. Informatikos nusikaltimų tyrimo problemos // Valstybinė mokslo programa ,,Nusikalstamumas ir kriminalinė justicija“. Galutinė ataskaita, III dalis. Nusikaltimų tyrimo problemos Lietuvoje, 4 knyga. – Vilnius: LPA, 1997.
55. Klimas T. Šiuolaikinis nusikalstamumas. - Kaunas: VDU, 2002.
56. Kompiuterinės sistemos programinė įranga. http://distance.ktu.lt/kursai/informatika1/3/index.html; prisijungimo laikas: 2008-09-21.
57. Ku R. S. R. ir kt. Cyberspace Law: Cases and Materials. - New York: Aspen law & Business, 2002.
58. Lessig L. Code and Other Laws of Cyberspace, Version 2.0. - Basic Books, 2006.
59. Lindsay J. Information Systems – Fundamentals and Issues. - Kingston University, School of Information Systems, 2000.
60. Macdonald E., Rowland D. Information technology law. – London, 2005.
61. Magnin C. J. The 2001 Council of Europe Convention on Cyber-Crime: an Efficient Tool to Fight Crime in Cyber-Space? http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf; prisijungimo laikas: 2008-02-17.
62. Mayer-Schönberger V. The Cookie Concept. http://www.cookiecentral.com/content.phtml?area= 2&id=1; prisijungimo laikas: 2008-06-02.
63. Mukhtar M. Computer Crime: The New Threat. http://www.crime-research.org/library/Mudavi1.htm; prisijungimo laikas: 2008-03-08.
64. Panomariovas A. Viešai neskelbiama informacija (paslaptis) baudžiamajame procese: daktaro disertacija (socialiniai mokslai, teisė) / LTU. – V., 2001.

65. Petrauskas R., Štitilis D. Kai kurios interneto teisinės problemos // Informacinės technologijos 99: konferencijos pranešimai. - Kaunas: Technologija, 1999.
66. Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. - Vilnius: LTA Leidybos centras, 2000.
67. Piesliakas V. Lietuvos baudžiamoji teisė. Baudžiamasis įstatymas ir baudžiamosios atsakomybės pagrindai. Kn. 1. - Vilnius: Justitia, 2006.
68. Piesliakas V. Lietuvos baudžiamoji teisė. Aplinkybės, darančios įtaką baudžiamajai atsakomybei, ir nusikalstamos veikos teisiniai padariniai pagrindai. Kn. 2. - Vilnius: Justitia, 2006.
69. Polivanjuk V. Criminal Characteristic of Crimes Committed in the Banking System by Using Up-To-Date Information Technologies. http://www.crime-research.org/library/Polivan_tem3E.htm; prisijungimo laikas: 2008-05-19.
70. Poullet Y. Towards Confidence: Views from Brussels: a European Internet law. - Brussels, 2003.
71. Robinson J. K. Internet as the Scene of Crime // International Computer Crime Conference. - Oslo, 2000.
72. Sbrizzo A. Nel 2003 Cupido è un computer e lo spam un crimine. http://www.infocity.go.it/vedi_a rticolo.php?id=2873; prisijungimo laikas: 2008-07-26.
73. Sieber U. Computerkriminalität und Strafrecht. - Köln: Carl Heymanns Verlag, 1980.
74. Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study. http://law.scu.edu/international/File/Sieber_final.pdf; prisijungimo laikas: 2008-01-26.
75. Sieber U. The International Handbook on Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy. – London: John Wiley & Sons Inc, 1996.
76. Steponavičienė G. Informacinės sistemos - galimybė sumažinti administravimo naštą. // Pranešimo tezės konferencijoje „Proliberalios reformos mokesčių naštai sumažinti“. - Vilnius, 1997.
77. The Privacy Dilemma in the Internet Age. http://www.usatoday.com/tech/news/2001-05-09-privacy-analysis.htm#more; prisijungimo laikas: 2008-06-21.
78. Trust and Privacy Online: Why Americans Want to Rewrite the Rules // The Internet Life Report. – Boston, 2000.
79. Tsai J. T. The Misery of Mitra: Considering Criminal Punishment for Computer Crimes. http://law.bepress.com/expresso/eps/853; prisijungimo laikas: 2008-04-17.
80. Vaišvila A. Teisės teorija. Vilnius: Justitia, 2000.

