MYKOLO ROMERIO UNIVERSITETAS

SOCIALINĖS INFORMATIKOS FAKULTETAS

ELEKTRONINIO VERSLO KATEDRA

VALDAS KLIŠAUSKAS

Naujų technologijų teisė

ELEKTRONINIŲ NUSIKALTIMŲ REGLAMENTAVIMAS RUSIJOJE IR LIETUVOJE: LYGINAMIEJI ASPEKTAI

Magistro baigiamasis darbas

Darbo vadovas –

doc. dr. Darius Štitilis

Vilnius, 2012

TURINYS

ĮVADAS

Temos aktualumas. XXI amžiuje sparčiai tobulėjant informacinėms ir kompiuterinėms technologijoms, didėjant interneto prieinamumui bei įvairiausių elektroninių paslaugų (tokių kaip elektroninė bankininkystė, internetinės parduotuvės ir pan.) pasiūlai, vis stipriau šios technologijos įsišaknija visose žmonių gyvenimo srityse. Nežiūrint to, kad šios vadinamosios „aukštosios technologijos“ įnešė daug teigiamų pokyčių į kasdieninį žmogaus gyvenimą, tačiau tuo pačiu atvėrė kelius ir naujos rūšies nusikaltimų atsiradimui.

Dabartiniame technikos amžiuje, nieko jau nebestebina žinios apie naujo viruso paplitimą, įsilaužimą į duomenų bazes, informacijos pavogimą ar neteisėto banko atsiskaitymo atlikimą. Tačiau kuo toliau tuo kibernetinės atakos darosi vis sudėtingesnės (Trojos arkliai, kompiuterių zombių tinklai ir kt.), jas rengiant dažnai vadovaujamasi ne tik noru parodyti savo išradingumą, profesines žinias ar gauti finansinės naudos, bet ir politiniais, rasistiniais ar seksualinio išnaudojimo motyvais. Elektroninis nusikalstamumas tapo pasauliniu reiškiniu, darančiu vis daugiau žalos atskiriems piliečiams, organizacijoms, visai visuomenei, valstybei. Dauguma pasaulio valstybių elektroninius nusikaltimus pagal jų pavojingumą ir pelningumą netgi prilygina tokioms nusikalstamoms veikoms kaip terorizmas ir prekyba narkotikais. Todėl elektroninių nusikaltimų teisinio reglamentavimo problema yra viena iš pačių aktualiausių visame pasaulyje, tame tarpe ir Lietuvoje, ir mūsų kaimynystėje esančioje Rusijoje.

Kaip liudija statistiniai duomenys, Rusijoje per metus yra įvykdomas ne vienas tūkstantis elektroninių nusikaltimų. Atsižvelgiant į tai, kad kai kurių ekspertų vertinimu elektroninių nusikaltimų latentiškumas Rusijoje sudaro 95 proc., realus įvykdomų elektroninių nusikaltimų skaičius turėtų būti dar keliasdešimt kartų didesnis. Be to, kasdien iš Rusijos registruojamos ir kompiuterinės atakos, nukreiptos prieš fizinius ar juridinius asmenis, įsikūrusius kitose valstybėse. Šios šalies elektroniniai nusikaltėliai neretai laikomi vienais profesionaliausių pasaulyje, sumaniai naudojantys kompiuterius ir internetą šnipinėjimui, manipuliavimui bankų informacija, interneto puslapių nulaužimui, duomenų vagystėms ir pan. Dėl to, Rusijoje skiriamas gana nemažas dėmesys elektroninių nusikaltimų problemai spręsti.

Atitinkamos teisinės bazės kūrimas Rusijoje buvo pradėtas jau 1990 metų pradžioje ir per pastaruosius kelis dešimtmečius vyko nuolatinis jos tobulinimas. Tačiau Rusija, skirtingai nei Lietuva, vis dar yra neratifikavusi Konvencijos dėl elektroninių nusikaltimų, kuri dabar jau neretai yra kritikuojama, kad yra neveiksminga, todėl svarbu yra išnagrinėti Rusijoje taikomą praktiką. Išnagrinėjus elektroninių nusikaltimų teisinio reglamentavimo praktikos Rusijoje ir Lietuvos Respublikoje panašumus ir skirtumus, būtų galima įvertinti Rusijos Federacijos ir Lietuvos

Respublikos įstatymų dėl elektroninių nusikaltimų išbaigtumą ir atitikimą greitai tobulėjantiems elektroniniams nusikaltimams, identifikuoti pagrindines elektroninių nusikaltimų reglamentavimo problemas ir pateikti pasiūlymus dėl gerosios Rusijos praktikos perėmimo. Taigi, šio darbo rezultatai galėtų būti naudingi įstatymų leidėjui, nes geriausią Rusijos Federacijos praktiką galima būtų perkelti į nacionalinius norminius teisės aktus.

Temos naujumas. Ilgą laiką elektroninių nusikaltimų reglamentavimo tema Lietuvoje mažai ką domino, tačiau pastaruoju laikotarpiu ji jau vis dažniau rūpi ne tik teisininkams – praktikams, bet ir mokslininkams. Vis gi, iki šiol elektroninių nusikaltimų nagrinėjimas Lietuvos mokslinėje literatūroje yra pakankamai ribotas. Atskirų elektroninių nusikaltimų rūšių reglamentavimo aspektus nagrinėjo: D. Štitilis, M. Kiškis, I. Rotomskis, R. Petrauskas, M. Laurinaitis, M. Civilka ir kt.

Visuose iki šiol rašytuose magistro baigiamuosiuose darbuose buvo nagrinėjami tik elektroninių nusikaltimų sampratos, atskirų elektroninių nusikaltimų rūšių teisinio reglamentavimo, elektroninių nusikaltimų tyrimo klausimai: Girdauskienė R. Nusikaltimų informatikai baudžiamoji teisinė charakteristika: magistro baigiamasis darbas. 2006; Bernotavičius V. Nusikaltimai elektroninių duomenų ir informacinių sistemų konfidencialumui, vientisumui ir prieinamumui: kriminalizavimas lyginamuoju aspektu: magistro baigiamasis darbas. 2006; Savickas M. Nusikaltimų informatikai sampratos problema: magistro baigiamasis darbas. 2007; Krikščiūnas R. Baudžiamosios jurisdikcijos elektroninėje erdvėje problemos: magistro baigiamasis darbas. 2008; Brundzas N. Elektroninių nusikaltimų konvencijos įgyvendinimas Lietuvoje baudžiamojo proceso prasme: magistro baigiamasis darbas. 2008; Gelažienė J. Vaikų pornografija internete: teisinis reguliavimas ir kontrolės problemos: magistro baigiamasis darbas. 2008; Barusevičienė J. Elektroninių nusikaltimų tyrimo ypatumai įgyvendinant konvenciją dėl elektroninių nusikaltimų: magistro baigiamasis darbas. 2009; Dauparaitė I. Tapatybės vagystės elektroninėje erdvėje teisiniai aspektai: magistro baigiamasis darbas. 2010.

Reikia pripažinti, jog rusų autoriai gerokai anksčiau pradėjo domėtis elektroniniais nusikaltimais ir jų teisinio reglamentavimo analize. Elektroninių nusikaltimų sąvokos problemą, elektroninių nusikaltimų teisinio reglamentavimo Rusijoje ir jų kriminalistinių tyrimų aspektus, tarptautinės teisinės bazės elektroninių nusikaltimų srityje klausimus nagrinėjo Богомолов М.В., Дремлюга Р.И., Мазуров В., А. Вехов В. Б., Попова В. В., Волеводз А. Г. Серго А. ir kt.

Tačiau literatūros šaltiniuose nepavyko surasti palyginimo tarp elektroninių nusikaltimų reglamentavimo praktikos Rusijos Federacijoje ir Lietuvos Respublikoje.

Tyrimo objektas – elektroniniai nusikaltimai.

Tyrimo dalykas – Rusijos Federacijos ir Lietuvos Respublikos teisės aktai, reglamentuojantys elektroninius nusikaltimus (lyginamuoju aspektu).

Darbo tikslas – išanalizuoti ir tarpusavyje palyginti elektroninių nusikaltimų reglamentavimą Rusijos Federacijoje ir Lietuvos Respublikoje.

Uždaviniai:

- Išanalizuoti elektroninių nusikaltimų sampratą.
- Lyginamuoju aspektu išanalizuoti svarbiausių Lietuvos Respublikos ir Rusijos Federacijos teisės aktų nuostatas dėl elektroninių nusikaltimų.
- Lyginamuoju aspektu išanalizuoti Lietuvos Respublikos ir Rusijos Federacijos baudžiamųjų kodeksų nuostatas dėl elektroninių nusikaltimų.
- Pateikti pasiūlymus dėl elektroninių nusikaltimų reglamentavimo problemų sprendimo galimybių.

Darbe kompleksiškai buvo naudojami įvairūs **tyrimo metodai.**

Dokumentų analizės metodo pagalba analizuotos mokslinėje literatūroje, teisiniuose aktuose bei kituose dokumentuose pateiktos elektroninių nusikaltimų sampratos, rūšys.

Teisinių dokumentų analizės metodas kartu su *loginiu - analitiniu metodu* naudotas nagrinėjant Lietuvos ir Rusijos nacionaliniuose teisės aktuose įtvirtintų nuostatų dėl elektroninių nusikaltimų ypatumus, atskleidžiant teisės normų turinį.

Lyginamasis metodas taikytas atskleidžiant Lietuvos ir Rusijos nacionalinių teisės aktų dėl elektroninių nusikaltimų skirtumus ir bendrumus, taip pat palyginant nacionalinių teisės aktų nuostatas su tarptautinių dokumentų reikalavimais. Lyginamasis metodas taip pat naudotas lyginant skirtingų autorių požiūrius.

Apibendrinimo metodo pagalba pateikiamos tarpinės ir galutinės darbo išvados ir apibendrinama naudota literatūra. Formuluojant šio darbo išvadas buvo taikyti ir dedukcijos bei indukcijos metodai.