81. Wahlert G. Crime in Cyberspace: Trends in Computer Crime in Australia // Australian Institute of Criminology Conference „Internet Crime“. - Melbourne, 1998. http://www.aic.gov.au/conferences/internet/wahlert.pdf; prisijungimo laikas: 2007-12-07.

82. Айков Д., Сейгер К. Компьютерные преступления: руководство по борьбе с компьютерными преступлениями. - Москва: Мир, 1999.

83. Дутов М. Ответственность за компьютерные преступления в Уголовном кодексе Украины. http://www.crime-research.org/library/dutov.htm; prisijungimo laikas: 2008-04-16.

84. Мандиа К., Просис К. Защита от вторжений: расследование компьютерных преступлений. - Москва: Лори, 2005.

85. Воронов Я. Понятие преступлений в сфере высоких технологий. http://www.crime-research.org/library/cyberpon.htm; prisijungimo laikas: 2007-11-09.

III. Periodiniai leidiniai

86. Anconelli M. Autopsy & Sleuthkit, Computer Forensics Open Source // Computer Forensics & Crimine Informatico. 2005, Nr. 5.

87. Babachinaitė G. Socialiniai pokyčiai ir nusikalstamumas. Teisinės valstybės link // Jurisprudencija. 2000, Nr. 15(7).

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

89. Chiliarchaki P., Dowland P. S., Furnell S. M. Security Analysers: Administrator Assistants or Hacker Helpers? // Information Management & Computer Security. 2001, Nr. 9/2.

90. Ciro T. The Scarcity of Intellectual Property // The Journal of Information, Law and Technology. 2005, Nr. 1.

91. Computer Intrusions and Attacks // The Electronic Library. 1999, Nr. 17(2).

92. Desai M. S., Richards T. S. System Insecurity – Firewalls // Information Management & Computer Security. 2002, Nr. 10(3).

93. Drakšienė A. Bausmių skyrimo ribos // Teisė. 1995, Nr. 29.

94. Exon S. N. Personal Jurisdiction: Lost in Cyberspace? // Computer Law Review and Technology Journal. 2003, Nr. 8.

95. Fedosiuk O. Nuosavybė ir turtas civiliniame ir baudžiamajame kodeksuose // Jurisprudencija. 2002, Nr. 28(20).

96. Fletcher N. Challenges for Regulating Financial Fraud in Cyberspace // Journal of Financial Crime. 2007, Nr. 14(2).

97. Hinnen T. M. The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet // The Columbia Science and Technology Law Review. 2004, Nr. 5.

98. Hoffstadt B. M., Wong Yang D. Countering the Cyber-Crime Threat // American Criminal Law Review. 2006, Nr. 43(2).
99. Hoofnagle C. J. Identity Theft: Making The Known Unknowns Known // Harvard Journal of Law and Technology. 2007, Nr. 21(1).
100. Hutchinson W., Warren M. Attitudes of Australian Information System Managers against Online Attackers // Information Management & Computer Security. 2001, Nr. 9/3.
101. Icove D. J. Collaring the Cybercrook: an Investigator‘s View // Spectrum. 1997, Nr. 34(6).
102. Yar M. Computer Hacking: Just Another Case of Juvenile Delinquency? // The Howard Journal. 2005, Nr. 44(4).
103. Johnson D., Post D. Law and Borders – the Rise of Law in Cyberspace // Stanford Law Review. 1996, Nr. 48.
104. Jordan T., Taylor P. A Sociology of Hackers // The Sociological Review. 1998, Nr. 2
105. Kaminskaitė J., Ramanauskas G. Kaip kovoti su nepageidaujamomis elektroninėmis žinutėmis // Juristas. 2006, Nr. 1.
106. Kapočiūtė J. Ar viešumo principas suponuoja tikrąjį viešumą? // Teisės apžvalga. 2005, Nr. 5.
107. Klingys V. ir kt. Nusikaltimų, susijusių su interneto panaudojimu, kompiuteriniai tyrimai // Jurisprudencija. 1999, Nr. 14(6).
108. Leichteris E. Kompiuteriniai nusikaltimai // Naujoji komunikacija. 1999, Nr. 19.
109. Mitašiūnas A. Žvilgsnis iš informatikos varpinės // Mokslas ir gyvenimas. 1999, Nr. 9.
110. Nykodym N., Taylor R. Control of Cyber Crime. The World‘s Current Legislative Efforts against Cyber Crime // Computer Law & Security Report. 2004, Nr. 20(5).
111. Overill R. Reacting to Cyber-Intrusions: the Technical, Legal and Ethical Dimensions // Journal of Financial Crime. 2006, Nr. 11(2).
112. Petrauskas R., Štitilis D. Lietuvos Respublikos baudžiamasis kodeksas Nusikaltimų elektroninėje erdvėje konvencijos kontekste // Jurisprudencija. 2002, Nr. 24(16).
113. Ryan P. S. War, Peace, or Stalemate: Wargames, Wardialing, Wardriving and the Emerging Market for Hacker Ethics // Virginia Journal of Law & Technology. 2004, Nr. 9(7).
114. Rupp T., Smith A. Issues in Cybersecurity: Understanding the Potential Risks Associated with Hackers/Crackers // Information Management & Computer Security. 2002, Nr. 10/4.
115. Sabaliauskas G. Informacijos saugumas internete: teisininkų ir informatikų problema // Justitia. 2001, Nr. 1.
116. Smith A. Cybercriminal Impact on Online Business and Consumer Confidence // Online Information Review. 2004, Nr. 28(3).