Tyrimo šaltiniai. Rašant šį darbą buvo naudojami įvairūs šaltiniai: tarptautiniai, Lietuvos Respublikos ir Rusijos Federacijos teisės aktai, mokslinė literatūra, straipsniai moksliniuose leidiniuose, su darbo tema susijusi teismų praktika ir statistika.

Darbo struktūra. Magistro darbą sudaro trys dalys ir išvados bei pasiūlymai. Atitinkamai dalys yra suskirstytos į skyrius pagal nagrinėjamų klausimų pobūdį. Pirmojoje dalyje aptariame

elektroninių nusikaltimų sampratą. Antrojoje darbo dalyje lyginamuoju aspektu nagrinėjame pagrindinių tarptautinių ir regioninių dokumentų įgyvendinimo Lietuvos Respublikoje ir Rusijos Federacijoje praktiką, elektroninių nusikaltimų teisinio reglamentavimo klausimus Lietuvos Respublikoje ir Rusijoje. Trečiojoje dalyje analizuojame ir tarpusavyje lyginame Lietuvos Respublikos ir Rusijos Federacijos baudžiamųjų kodeksų nuostatas, numatančias atsakomybę už elektroninius nusikaltimus.

1. ELEKTRONINIŲ NUSIKALTIMŲ SAMPRATA

Prieš pradedant nagrinėti elektroninių nusikaltimų reglamentavimo Lietuvoje ir Rusijoje teisinius aspektus, svarbu būtų apsibrėžti pačią „elektroninio nusikaltimo“ sąvoką. Siekiant šio uždavinio apžvelgsime teisinėje literatūroje ir teisės aktuose pateikiamų apibrėžimų įvairovę.

Nuo pat elektroninių nusikaltimų atsiradimo, mokslininkai vis ieško naujų sąvokų, kurios galėtų tiksliau išreikšti šių nusikaltimų esmę. Literatūroje kalbant apie elektroninius nusikaltimus naudojami įvairūs terminai, tokie kaip: „kompiuteriniai nusikaltimai“, internetiniai nusikaltimai“, „su kompiuteriais susiję nusikaltimai“, „aukštųjų technologijų nusikaltimai“, „informaciniai nusikaltimai“ ir kt. Neretai šie terminai vartojami ir kaip sinonimai. Tai patvirtina ir Europos Bendrijų Komisija 2007 m. gegužės 22 d. Komunikate Europos Parlamentui, Tarybai ir Regionų komitetui „Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais linkme” nurodydama, kad „terminai „elektroniniai nusikaltimai“, „kompiuteriniai nusikaltimai“, „su kompiuteriais susiję nusikaltimai“ arba „modernių technologijų nusikaltimai“ dažnai vartojami kaip sinonimai, nes nėra sutartos elektroninių nusikaltimų apibrėžties“[1]. George E. Higgings taip pat nurodo, kad kompiuteriniai nusikaltimai ir elektroniniai nusikaltimai yra iš esmės tas pats, nes skirtumas tarp jų yra labai nežymus. Kompiuteriniai nusikaltimai negali būti padaromi be kompiuterio. Elektroniniai nusikaltimai negali būti padaromi be kompiuterio ir tinklo[2].

Terminas „kompiuteriniai nusikaltimai“ pirmą kartą paminėtas jau 6 dešimtmetyje Jungtinių Amerikos Valstijų literatūroje, kai pirmą kartą buvo padaryti nusikaltimai kompiuterio pagalba. Nuo to laiko įvairūs mokslininkai bandė apibrėžti elektroninius nusikaltimus. Nagrinėjant mokslinėje literatūroje pateikiamus elektroninių nusikaltimų apibrėžimus galima teigti, jog šiuo metu egzistuoja keletas mokslinės minties srovių, skirtingai traktuojančių elektroninių nusikaltimų esmę.

Viena grupė mokslininkų elektroninių nusikaltimų sąvoką traktuoja ypač plačiai. Jie mano, kad prie elektroninių nusikaltimų turi būti priskiriamos tiek tos pavojingos veikos, kuriose kompiuteris ir/ar kompiuterinė informacija yra nusikaltimo objektas, tiek tos pavojingos veikos, kuriose kompiuteris ir/ar kompiuterinė informacija yra nusikalstamos veikos priemonė. Šiuo atveju prie elektroninių nusikaltimų priskiriama netgi paties kompiuterio vagystė.

Tuo tarpu kita grupė mokslininkų jau naudoja kiek siauresnę, tačiau tuo pačiu ir pakankamai plačią elektroninių nusikaltimų sąvoką. Jie pasisako, kad prie elektroninių nusikaltimų turi būti

[1] Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme {SEK(2007) 641} {SEK(2007) 642} http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:LT:NOT [2012-01-07]

[2] Higgins George E. Cybercrime: an introduction to an emerging phenomenom. New York: McGraw-Hill, 2010, p.1.

priskiriami tik tie nusikaltimai, kuriuose kompiuterinė informacija yra nusikaltimo dalykas, o kompiuteris tarnauja kaip nusikaltimo įrankis. Elektroniniais nusikaltimais turėtų būti laikomos baudžiamojo įstatymo numatytos pavojingos veikos, kurių objektai gali būti įvairūs, t.y. ne tik visuomeniniai santykiai informacijos apdorojimo srityje, bet ir autorių teisės, piniginės lėšos ir pan. Taigi, šiuo atveju elektroniniams nusikaltimams galime priskirti ir tokias pavojingas veikas kaip neteisėtas pinigų pervedimas iš vienos sąskaitos banke į kitą (taip vadinama „kompiuterinė vagystė“), nesankcionuotas informacijos rinkimas siekiant pakenkti kokiai nors organizacijai ar netgi valstybei („kompiuterinis špionažas“) ir pan. Elektroninis nusikaltimas nuo paprasto atskiriamas dėl savo technologijos, t.y. kompiuterinės technikos panaudojimo nusikaltimo padarymui. Vienas iš šios krypties atstovų Дремлюга Р.И. kalbėdamas apie elektroninius nusikaltimus vartoja internetinių nusikaltimų sąvoką ir apibrėžia juos taip: „tai bet kokios baudžiamuoju įstatymu uždraustos visuomenei pavojingos veikos, kurios padaromos internetu arba interneto pagalba. Tai apima ir nusikaltimus, kai internetas buvo naudojamas pasiruošimo nusikaltimui stadijoje“[3].

Trečioji dalis autorių dar labiau susiaurina elektroninių nusikaltimų sąvoką. Jie nurodo, kad elektroniniais nusikaltimais turėtų būti laikomos tik tos veikos, kurios nurodytos atskiruose baudžiamųjų įstatymų skirsniuose ir kurių objektas yra bendras – visuomeniniai santykiai informacijos apdorojimo srityje. Šiuo atveju elektroniniai nusikaltimai traktuojami gerokai siauresne prasme. Šios krypties atstovas Вехов В. Б. mano, kad kompiuteriniais nusikaltimais yra „...baudžiamojo įstatymo numatytos pavojingos veikos, kuriomis kėsinamasi į kompiuterinės informacijos saugumą ir šios informacijos apdorojimo priemones ir kurios yra išskirtos Rusijos Federacijos Baudžiamojo kodekso specialioje dalyje Nr. 28 „Nusikaltimai kompiuterinės informacijos srityje“[4].

Pateikus elektroninio nusikaltimo sąvokos apibrėžimus teisės doktrinoje, tikslinga būtų aptarti ir kaip ši sąvoka reglamentuota teisės aktuose.

Per pastaruosius dešimtmečius įvairios tarptautinės institucijos savo dokumentuose bandė apibrėžti elektroninių nusikaltimų sąvoką. Pirmosios šios sąvokos užuomazgos aptinkamos 1986 m. Ekonominio bendradarbiavimo ir plėtros organizacijos priimtoje rekomendacijoje, kurioje „su kompiuteriais susijęs nusikaltimas“ apibrėžiamas kaip bet koks neteisėtas, neetiškas ar nesankcionuotas elgesys, susijęs su automatiniu duomenų apdorojimu ir siuntimu. Mūsų nuomone, ši formuluotė yra pernelyg nekonkreti ir plati, nes joje neapibrėžiama, kokia teisės šaka reglamentuoja tokį neteisėtą elgesį. Be to, šiais laikais automatinis duomenų apdorojimas

[3] Дремлюга Р.И. Интернет преступность: моногр. Владивосток: Издательство Дальневосточного университета, 2008. http://www.telecomlaw.ru/monograph/Internet_crime_Dremlyga.pdf [2012-01-07]
[4] Вехов В. Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. Москва, 2000. www.cyberpol.ru/public/osobennosti_rassled.doc [2012-01-07]

naudojamas labai plačiai, taigi tokiu atveju šis apibrėžimas apimtų labai daug sričių, tokių kaip pavyzdžiui, nusikaltimai padaryti mobiliojo telefono pagalba.

1989 m. Europos Taryba rekomendacijoje Nr. R 89 (9) nepatvirtino jokio formalaus apibrėžimo, paprasčiausiai nurodydama, kad su kompiuteriu susiję nusikaltimai yra tos neteisėtos veikos, kurios yra išvardintos ir apibrėžtos pasiūlytose rekomendacijose valstybėms ir palikdama teisę kiekvienai valstybei pasitvirtinti savo apibrėžimą[5].

2001 m. lapkričio 23 d. Konvencijoje dėl elektroninių nusikaltimų taip pat nėra pateikta elektroninio nusikaltimo sąvokos. Tačiau, mūsų nuomone, elektroninių nusikaltimų sąvoka atsiskleidžia per šios konvencijos 2-10 str. kriminalizuotas veikas – apimamas itin platus spektras nusikalstamų veikų, kurių objektas iš esmės yra kompiuterinė informacija ir/ar kuriose kompiuteris naudojamas kaip nusikaltimo priemonė. Tai iš esmės atitinka mūsų jau minėtos antrosios mokslinės minties srovės atstovų nuomonę.

2007 m. gegužės 22 d. Komisijos Komunikate Europos Parlamentui, Tarybai ir Regionų komitetui „Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais linkme" elektroniniai nusikaltimai suprantami kaip „nusikalstamos veikos, padarytos naudojant elektroninių ryšių tinklus ir informacines sistemas, arba nusikalstamos veikos prieš tokius tinklus ir sistemas"[6]. Tai taip pat atitinka antrosios mokslinės minties srovės atstovų nuomonę.

Lietuvos Respublikos baudžiamajame kodekse terminas elektroniniai nusikaltimai nevartojamas ir sąvoka nepateikiama. Tačiau reikia pažymėti, kad Lietuvos Respublikos Seimas 2004 m. sausio 22 d. ratifikavo konvenciją dėl elektroninių nusikaltimų ir tokiu būdu Lietuvoje įteisino elektroninio nusikaltimo sąvoką.

Rusijos Federacijos Baudžiamajame kodekse terminas elektroniniai nusikaltimai taip pat nevartojamas, šiame teisės akte vartojama sąvoka „kompiuterinė informacija". Rusijos Federacijos Baudžiamojo kodekso 29 skyrius būtent taip ir vadinasi - „Nusikaltimai kompiuterinės informacijos srityje".

Taigi, apibendrinant tai, kas išdėstyta galime daryti išvadą, kad teisinėje literatūroje ir teisės aktuose trūksta aiškaus vieningo elektroninių nusikaltimų apibrėžimo, o Lietuvos Respublikos ir Rusijos Federacijos baudžiamuosiuose įstatymuose tokia sąvoka iš viso nepateikiama, todėl, tai skatina įvairių elektroninių nusikaltimų sąvokos interpretacijų atsiradimą. Nesant vieningos elektroninių nusikaltimų sampratos yra ypač apsunkinamas tokių nusikalstamų veikų susekimas, tyrimas ir baudžiamasis persekiojimas tarptautiniu lygiu, nes neretai gali nutikti taip, kad atitinkama

[5] Council of Europe. Computer-related crime. Recommendation No. R(89)9, adopted by Committee of Ministers of the Council of Europe on 13 September 1989 // Strasbourg, 1990. http://cm.coe.int/ta/rec/1989/89r9.htm [2012-01-08]

[6] Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui - Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme {SEK(2007) 641} {SEK(2007) 642} http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:LT:NOT [2012-01-08]

veika vienoje valstybėje bus laikoma nusikalstama, o kitoje valstybėje – ne. Elektroninių nusikaltimų sąvokų įvairovė taip pat gali neigiamai veikti šių nusikaltimų plitimą. Tai, kad vienoje valstybėje atitinkama nusikalstama veika yra laikoma elektroniniu nusikaltimu, o kitoje – ne, gali paskatinti nusikalstamas veikas daryti toje valstybėje, kurioje atitinkama veika nėra laikoma elektroniniu nusikaltimu. Galima daryti prielaidą, kad atsižvelgiant į pastaruoju metu neretai pasitaikantį tarptautinį elektroninių nusikaltimų pobūdį, vienodos elektroninio nusikaltimo sampratos įtvirtinimas galėtų užtikrinti efektyvesnę kovą su tokiomis nusikalstamomis veikomis.

Žinoma, iš kitos pusės pasaulinėje praktikoje yra pripažinta, kad apibrėžti elektroninį nusikaltimą yra ypač sudėtinga. Tai paprastai sąlygoja ypač didelė naujų technologijų įvairovė ir dinamika, ko pasekoje gali tekti nuolat keisti/pildyti elektroninio nusikaltimo sąvoką. Tačiau vis gi manytume, kad baudžiamosios teisės doktrinoje, atlikus gilią analizę, būtų galima pabandyti sumodeliuoti kuo tikslesnį „elektroninio nusikaltimo“ apibrėžimą arba bent jau bendrai apsispręsti, kurios iš mokslininkų pateikiamų elektroninių nusikaltimų sampratos krypties reikėtų laikytis, apibrėžiant elektroninius nusikaltimus.

2. ELEKTRONINIŲ NUSIKALTIMŲ TEISINIS REGLAMENTAVIMAS LIETUVOS IR RUSIJOS NACIONALINĖJE TEISĖJE

2.1. Pagrindiniai tarptautiniai ir regioniniai teisės aktai dėl elektroninių nusikaltimų ir jų įgyvendinimas Lietuvoje ir Rusijoje

Elektroniniai nusikaltimai – tai reiškinys, kurio nepavyksta išvengti nei vienai moderniai pasaulio valstybei. Maža to, elektroniniai nusikaltimai vis dažniau vykdomi ne vienos valstybės teritorijoje – nusikaltėlis gali būti įsikūręs vienoje valstybėje, o jo vykdomi elektroniniai nusikaltimai gali būti nukreipti prieš aukas, esančias kitose valstybėse. Augantis interneto vartojimas suteikia vis daugiau galimybių nusikaltėliams, todėl bet kuriai valstybei vienai pačiai kovoti su elektroniniu nusikalstamu darosi vis sunkiau. Suvokdamos tai, įvairios tarptautinės organizacijos (pvz. Europos Taryba, Europos ekonominio bendradarbiavimo ir vystymo organizacija, Europos Komisija ir kt.) imasi reguliuoti elektroninių nusikaltimų sritį tarptautiniu ir regioniniu mastu. Vis tik reikia pažymėti, kad nemaža dalis šių organizacijų priimtų dokumentų yra neprivalomo, rekomendacinio pobūdžio.

Vienas pagrindinių tarptautinių norminio pobūdžio dokumentų elektroninių nusikaltimų srityje yra 2001 m. lapkričio 23 d. Europos Tarybos konvencija dėl elektroninių nusikaltimų[7] (toliau – Konvencija). Tai kompleksinis dokumentas, skirtas kovoti su nusikaltimais kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui, kompiuteriniu sukčiavimu, nusikaltimais, susijusiais su vaikų pornografija ir kitais panašaus pobūdžio nusikaltimais.

Galima teigti, jog šios Konvencijos normos yra skirtos reguliuoti tris pagrindines klausimų grupes:

1. Klausimus, susijusius su nacionalinių baudžiamųjų įstatymų unifikavimu, t.y. vienodų teisinės atsakomybės pagrindų už elektroninius nusikaltimus, nustatymu.

2. Klausimus, susijusius su nacionalinių baudžiamojo proceso normų, tiriant elektroninius nusikaltimus, suvienodinimu.

3. Klausimus, susijusius su ekstradicijos ir savitarpio pagalbos teikimo reglamentavimo suvienodinimu.

2011 m. balandžio mėn. Konvenciją buvo pasirašiusios 47 valstybės, o ratifikavusios - 33 valstybės[8]. Kadangi iš viso yra 195 valstybės, Konvencija labai minimaliai įtakoja globalią kovą su

[7] Lietuvos Respublikos įstatymas dėl konvencijos dėl elektroninių nusikaltimų ratifikavimo. Valstybės žinios, 2004, Nr. 36- 1178.

[8] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [2012-04-15]

elektroniniais nusikaltimais[9]. Todėl Konvencija gali būti svarbus, bet ne vienintelis teisinis dokumentas kovojant su elektroniniais nusikaltimais[10].

Lietuva yra Konvencijos narė – ji šią konvenciją pasirašė 2003 m. birželio 23, o ratifikavo – 2004 m. kovo 18 d. Prisijungdama prie Konvencijos Lietuva privalėjo ir atitinkamai su Konvencijos nuostatomis suderinti savo baudžiamuosius įstatymus. Siekdama įgyvendinti Konvencijos 2-13 straipsnių nuostatas Lietuva pakeitė ir papildė atskirus Lietuvos Respublikos baudžiamojo kodekso straipsnius, o siekdama įgyvendinti Konvencijos 14 straipsnį – papildė Lietuvos Respublikos baudžiamojo kodekso 154 str. (kartu su Lietuvos Respublikos įstatymu „Dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo" projektu buvo pateiktas ir Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 str. pakeitimo ir papildymo bei Kodekso papildymo 198^1 ir 198^2 str. įstatymo ir Lietuvos Respublikos baudžiamojo proceso kodekso 154 str. papildymo įstatymo projektai). Be to, Lietuva, ratifikuodama Konvenciją, pasinaudojo šiame dokumente numatyta išlygų ir pareiškimų galimybe, „tokiu būdu išsprendžiant tarp Lietuvos Respublikos įstatymų bei Konvencijos nuostatų egzistuojančius neatitikimus"[11]. Reikia pažymėti, kad šiuo atžvilgiu Lietuva yra viena iš nedaugelio Konvenciją pasirašiusių ir/ar ratifikavusių valstybių (viena iš vienuolikos valstybių) pareiškusių tiek išlygas, tiek ir pareiškimus.

2004 m. sausio 22 d. Lietuvos Respublikos įstatymo Nr. IX-1974 „Dėl konvencijos dėl elektroninių nusikaltimų ratifikavimo"[12] 2 straipsnyje nurodoma, kad Lietuva taiko 2 išlygas:

1. Už Konvencijos 4 straipsnyje nurodytų veikų (sąmoningą ir neteisėtą kompiuterinių duomenų sugadinimą, sunaikinimą, apgadinimą, pakeitimą ar galimybės naudotis tokiais duomenimis panaikinimą) padarymą baudžiamoji atsakomybė atsiranda padarius didelę žalą.

2. Lietuvos Respublika pasilieka teisę atsisakyti vykdyti prašymą išsaugoti duomenis, jeigu yra pagrindas manyti, kad atskleidimo metu pažeidimas, kurio pagrindu prašoma išsaugoti duomenis, nebus laikomas nusikaltimu pagal Lietuvos Respublikos įstatymus.