117. Štitilis D. Neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimas // Informacijos mokslas. 2003, Nr. 26.
118. Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai // Jurisprudencija. 2003, Nr. 47(39).
119. United Nations Manual on the Prevention and Control of Computer-Related Crime // International Review of Criminal Policy. 1994, No. 43/44.

IV. Statistiniai rinkiniai

120. Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos statistika // http://www.vrm.lt/fileadmin/Image_Archive/IRD/Statistika/index2.phtml?id=198; prisijungimo laikas: 2008-09-15.
121. Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Nusikalstamumas ir teisėsaugos insttiucijų veikla 2006. - Vilnius, 2007.
122. Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Nusikalstamumas ir teisėsaugos institucijų veikla 2007. - Vilnius, 2008.

V. Teismų praktika

123. Byla Korporacija (duomenys neskelbtini) v. K. H. The Berkman Center for Internet & Society. http://cyber.law.harvard.edu/ openlaw/intelvhamidi/; prisijungimo laikas: 2008-09-11.
124. Byla O. v. M. http://74.125.113.132/search?q=cache:9BrWpRvWdj8J:www.a-level-law.com/caselibrary/OXFORD%2520v%2520MOSS%2520%255B1979%255D%2520Crim%2520LR%2520119%2520-%2520DIV.doc+Oxford+v.+Moss&hl=lt&ct=clnk&cd=3&gl=lt; prisijungimo laikas: 2008-08-21.
125. Byla R v. S. G. ir R. S. Discuss Law. http://www.swarb.co.uk/lawb/cpucmaRvGold.shtml ; prisijungimo laikas: 2008-07-05.
126. Byla Jungtinės Amerikos Valstijos v. M. The Center for Internet and Society. http://cyberlaw.Stanford.edu/taxon omy/term/198; prisijungimo laikas: 2008-08-14.
127. Byla Jungtinės Amerikos Valstijos v. R. T. M. http://www.loundy.com/cases/us_v_Morris2.html; prisijungimo laikas: 2008-07-26.
128. Vilniaus miesto 1 apylinkės teismo baudžiamoji byla Nr. 1-00857-276/2005.
129. Vilniaus miesto 1 apylinkės teismo baudžiamoji byla Nr. 1-538-463/2007.
130. Vilniaus miesto 1 apylinkės teismo baudžiamoji byla Nr. 1-17-296/2008.
131. Vilniaus miesto 3 apylinkės teismo baudžiamoji byla Nr. N-1-565-119/05.

SANTRAUKA

,,Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui samprata ir baudžiamoji atsakomybė už juos. Problemos pagal Lietuvos Respublikos baudžiamąjį kodeksą“

Pagrindinės sąvokos: nusikalstamos veikos elektroninėje erdvėje, nusikalstamos veikos, susijusios su kompiuteriais, kompiuterinis nusikaltimas, nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui, baudžiamoji atsakomybė, Lietuvos Respublikos baudžiamasis kodeksas.