Minėto įstatymo 3 straipsnyje taip pat įtvirtinami 5 pareiškimai:

1. Už Konvencijos 2 straipsnyje nurodytos veikos (už sąmoningą ir neteisėtą prieigą prie visos kompiuterinės sistemos arba jos dalies) padarymą baudžiamoji atsakomybė atsiranda neteisėtai prisijungus prie visos ar dalies kompiuterinės sistemos, pažeidžiant kompiuterio ar kompiuterinio tinklo apsaugos priemones.

---

[9] Brenner. S. W. Cybercrime. Criminal Threats from Cyberspace. Library of Congress Cataloging, 2010, p. 209.
[10] Štitilis D. Elektroniniai nusikaltimai. Metodinė priemonė. Mykolo Riomerio universitetas. Vilnius, 201,p.. 347.
[11] Aiškinamasis raštas „Dėl Lietuvos Respublikos įstatymo „Dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo", Lietuvos Respublikos baudžiamojo kodekso (Žin., 2000, 89-2741) 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 str. pakeitimo ir papildymo bei Kodekso papildymo 198^1 ir 198^2 str. įstatymo ir Lietuvos Respublikos baudžiamojo proceso kodekso (Žin., 2002, 37-1341) 154 str. papildymo įstatymo projektų. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=223058 [2012-01-22]
[12] Lietuvos Respublikos įstatymas dėl konvencijos dėl elektroninių nusikaltimų ratifikavimo. Valstybės žinios, 2004, Nr. 36- 1178.

2. Teisingumo ministerija ir Generalinė prokuratūra skiriamos atsakingomis institucijomis Konvencijos 24 straipsnio 7 dalies a punkte nurodytoms funkcijoms atlikti (t.y. institucijomis, atsakingomis už prašymo išduoti arba laikinai suimti asmenį pateikimą arba gavimą).

3. Teisingumo ministerija ir Generalinė prokuratūra skiriamos centrinėmis įstaigomis Konvencijos 27 straipsnyje nurodytoms funkcijoms atlikti (t.y. institucijomis, atsakingomis už savitarpio pagalbos prašymų ir atsakymų į juos siuntimą, tokių prašymų vykdymą arba jų perdavimą vykdyti kompetentingoms institucijoms).

4. Policijos departamentas prie Vidaus reikalų ministerijos skiriamas kompetentinga įstaiga Konvencijos 35 straipsnyje nurodytoms funkcijoms atlikti (t.y. skiriamas ryšio punktu, veikiančiu visą parą 7 dienas per savaitę, kuris teikia skubią pagalbą tyrimui ar bylų nagrinėjimui, susijusiems su nusikaltimais kompiuterinėms sistemoms ir duomenims, arba nusikaltimo įrodymų rinkimui elektroniniu pavidalu).

5. Skubiu atveju savitarpio pagalbos ar su ja susijusios informacijos prašymai turi būti siunčiami centrinei įstaigai, t.y. Teisingumo ministerijai ir Generalinei prokuratūrai.

Pažymėtina, kad Rusijos Federacija, skirtingai nei Lietuva, nėra nei pasirašiusi, nei ratifikavusi Konvencijos, taigi atitinkamai Rusijos Federacija nėra įsipareigojusi suderinti savo baudžiamųjų įstatymų nuostatų su atitinkamomis Konvencijos nuostatomis. Nors jau 2005 m. Rusijoje buvo priimtas sprendimas pasirašyti Konvenciją – 2005 m. lapkričio 15 d. Rusijos Federacijos prezidentas buvo pasirašęs įsaką Nr. 557-rp “Dėl konvencijos dėl elektroninių nusikaltimų pasirašymo”[13], kuriuo pavedė Rusijos užsienio reikalų ministerijai pasirašyti Konvenciją su tam tikrais pareiškimais. Tačiau 2008 m. Rusija atsisakė savo ketinimo pasirašyti Konvenciją – 2008 m. kovo 22 d. buvo priimtas Rusijos Federacijos Prezidento įsakas Nr. 144-rp "Dėl pripažinimo netekusiu galios Rusijos Federacijos prezidento 2005 lapkričio 15 d. įsaku Nr. 557-rp “Dėl konvencijos dėl elektroninių nusikaltimų pasirašymo”[14].

Т. А. Полякова nurodo, jog ekspertų nuomone visa eilė Konvencijos nuostatų prieštarauja kai kurioms Rusijos įstatymų normoms. Visų pirma, kai kurie Konvencijos straipsniai numato suteikti tarpvalstybinę prieigą prie kompiuterinių duomenų, kas gali padaryti žalą valstybės informaciniam saugumui[15].

Y. B. Зинина detalizuoja šią nuostatą, nurodydama, kad Rusijos teisėsaugos institucijos mano, kad pagal Konvencijos 23 straipsnio b punktą tam tikromis aplinkybėmis vienos Konvencijos

[13] Распоряжение Президента РФ от 15 ноября 2005 г. N 557-рп "О подписании Конвенции о киберпреступности". http://www.lawrussia.ru/texts/legal_712/doc712a781x217.htm [2012-01-22]

[14] Распоряжение Президента РФ от 22 марта 2008 г. N 144-рп "О признании утратившим силу распоряжения Президента РФ от 15 ноября 2005 г. N 557-рп "О подписании Конвенции о киберпреступности". http://news-city.info/akty/lawbook-36/tekst-ey-civil-moskwa.htm [2012-01-22]

[15] Полякова Т. А. Проблемы совершенствования правового регулирования противодействия использованию информационных технологий в преступных целях. Доклад на VII Международной конференции “Право и Интернет”. http://www.ifap.ru/pi/07/ [2012-01-22]

narės teisėsaugos institucijos gali vykdyti operatyvinį darbą kitos valstybės – Konvencijos narės teritorijoje be jos sutikimo, kas traktuojama kaip grėsmė valstybės saugumui ir kišimasis į šalies vidaus reikalus. Atsižvelgiant į šią aplinkybę, taip pat į tai, kad iki Rusijos sprendimo pasirašyti ir ratifikuoti Konvenciją nei viena iš didžiojo aštuoneto valstybių nebuvo ratifikavusi Konvencijos (2006 m. sausio mėn. Konvenciją ratifikavo Prancūzija, o po to 2006 m. spalio mėn. ją ratifikavo JAV), buvo nuspręsta kol kas apsiriboti Konvencijos pasirašymu, o dėl jos ratifikavimo spręsti vėliau[16]. Tačiau kaip jau minėjome savo darbe anksčiau 2008 metais Rusijos Federacija iš viso atsisakė savo ketinimo pasirašyti Konvenciją.

Tačiau yra ir nemaža dalis Rusijos mokslininkų, pasisakančių už tai, kad Rusija turėtų prisijungti prie Konvencijos.

И. М. Рассолов nuomone, kuo greitesnis Rusijos prisijungimas prie Konvencijos išspręstų daugelį problemų Rusijos baudžiamosios teisės srityje, įtakotų konceptualių valstybės ir teisės teorijos normų sukūrimą[17].

Y. B. Зинина taip pat mano, kad atsižvelgiant į tai, kad tarptautinis bendradarbiavimas neįmanomas kol nėra tarpusavyje sutartų baudžiamosios teisės normų kompiuterinių nusikaltimų srityje, o taip pat kol nėra sukurtos universalios sutartos teisėsaugos institucijų tarpusavio bendradarbiavimo procedūros tiriant tokius nusikaltimus, yra būtinas kuo skubesnis Rusijos prisijungimas prie konvencijos dėl elektroninių nusikaltimų[18].

Taigi, atsižvelgiant į tai, kad Rusijos mokslininkų tarpe vis dažniau pripažįstama Konvencijos kaip ypač svarbaus tarptautinio mechanizmo reikšmė suvienodinant valstybių įstatymus elektroninių nusikaltimų srityje ir į tai, kad Rusijos Federacijoje jau buvo padaryti pirmieji žingsniai siekiant prisijungti prie Konvencijos, tikėtina, kad Rusijos Federacija vis tik anksčiau ar vėliau prisijungs prie Konvencijos. Aišku, toks Rusijos Federacijos prisijungimas prie Konvencijos matyt neišvengiamai pareikalaus, kaip ir Lietuvos atveju, pareikšti išlygas ir/ar pareiškimus dėl tam tikrų Konvencijos straipsnių ir/ ar padaryti pakeitimus Rusijos baudžiamuosiuose įstatymuose.

2003 m. sausio 28 d. Strasbūre buvo pasirašytas Konvencijos dėl elektroninių nusikaltimų Papildomas protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo. Šio protokolo tikslas – protokolo šalims papildyti 2001 m. lapkričio 23 d. Budapešte pateiktos pasirašyti Konvencijos dėl elektroninių nusikaltimų

[16] Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Автореферат. Москва , 2007. http://www.russianlaw.net/files/law/doc/a212.pdf [2012-01-22]
[17] Рассолов И.М. Право и Интернет. http://tawkataw.ucoz.ru/_ld/1/105_pravo_i_interne.pdf [2012-01-22]
[18] Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Автореферат. Москва , 2007. http://www.russianlaw.net/files/law/doc/a212.pdf [2012-01-22]

nuostatas dėl rasistinio ir ksenofobinio pobūdžio veikos, padarytos naudojantis kompiuterinėmis sistemomis, kriminalizavimo[19].

Deja, prie šio protokolo yra prisijungę dar mažiau valstybių negu prie Konvencijos - 2012 m. balandžio mėn. buvo pasirašiusios 35 valstybės, o ratifikavusios tik 20 valstybių[20].

Lietuva Konvencijos Papildomą protokolą dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo ratifikavo 2006 m. birželio 8 d. su pareiškimu. Lietuvos Respublikos įstatyme dėl konvencijos dėl elektroninių nusikaltimų papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo ratifikavimo[21] 2 straipsnyje nustatyta, kad baudžiamoji atsakomybė už Papildomo protokolo 6 straipsnio 1 dalyje nurodytą neigimą arba šiurkštų menkinimą atsiranda, jei tai padaryta ketinant kurstyti neapykantą, diskriminavimą arba smurtą, nukreiptą prieš asmenį arba asmenų grupę dėl rasės, odos spalvos, kilmės arba tautinės ar etninės kilmės, taip pat religijos, jeigu ji naudojama kaip pretekstas kuriam nors iš šių veiksnių.

Kadangi Rusijos Federacija nėra prisijungusi prie Konvencijos, tai, žinoma, ji taip pat nėra prisijungusi ir prie šios konvencijos papildomo protokolo.

Pastaruoju laikotarpiu Europos Sąjungos institucijos taip pat skiria nemažai dėmesio elektroninių nusikaltimų reglamentavimo klausimui. Europos Komisija yra priėmusi ne vieną dokumentą šioje srityje, tačiau iš esmės visi jie yra rekomendacinio pobūdžio:

- 2001 m. sausio 26 d. Komisijos komunikatas Tarybai, Europos Parlamentui, ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Saugesnės informacinės visuomenės kūrimas, gerinant informacinių infrastruktūrų saugą ir kovą su nusikaltimais, susijusiais su kompiuteriais[22]“;

- 2007 m. gegužės 22 d. Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme[23];

- 2009 m. kovo 30 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės

[19] Konvencijos dėl elektroninių nusikaltimų Papildomas protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo. Valstybės žinios, 2006, Nr. 75-2850

[20] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG [2012-04-15]

[21] Lietuvos Respublikos įstatymas dėl konvencijos dėl elektroninių nusikaltimų Papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo ratifikavimo. Valstybės žinios, 2006, Nr. 75- 2848.

[22] 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=COM:2000:0890:FIN:EN:PDF [2012-01-28]

[23] Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui - Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme {SEK(2007) 641} {SEK(2007) 642}
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:LT:NOT [2012-01-28]

infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“[24];

- 2011 m. kovo 31 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“[25].

Apibendrinant galima teigti, kad šie priimti Komunikatai atspindi Europos Komisijos susirūpinimą dėl įvykdomų vis sudėtingesnių elektroninių nusikaltimų, neretai apimančių ne vieną valstybę ir pastovaus jų skaičiaus didėjimo. Be to, juose atspindima Europos Komisijos pozicija, kad skubiai būtina imtis įvairiausių priemonių (materialinės teisės, proceso teisės, bendradarbiavimo gerinimo, statistinių duomenų vystymo ir t. t.) tiek nacionaliniu lygmeniu, tiek ir Europos Sąjungos lygmeniu prieš įvairias elektroninių nusikaltimų formas. Iš vienos pusės tokio pobūdžio komunikatai skatina Europos Sąjungos valstybes kurti vienodas elektroninių nusikaltimų reglamentavimo ir kovos su šiais nusikaltimais sąlygas. Tačiau iš kitos pusės neprivalomas tokių dokumentų pobūdis palieka didelę laisvę Europos Sąjungos valstybėms elgtis savo nuožiūra. Bet kuriuo atveju nors komunikatai ir neįpareigoja Lietuvos įtvirtinti atitinkamų reikalavimų nacionaliniuose teisės aktuose, tačiau jie nurodo gaires kaip būtų tikslinga elgtis.

2005 m. vasario 24 d. buvo priimtas Tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas[26]. Šio pamatinio sprendimo tikslas yra pagerinti valstybių narių teisminių ir kitų kompetentingų institucijų, įskaitant policijos ir kitas specializuotas teisėsaugos tarnybas, bendradarbiavimą derinant valstybėse narėse baudžiamosios teisės taisykles atakų prieš informacines sistemas srityje. Pamatiniai sprendimai valstybėms narėms privalomi siektinų rezultatų atžvilgiu, bet nacionalinėms valdžios institucijoms paliekama galimybė pasirinkti jų įgyvendinimo formą ir būdus.

2008 m. Komisija pateikė ataskaitą Tarybai parengtą pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas 12 straipsnį[27]. Išnagrinėjus šią ataskaitą,

---

[24] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ {SEC(2009) 399} {SEC(2009) 400} KOM(2009) 149 galutinis http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:HTML [2012-01-28]

[25] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“. KOM (2011) 163 galutinis. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:LT:HTML [2012-01-28]

[26] Tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:LT:HTML [2012-01-28]

[27] Komisijos ataskaita Tarybai parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas 12 straipsnį. KOM (2008) 0448 galutinis http://eur-law.eu/LT/Komisijos-ataskaita-Tarybai-parengta-2005-m-vasario-24,480987,d [2012-01-28]

galima daryti išvadą, kad Lietuva yra viena iš tų Europos Sąjungos valstybių, kurios pakankamai gerai įgyvendino minėtą sprendimą ir su atitinkamomis sprendimo nuostatomis suderino savo nacionalinius teisės aktus.

Tuo tarpu Rusijos Federacija nėra Europos Sąjungos narė, todėl ji nėra saistoma ir Europos Sąjungos institucijų priimtų dokumentų.

Atlikus pagrindinių tarptautinių ir regioninių dokumentų įgyvendinimo Lietuvoje ir Rusijos Federacijoje analizę, galima daryti išvadą, kad atsižvelgiant į tai, kad Lietuva yra prisijungusi prie pagrindinės tarptautinės konvencijos dėl elektroninių nusikaltimų ir jos papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo ir atitinkamai su šių dokumentų nuostatomis suderinusi savo baudžiamuosius įstatymus, taip pat į tai, kad Lietuva yra Europos Sąjungos narė ir privalo (arba jai rekomenduojama) įgyvendinti aukščiau darbe minėtus Europos Sąjungos institucijų dokumentus elektroninių nusikaltimų reglamentavimo srityje, elektroninių nusikaltimų reglamentavimui Lietuvoje įtaką daro tiek tarptautinis, tiek regioninis teisinis reglamentavimas. Tuo tarpu Rusijos Federacija nėra prisijungusi prie Konvencijos ir jos protokolo, ji taip pat nėra Europos Sąjungos narė, todėl elektroninių nusikaltimų reglamentavimui šioje valstybėje jokios minėtos tarptautinės ir regioninės iniciatyvos įtakos nedaro.

2.2. Lietuvos ir Rusijos teisinė bazė dėl elektroninių nusikaltimų

Nuolat tobulėjant kompiuterinėms technologijoms ir augant interneto vartojimui, elektroninės erdvės apsaugojimas teisinėmis priemonėmis tampa svarbiu procesu kiekvienoje valstybėje. Neužtikrinus veiksmingo elektroninės informacijos saugos reguliavimo, sudaromos prielaidos elektroninių nusikaltimų vykdymui. Elektroninių nusikaltimų sritis gali būti reguliuojama reglamentuojant elektroninės informacijos saugos santykius[28]. Pastaruoju metu visos pasaulio valstybės vis daugiau dėmesio skiria elektroninės informacijos saugai, ne išimtis ir Lietuvos Respublika, ir Rusijos Federacija. Šioje dalyje aptarsime pamatinį teisinį visuomeninių santykių elektroninės informacijos saugos srityje reguliavimą (strateginius dokumentus ir pagrindinius įstatymus), nes būtent nuo jo priklauso visos detalesnės teisinės bazės kūrimas. Atsižvelgiant į šio darbo tikslą, atitinkamus teisės aktus nagrinėsime lyginamuoju aspektu.

Elektroninės informacijos saugos strategija yra vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų[29]. Lietuvoje pirmoji elektroninės informacijos saugos

[28] Štitilis D. Elektroniniai nusikaltimai: metodinė priemonė. Vilnius: Mykolo Romerio universitetas, 201, p. 83.

[29] Štitilis D.; Paškauskas, Ž. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. Jurisprudencija, 2007, 2 (92).

valstybės institucijų informacinėse sistemose valstybinė strategija buvo patvirtinta tik 2006 m. ir galiojo iki 2008 m. Šiuo metu galiojanti elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa (toliau – Lietuvos programa) buvo patvirtinta 2011 m. birželio 29 d. Vyriausybės nutarimu Nr. 796[30]. Šioje Lietuvos programoje įvardijamos pagrindinės elektroninės informacijos saugos (kibernetinio saugumo) problemos, nustatomi elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslai ir uždaviniai.

Rusijoje strateginis dokumentas, kuris apibrėžia valstybės politiką elektroninės informacijos saugos srityje yra 2000 m. rugsėjo 9 d. Rusijos Prezidento patvirtinta Doktrina dėl informacijos saugumo Rusijos Federacijoje[31] (toliau – Rusijos doktrina). Šioje Rusijos doktrinoje, taip pat kaip ir Lietuvos programoje, įvardijamos pagrindinės informacijos saugos problemos, nustatomi informacijos saugos tikslai, uždaviniai, principai ir pagrindinės kryptys užtikrinant informacijos saugą Rusijos Federacijoje. Tačiau skirtingai negu Lietuvos programoje, Rusijos doktrinoje žymiai daugiau dėmesio skiriama informacinės saugos būklės aprašymui, galimų grėsmių ir šių grėsmių šaltinių įvardijimui, joje taip pat įvardijamos informacinės saugos užtikrinimo įvairiose visuomeninio gyvenimo srityse ypatybės (pvz. ekonomikos, vidaus ir išorės politikos, mokslo ir technikos ir kt.). Mūsų nuomone, Lietuvos programoje taip pat galėtų būti padaryta gilesnė esamos būklės analizė, įvardintos galimos grėsmės, dėl kokių priežasčių atitinkami uždaviniai gali būti nepasiekti, nes tai galėtų padėti lengviau planuoti žingsnius, būtinus, kad nustatyti tikslai ir uždaviniai būtų pasiekti.

Lietuvos programos 2 punkte nustatytas pakankamai konkretus ir ambicingas strateginis tikslas, kuris turėtų būti pasiektas iki 2019 m.– plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų.