Informacinės sistemos ir elektroniniai duomenys gali būti naudojami daryti baudžiamajame įstatyme numatytoms nusikalstamoms veikoms bei sudaryti naujas galimybes įvykdyti veikas, iki tol nežinomas teisinėje praktikoje. Nors fiziniai asmenys, padarę nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, de lege lata yra traukiami baudžiamojon atsakomybėn, tačiau de lege ferenda tai padaryti yra nelengva, kadangi Lietuvoje beveik nėra išsamios baudžiamosios teisinės doktrinos ir teismų praktikos, kuria būtų galima remtis, aiškinant ir taikant baudžiamojo įstatymo normas, nustatančias baudžiamosios atsakomybės už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui prielaidas. Todėl, mūsų manymu, viena iš aktualiausių Lietuvos baudžiamosios teisės teorijos temų ir yra konceptuali baudžiamosios atsakomybės už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui analizė.

Šiame tiriamajame darbe yra nagrinėjami nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui objektyvieji ir subjektyvieji požymiai, pagal kokius požymius šios veikos atribojamos nuo kitų nusikalstamų veikų, kokios kyla nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kvalifikavimo problemos. Dėl ribotos šio darbo apimties nagrinėjama tik fizinių asmenų baudžiamoji atsakomybė už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, neanalizuojant juridinių asmenų atsakomybės už šias nusikalstamas veikas. Tarptautiniai teisės aktai, reglamentuojantys baudžiamosios atsakomybės nustatymą ir taikymą už šias nusikalstamas veikas, taip pat nebus detaliai nagrinėjami, o apžvelgiami tik BK XXX skyriuje įtvirtintų nusikalstamų veikų sudėčių suderinamumo su jais aspektu. Šalia teorinių aspektų analizuojama teismų praktika, siekiant atskleisti BK XXX skyriuje numatytų straipsnių taikymą ir aiškinimą, nagrinėjant baudžiamąsias bylas dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui.

SUMMARY

„Concept of Criminal Acts against Security of Electronic Data and Information Systems and Criminal Liability for Them. Problems in Accordance with Criminal Code of the Republic of Lithuania“

Keywords: computer crime, crimes related with computer, criminal acts against security of electronic data and information systems, electronic data, information system, criminal liability, electronic space, Criminal Code of the Republic of Lithuania.

In the process of creating an information society, modern information technologies are being spread in all spheres of human activity, thus information technologies are being inevitably used both for legitimate and non legitimate purposes. Information systems and electronic data can be used by criminals to commit criminal acts against security of electronic data and information systems.

This topic is a matter of great relevance of several causes. Prima facie, although the criminal acts against security of electronic data and information systems represent a very small part of a total criminality, their significance among other crimes are caused by special values secured by criminal laws (security of electronic data and information systems) and big damages made by them to the victim, or in some cases, to the state management, financial and economy systems, objects of the strategic importance of national security. Secondly, these criminal acts are of big delitescence, thirdly, investigation of these crimes require enormous time and funds. Fourthly and thus the most important, criminals, had committed criminal acts against security of electronic data and information systems, de lege lata are arraign for criminal liability, but de lege ferenda it is not easy, since there is a big lack of complete criminal legal doctrines and case law, which could be used for the interpretation and application of criminal laws, stipulating criminal liability for criminal acts against security of electronic data and information systems in the Republic of Lithuania.

The object of thesis – criminal acts against security of electronic data and information systems and criminal liability for them in accordance with Criminal Code of the Republic of Lithuania and case law. The hypothesis is that the legal regulation of criminal acts against security of electronic data and information systems is complicated and presently not capable because of theoretical and practical problems of concept of these criminal acts and criminal liability for them. To disclose all the issues mentioned above the analysis of the scientific literature of criminal law theory, Criminal Code of the Republic of Lithuania, case law,

conceptual issues of criminal liability for criminal acts against security of electronic data and information systems is made, to assess statistical data trends of the criminal acts against security of electronic data and information systems during 2004 - 2008-09-01 period. Methods used: comparative, historical, systemic analysis, inductive - deductive, logical - analytical and content analysis.

Magistro baigiamasis darbas ,,Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui samprata ir baudžiamoji atsakomybė už juos. Problemos pagal Lietuvos Respublikos baudžiamąjį kodeksą“ baigtas 2008 m. gruodžio 1 d.

Asta Benetytė