Apibendrinant Lietuvos programos 6-10 punkte išdėstytas nuostatas galime teigti, kad joje nustatyti šie pagrindiniai siektini tikslai ir uždaviniai:

- Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas. Šiam tikslui pasiekti numatyti tokie uždaviniai: tobulinti elektroninės informacijos saugos (kibernetinio saugumo) koordinavimą ir priežiūrą; tobulinti elektroninės informacijos

[30] Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 "Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo". Valstybės žinios, 2011, Nr. 83-4033; 2011, Nr.106 (atitaisymas).
[31] Доктрина информационной безопасности Российской Федерации http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm [2012-02-18]

saugos (kibernetinio saugumo) teisinį reglamentavimą; plėsti ir tobulinti saugią valstybės informacinę infrastruktūrą; skatinti elektroninės informacijos saugos (kibernetinio saugumo) projektų įgyvendinimą; plėtoti tarptautinį bendradarbiavimą elektroninės informacijos saugos (kibernetinio saugumo) srityje.

- Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą. Šiam tikslui pasiekti numatytas uždavinys - užtikrinti ypatingos svarbos informacinės infrastruktūros saugumą.
- Siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje. Šiam tikslui pasiekti numatyti tokie uždaviniai: kelti elektroninės informacijos saugos (kibernetinio saugumo) kultūrą; stiprinti Lietuvos kibernetinės erdvės saugumą; užtikrinti virtualaus Lietuvos kibernetinės erdvės perimetro apsaugą nuo išorinių kibernetinių atakų; stiprinti kibernetinėje erdvėje teikiamų paslaugų saugumą.

Lietuvos programos priede šalia siektinų tikslų ir uždavinių nustatyti ir programos įgyvendinimo vertinimo kriterijai ir siekiamos jų reikšmės 2011, 2015 ir 2019 metais bei už šių kriterijų įgyvendinimą atsakingos institucijos. Reikia pastebėti, kad nustatytos konkrečios ir ambicingos vertinimo kriterijų reikšmės, tik nežinia, kiek realiai įgyvendinamos, nes daugelis indikatorių iki Lietuvos programos priėmimo iš viso nebuvo vertinami, pvz. numatyta, kad iki 2015 m. saugią valstybės infrastruktūrą naudojančių informacinių išteklių dalis pasieks 70 proc., o 2019 m. – 100 proc., nors nėra žinoma, koks šis rodiklis buvo 2011 m. Mūsų nuomone, atsižvelgiant į tai, kad daugelio vertinimo kriterijų reikšmės nėra žinomos, Lietuvos programoje reikėjo nustatyti, kad pirmasis įvertinimas būtų atliktas daug anksčiau negu 2015 m., siekiant nustatyti pirmines atitinkamų rodiklių reikšmes (t.y. įvertinti esamą situaciją), o tuomet jau nuosekliai būtų galima nustatyti ir reikšmes, kurias reikėtų pasiekti tolimesniais metais.

Be to, mūsų nuomone, kai kuriuos indikatorius iš viso gali būti sunku tiksliai įvertinti, pvz. nustatyta, kad saugiai besijaučiančių kibernetinėje erdvėje Lietuvos gyventojų dalis 2015 m. turėtų siekti 40 proc., o 2019 m. – jau 60 procentų, nors nežinia kaip tą saugumo pojūtį reikės įvertinti. Nors Lietuvos programoje daug dėmesio skiriama visuomenės švietimui elektroninės informacijos srityje, tačiau, mūsų nuomone, trūksta konkretesnių priemonių, skirtų kovai su tam tikromis problemomis, pvz. piratinės programavimo įrangos naudojimui, kuri yra tikrai aktuali. „Microsoft" korporacijos užsakymu atliktos pasaulinės apklausos duomenimis, trys ketvirtadaliai kompiuterių vartotojų sutinka, kad naudotis nelegalia programine įranga yra nesaugu. Bendrovės „Synopticom" Lietuvoje atlikto interneto vartotojų tyrimo duomenimis Lietuvoje daugiau nei pusė vartotojų naudojasi nelegalia programine įranga.

Rusijos doktrinoje yra pateikiamos iš esmės 2 nacionalinių interesų (tikslų) grupės informacijos saugos srityje. Išanalizavus Rusijos doktrinos 1 straipsnį galima daryti prielaidą, kad pirmoji interesų (tikslų) grupė yra išskiriama pagal tai, kam šie interesai priklauso:

- asmeniui – realizuoti konstitucinę teisę į informacijos prieinamumą, apsaugoti asmeninę informaciją, turėti galimybę naudoti įstatymo nedraudžiamu būdu informaciją fiziniam, dvasiniam ir intelektualiniam vystymuisi ir kt.;
- visuomenei – užtikrinti asmens interesus informacijos saugos srityje, sukurti teisinę-socialinę valstybę, pasiekti ir išlaikyti bendrą sutarimą ir kt.
- valstybei – sudaryti sąlygas harmoningam Rusijos informacijos infrastruktūros vystymuisi, parengti reikalingus įstatymus ir tvarkas, vystyti tarptautinį bendradarbiavimą ir kt.

Analizuojant į antrąją grupę įtrauktų interesų turinį, galima daryti prielaidą, kad ši grupė yra išskirta pagal interesų svarbą:

- Gerbti žmogaus konstitucines teises ir laisves informacijos gavimo ir naudojimo srityje.
- Užtikrinti valstybės vidaus politikos saugą, kad Rusijos ir tarptautinei visuomenei būtų pateikiama patikima informacija apie Rusijos Federacijos vykdomą vidaus ir išorės politiką.
- Skatinti šiuolaikinių informacinių technologijų bei Rusijos Federacijos pramonės informavimo priemonių telekomunikacijų ir ryšių srityje vystymąsi, kad ši pramonė galėtų patenkinti poreikius tiek vidaus, tiek išorės rinkose.
- Apsaugoti informacinius išteklius nuo neteisėtos prieigos, užtikrinti informacijos perdavimo infrastruktūros saugą.

Rusijos doktrinos 9 straipsnyje išskiriamos tokios prioritetinės priemonės informacijos saugos srityje:

- sukurti ir įgyvendinti mechanizmus, padėsiančius įgyvendinti teisės normas, reguliuojančias santykius informacijos srityje, o taip pat parengti teisinio informacijos apsaugos užtikrinimo koncepciją;
- sukurti ir įgyvendinti mechanizmus, padėsiančius padidinti valdžios vadovavimo efektyvumą valstybinių masinės informacijos priemonių darbui, įgyvendinti valstybinę informacinę politiką;
- priimti ir įgyvendinti federalines programas, kuriose būtų numatyta formuoti visiems prieinamus valstybinės valdžios įstaigų/organizacijų informacinius archyvus, didinti teisinę kultūrą ir piliečių kompiuterinį raštingumą, tobulinti Rusijos Federacijos

vieningą informacinę erdvę, imtis kompleksinių veiksmų prieš informacinių karų grėsmes ir pan.,

- tobulinti personalo, dirbančio Rusijos Federacijos informacijos saugos srityje, rengimo sistemą,
- tobulinti valstybės standartus informatizavimo ir informacinės saugos srityje ir pan.

Mūsų nuomone, Rusijos doktrinoje nurodytų tikslų ir prioritetinių priemonių formuluotės yra ganėtinai deklaratyvios ir nekonkrečios, taip pat skirtingai negu Lietuvos programoje nenustatyta jokių vertinimo kriterijų, pagal kuriuos galima būtų spręsti, ar ši Rusijos doktrina yra sėkmingai įgyvendinama. Е. К. Волчинская analizuodama valstybės vaidmenį užtikrinant informacijos apsaugą nurodo, kad jos nuomone, dauguma Rusijos doktrinoje nurodytų priemonių yra neįgyvendinama, pvz. nesukurta valstybės politika šioje srityje, neparengta tikslinė federalinė programa[32].

Rusijos doktrinoje, skirtingai negu Lietuvos programoje, dar papildomai yra įtvirtinti ir valstybinės informacijos apsaugos metodai. Jie suskirstyti į teisinius, organizacinius – techninius ir ekonominius. Prie teisinių informacijos saugumo užtikrinimo metodų priskiriamas norminių teisės aktų, kurie reglamentuotų informacinius santykius, ir norminių metodinių dokumentų dėl informacijos saugumo užtikrinimo Rusijos Federacijoje kūrimas. Organizaciniams – techniniams metodams dėl informacijos saugumo užtikrinimo priskiriami: teisėsaugos organų sustiprinimas; informacijos apsaugos priemonių sukūrimas ir panaudojimas, jų efektyvumo kontrolė; apsaugotų telekomunikacinių sistemų vystymas, specialios programinės įrangos patikimumo didinimas; priemonių ir sistemų, galėsiančių apsaugoti informaciją nuo neteisėto – nesankcionuoto prisijungimo ir pakenkimo, sunaikinimo ar pakeitimo, kūrimas ir pan. Ekonominiams informacijos saugumo užtikrinimo metodams priskiriami: informacijos saugumo užtikrinimo programų kūrimas ir jų finansavimo tvarkos nustatymas; darbų, susijusių su teisinių ir organizacinių–techninių informacijos apsaugos metodų įgyvendinimu, finansavimo sistemos sukūrimas; fizinių ir juridinių asmenų informacinės rizikos draudimo sistemos sukūrimas ir pan. Mūsų nuomone, toks valstybinės informacijos apsaugos metodų įtvirtinimas strateginiame dokumente yra perteklinis ir nereikalingas, nes svarbiausi būtini atlikti veiksmai tokio pobūdžio strateginiuose dokumentuose turėtų būti nustatomi priemonių dalyje.

Pažymėtina, kad Lietuvos programoje neišskiriama konkrečių institucijų kompetencija elektroninės informacijos saugos srityje, tiktai nurodoma, kurios Lietuvos institucijos ir už kokių konkrečiai programoje nustatytų tikslų ir uždavinių įgyvendinimą atsakingos. Už Lietuvos programos įgyvendinimo koordinavimą, Lietuvos programoje numatytų uždavinių ir jų vertinimo

[32] Волчинская Е. К. Роль государства в обеспечении информационной безопасности. rniiis.ru/articlesip409/volchinskaya.doc [2012-02-18]

kriterijų reikšmių pokyčių peržiūrą ir programos atnaujinimą atsakinga Vidaus reikalų ministerija. Už Lietuvos programos tikslų ir uždavinių įgyvendinimą atsako institucijos ir įstaigos – Ministro Pirmininko Tarnyba, Ryšių reguliavimo tarnyba, Valstybės duomenų apsaugos inspekcija, Policijos departamentas prie VRM, Krašto apsaugos ministerija, Susisiekimo ministerija, Finansų ministerija, Švietimo ir mokslo ministerija bei Ūkio ministerija.

Tuo tarpu Rusijos doktrinoje yra ganėtinai aiškiai atskirta įstatymų leidžiamosios, vykdomosios ir teisminės valdžios kompetencija informacijos saugos srityje. Detalizuojama, kokias funkcijas šioje srityje atlieka Rusijos Federacijos prezidentas, Rusijos Federacijos dūma, Vyriausybė, Rusijos Federacijos saugumo Taryba, Rusijos Federacijos prezidento ir vyriausybės paskirti vykdomųjų institucijų subjektai, tarpinstitucinės ir valstybinės komisijos savivaldos institucijos, teismai ir kt.

Mūsų nuomone, siekiant formuoti ir įgyvendinti veiksmingą politiką elektroninės informacijos saugos srityje, Lietuvos programoje taip pat turėtų būti nurodyta ne tik kokia institucija yra atsakinga už konkrečios priemonės įgyvendinimą, bet taip pat aiškiai atskirtos kiekvienos institucijos funkcijos šioje srityje.

Atkreiptinas dėmesys, kad Lietuvoje elektroninės informacijos saugos santykiai tam tikra dalimi reguliuojami daugelyje įstatymų, Vyriausybės nutarimų, ministrų ar atitinkamos įstaigos vadovų pasirašytų įsakymų. Galima būtų paminėti keletą, mūsų nuomone, svarbesnių įstatymų, kuriuose fragmentiškai yra reglamentuoti šie santykiai: Lietuvos Respublikos elektroninių ryšių, Lietuvos Respublikos asmens duomenų teisinės apsaugos, Lietuvos Respublikos autorių teisių ir gretutinių teisių, Lietuvos Respublikos elektroninio parašo ir kt. įstatymuose. D.Štitilis ir kt. atkreipia dėmesį, kad „...galiojantys teisės aktai neužtikrina visapusiško ir nuoseklaus tinklų ir elektroninės informacijos saugumo visuomeninių santykių reglamentavimo, nesudaro sąlygų vartotojų pasitikėjimui informacine visuomene ir saugios informacinės visuomenės plėtrai“[33]. Manytume, kad šią problemą padėtų išspręsti pamatinio įstatymo, reglamentuojančio visuomeninius santykius, susijusius su elektroninės informacijos sauga, priėmimas. Deja, Lietuvoje iki šiol toks įstatymas nėra priimtas, nors jau 2006 m. gruodžio 6 d. Vyriausybės nutarimu Nr. 1211 buvo patvirtinta Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija[34] (toliau – Koncepcija).

Koncepcijos 2 punkte numatyta, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas reglamentuos santykius, susijusius su elektroninių ryšių tinklų ir informacijos saugumu, sudarys sąlygas saugios informacinės visuomenės plėtrai, didins vartotojų

[33] Štitilis D., Pakutinskas P., Dauparaitė I., Laurinaitis M. Teisinė aplinka siekiant išvengti tapatybės vagystės elektroninėje erdvėje: JAV ir Lietuvos teisės aktų lyginamoji analizė. Socialinės technologijos, 2011, 1 (1), p. 68.
[34] Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“. Valstybės žinios, 2006, Nr.134-5081.

pasitikėjimą informacine visuomene. 10 punkte detalizuota, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatyme bus numatyta:

1. aiški valstybės institucijų struktūra tinklų ir informacijos saugumo srityje, kad nebūtų dubliuojamos institucijų funkcijos ir atsakingos institucijos veiksmingai bendradarbiautų;

2. nustatyti bendrieji tinklų ir informacijos saugumo reikalavimai, daugiausia skirti vartotojams apsaugoti nuo tinklų ir informacijos saugumo incidentų;

3. valstybės ir savivaldybių institucijų tinklų ir informacinių sistemų, saugaus informacijos perdavimo tarp valstybės ir savivaldybių institucijų, kritinių informacinių infrastruktūrų tinklų ir informacijos saugumo reikalavimai;

4. aiški tinklų ir informacijos saugumo lygio įvertinimo sistema, reglamentuojanti tinklų ir informacijos saugumo audito atlikimą, techninės ir programinės įrangos saugumo įvertinimą. Ši sistema daugiausia bus taikoma valstybės ir savivaldybių institucijų tinklams ir informacinėms sistemoms, kritinėms informacinėms infrastruktūroms, didesnių įmonių, taip pat informacinės visuomenės paslaugų teikėjų tinklams ir informacinėms sistemoms – t.y. tais atvejais, kai tinklų ir informacijos saugumas daugiausia užtikrinamas laikantis atitinkamos saugumo politikos.

Reikėtų atkreipti dėmesį, kad Koncepcijos 21 punkte nurodoma, kad numatomu įstatymu nebus siekiama pakeisti Lietuvos Respublikos baudžiamajame kodekse įtvirtintos nusikaltimų informatikai sistemos. Jis sudarys galimybes ne tik reaguoti į jau įvykusius pažeidimus (nubausti asmenis), bet ir užtikrinti tokių pažeidimų prevenciją, užkirsti kelią neigiamiems jų padariniams. Taip pat aiškiai nustatys elgesio ribas – apibrėš veikas, kurios formaliai nėra kriminalizuotos (dėl to, kad Lietuvos Respublikos baudžiamasis kodeksas kai kurias veikas kriminalizuoja tik įtraukdamas papildomą požymį – padarytą didelę žalą), bet yra aiškiai pavojingos – kenksmingo programinio kodo kūrimas ir disponavimas juo; prisijungimas prie elektroninių ryšių tinklo ar informacinės sistemos, neturint tam teisės, ar sąlygų tam sudarymas; elektroninio pašto adreso rinkimas, platinimas, įsigijimas, naudojimas ar kitoks disponavimas elektroninio pašto adresu be naudotojo sutikimo tiesioginės rinkodaros tikslu ir panašiai, o už tokių veikų padarymą Lietuvos Respublikos administracinių teisės pažeidimų kodekse bus numatyta administracinė atsakomybė.

Jeigu Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas būtų priimtas jį būtų galima vadinti „holistinio elektroninės informacijos saugos teisinio reguliavimo apraiška“[35]. Deja, tenka konstatuoti, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo priėmimas ypač užsitęsė. Kaip jau minėjome aukščiau Koncepcija buvo patvirtinta jau 2006 m. gruodžio 6 d., taigi daugiau kaip prieš penkerius metus.

[35] Štitilis D. Elektroniniai nusikaltimai: metodinė priemonė. Vilnius: Mykolo Romerio universitetas, 2011. p. 83.

Lietuvos Respublikos Vyriausybės 2008–2012 metų programos įgyvendinimo priemonėse, patvirtintose Lietuvos Respublikos Vyriausybės 2009 m. vasario 25 d. nutarimu Nr. 189[36] buvo numatyta, kad Susisiekimo ministerija, Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba turi parengti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektą 2009 metų II ketvirtį. Tačiau nepavyko rasti informacijos, kad Lietuvos Respublikos Seime šiuo metu jau būtų užregistruotas tokio įstatymo projektas.

Analizuodami elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos, patvirtintos Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796[37], priedą matome, kad Vidaus reikalų ir Susisiekimo ministerijoms bei Ryšių reguliavimo tarnybai pavesta priimti esminius su elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu susijusius reikalavimus nustatančius specialius atitinkamą veiką ir teisinius santykius reglamentuojančius įstatymus (tarp jų Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas). Tačiau šios užduoties įvykdymas bus pirmą kartą vertinamas tik 2015 m, o vėliau 2019 metais, taigi, galima daryti prielaidą, jog tikėtina, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo priėmimas nusikels dar mažiausiai porą metų.

Vienas iš pagrindinių įstatymų Rusijos Federacijoje, reguliuojančių elektroninės informacijos saugos sritį, yra 2006 m. liepos 27 d. Rusijos Federacijos federalinis įstatymas Nr. 149-FZ „Dėl informacijos, informatizacijos ir informacijos apsaugos“[38]. Šis federalinis įstatymas reglamentuoja santykius, kylančius:

- įgyvendinant teisę į informacijos paiešką, gavimą, perdavimą, kūrimą ir skleidimą;
- taikant informacines technologijas;
- užtikrinant informacijos apsaugą.

Rusijos Federacijoje, taip pat kaip ir Lietuvoje, yra nemažai įstatymų, kuriuose galima rasti nuostatų, susijusių su elektroninės informacijos saugos klausimais: Rusijos Federacijos federalinis įstatymas „Dėl ryšių“, Rusijos Federacijos Federalinis įstatymas „Dėl masinės informacijos priemonių“, Rusijos Federacijos Civilinio kodekso IV dalis ir kt. Taip pat nuostatų, susijusių su šia sritimi, galima rasti ir Rusijos Federacijos prezidento įsakuose, Vyriausybės potvarkiuose, valstybiniuose ir tam tikros pramonės šakos standartuose ir kt.

[36] Lietuvos Respublikos Vyriausybės 2009 m. vasario 25 d. nutarimas Nr. 189 “Dėl Lietuvos Respublikos Vyriausybės 2008–2012 metų programos įgyvendinimo priemonių patvirtinimo”. Valstybės žinios, 2009, Nr. 33-1268.

[37] Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 “Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo”. Valstybės žinios, 2011, Nr. 83-4033; 2011, Nr.106 (atitaisymas).

[38] Федеральный закон „Об информации, информационных технологиях и о защите информации“. http://www.rg.ru/2006/07/29/informacia-dok.html [2012-02-18]

Išanalizavus pagrindinius Lietuvos ir Rusijos Federacijos teisės aktus, reglamentuojančius elektroninės informacijos saugą, galime daryti išvadą, kad šiuo metu Lietuvos Respublikoje ir Rusijos Federacijoje yra priimti strateginiai dokumentai, kurie apibrėžia planuojamą valstybės politiką elektroninės informacijos saugos srityje, tačiau Lietuvos programoje nustatyti pakankamai konkretūs ir ambicingi, kai kurie galbūt realiai netgi sunkiai įgyvendinami, tikslai, uždaviniai ir programos vertinimo kriterijai, tuo tarpu Rusijos doktrinoje nurodytų tikslų ir prioritetinių priemonių formuluotės yra ganėtinai deklaratyvios ir nekonkrečios, taip pat skirtingai negu Lietuvos programoje nenustatyta jokių vertinimo kriterijų, pagal kuriuos galima būtų spręsti, ar ši Rusijos doktrina yra sėkmingai įgyvendinama. Abiejose lyginamose valstybėse yra daug įstatymų ir poįstatyminių teisės aktų, kuriuose yra įtvirtintos pavienės nuostatos, reglamentuojančios elektroninės informacijos saugos santykius, tačiau Rusijos Federacijoje yra priimtas vienas pagrindinis įstatymas, reguliuojantis elektroninės informacijos saugos sritį, kai tuo tarpu Lietuvoje dar iki šiol nėra priimtas įstatymas, kuriuo visapusiškai ir nuosekliai būtų reglamentuoti visuomeniniai santykiai susiję su elektroninės informacijos sauga, nors koncepcija dėl šio įstatymo priėmimo buvo patvirtinta jau daugiau kaip prieš penkerius metus. Mūsų nuomone, siekiant užtikrinti visapusišką ir veiksmingą elektroninės informacijos saugą, būtina kiek įmanoma greičiau patvirtinti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymą, neatidėliojant jo priėmimo dar keletui metui kaip buvo daroma iki šiol.

3. ELEKTRONINIŲ NUSIKALTIMŲ KRIMINALIZAVIMAS LIETUVOS IR RUSIJOS BAUDŽIAMUOSIUOSE KODEKSUOSE

Paskutiniais dešimtmečiais stebima sparti informacinių technologijų sklaida ir ženkliai padidėjusi kompiuterinės informacijos vertė ir reikšmė socialiniame gyvenime, o kartu ir elektroninių nusikaltimų masto išaugimas. Tai sąlygojo būtinybę įstatymų leidėjui imtis priemonių, padedančių apsaugoti elektroninę erdvę. Vienas iš pagrindinių nacionalinių valstybių įstatymų leidėjų uždavinių kovojant su elektroniniais nusikaltimais – uždrausti šias pavojingas veikas nacionaliniuose baudžiamuosiuose kodeksuose[39].

Žinoma, kompiuterio/kompiuterinių sistemų pagalba galima atlikti nemažai nusikalstamų veikų, ir tokių, kai kompiuterinė informacija yra nusikaltimo dalykas, ir tokių, kai kompiuteris/kompiuterinė sistema yra naudojama kaip nusikaltimo padarymo priemonė. Atsižvelgiant į ribotą mūsų darbo apimtį, mes savo darbe nagrinėsime kaip elektroniniai nusikaltimai, suprantami siaurąja prasme, yra uždrausti Lietuvos ir Rusijos baudžiamuosiuose kodeksuose, t.y. nagrinėsime tik tas nusikalstamas veikas, kurios nurodytos atskiruose baudžiamųjų įstatymų skirsniuose ir kurių objektas yra bendras – visuomeniniai santykiai informacijos apdorojimo srityje.

2003 m. gegužės 1 d. įsigaliojus naujajam Lietuvos Respublikos baudžiamajam kodeksui (toliau – LR BK), buvo pertvarkyta Lietuvos Respublikos baudžiamosios teisės sistema. „Išskirtinis naujo BK bruožas, kad jis yra modernus kodeksas, parodantis baudžiamosios teisės raidos tendencijas, idėjas ir šios teisės srities mokslo laimėjimus“.[40] Šiame kodekse buvo išskirtas atskiras XXX skyrius „Nusikaltimai informatikai“, kuris 2007 m. buvo pervadintas į „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui”.

Kokias vertybes siekia apsaugoti įstatymų leidėjas galime nustatyti pasinaudodami būdu, kurį siūlo baudžiamosios teisės doktrina, nes būtent „baudžiamojo įstatymo saugomos vertybės yra Baudžiamojo kodekso specialiosios dalies normų suskirstymo i skyrius pagrindinis kriterijus“[41]. Taigi, pirmiausia atkreiptinas dėmesys į atitinkamo LR BK skyriaus pavadinimą - „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui”. Akivaizdu, kad šiuo skyriumi siekiama apsaugoti elektroninius duomenis ir informacines sistemas, taigi visomis šiame LR BK skyriuje nurodomomis nusikalstamomis veikomis kėsinamasi į bendrą objektą - visuomeninius santykius informacijos apdorojimo srityje.

[39] Štitilis D. Elektroniniai nusikaltimai. Metodinė priemonė. Vilnius: Mykolo Romerio universitetas, 2011, p. 84.
[40] Piesliakas V. Lietuvos baudžiamoji teisė. Pirmoji knyga. Vilnius: Justitia, 2006, p. 63.
[41] Piesliakas V. Lietuvos baudžiamoji teisė. Pirmoji knyga. Vilnius: Justitia, 2006, p. 180 .

LR BK XXX skyrių „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui"[42] sudaro 5 straipsniai, nustatantys baudžiamąją atsakomybę už šias nusikalstamas veikas:

- neteisėtą prieigą ir poveikį elektroniniams duomenims, sukėlusį didelę žalą (196 str.);
- neteisėtą poveikį informacinei sistemai, sukėlusį didelę žalą (197 str.);
- neteisėtą neviešų elektroninių duomenų perėmimą ir fiksavimą (198 str.);
- neteisėtą prisijungimą prie informacinės sistemos pažeidžiant informacinės sistemos apsaugos priemones (198^1 str.);
- neteisėtą disponavimą įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, tiesiogiai skirtais daryti nusikalstamas veikas (198^2 str.).

Baudžiamosios atsakomybės nustatymas už elektroninius nusikaltimus nėra išskirtinis Lietuvos Respublikos baudžiamosios teisės bruožas. Šias veikas kriminalizuojantis skyrius yra įtvirtintas ir Rusijos Federacijos baudžiamajame kodekse (toliau – RF BK). 1997 m. sausio 1 d. įsigaliojusiame Rusijos Federacijos baudžiamajame kodekse išskirtas specialus 28 skyrius „Nusikaltimai kompiuterinės informacijos srityje". Iš skyriaus pavadinimo galima daryti išvadą, kad šiame skyriuje išskirtos nusikalstamos veikos, kuriomis kėsinamasi į bendrą objektą - visuomeninius santykius kompiuterinės informacijos apdorojimo srityje.

RF BK 28 skyrių „Nusikaltimai kompiuterinės informacijos srityje" sudaro 3 straipsniai, kurie 2011 m. pabaigoje buvo iš esmės pakeisti ir išdėstyti naujomis redakcijomis, priėmus 2011 m. gruodžio 7 d. Rusijos Federalinį įstatymą Nr. 420-FZ „Dėl Rusijos Federacijos baudžiamojo kodekso ir atskirų Rusijos Federacijos teisės aktų pakeitimo“[43]. Šiuose 3 straipsniuose nustatyta baudžiamoji atsakomybė už šias nusikalstamas veikas:

- neteisėtą prieigą prie kompiuterinės informacijos (272 str.);
- kenkėjiškų programų sukūrimą, naudojimą ar platinimą (273 str.);
- kompiuterinės informacijos ir informacinės-telekomunikacijos tinklų saugojimo, perdirbimo ar perdavimo taisyklių pažeidimą (274 str.).

Nagrinėjamos temos kontekste minėtuose baudžiamojo kodekso skyriuose įtvirtintos nuostatos yra aktualios tuo aspektu, kad baudžiamųjų nuostatų analizė yra svarbi norint atskleisti bendrą elektroninių nusikaltimų reglamentavimo situaciją valstybėje, nes būtent tinkamas baudžiamasis reglamentavimas yra viena iš prielaidų, galinčių sumažinti elektroninių nusikaltimų skaičių. Siekiant atskleisti Lietuvoje ir Rusijoje naudojamos elektroninių nusikaltimų

[42] Lietuvos Respublikos baudžiamasis kodeksas. Valstybės žinios, 2000, Nr. 89-2741; 2004, Nr. 25-760; 2007, Nr. 81-3309.

[43] Федеральный закон Российской Федерации от 7 декабря 2011 года № 420-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации". http://www.rg.ru/2011/12/08/p-raboty-site-dok.html [2012-02-24]

reglamentavimo baudžiamuosiuose įstatymuose praktikos panašumus ir skirtumus bei tokiu būdu išryškinti galimas reglamentavimo spragas, Lietuvos Respublikos ir Rusijos Federacijos baudžiamųjų kodeksų nuostatas dėl elektroninių nusikaltimų nagrinėsime lyginamuoju aspektu. Šią lyginamąją analizę atliksime remdamiesi nusikalstamos veikos sudėties atskirų požymių turinio analize, daugiau dėmesio skirdami diskusijų keliančiam nusikalstamos veikos požymių turiniui.

3.1. Baudžiamoji atsakomybė už neteisėtą prieigą prie elektroninių duomenų ir poveikį jiems

Lietuvoje baudžiamoji atsakomybė už neteisėtą prieigą prie elektroninių duomenų ir poveikį šiems duomenims gali kilti pagal LR BK 196 str. „Neteisėtas poveikis elektroniniams duomenims".

LR BK 196 str. 1 d. numatyta baudžiamoji atsakomybė už neteisėtą elektroninių duomenų sunaikinimą, sugadinimą, pašalinimą, pakeitimą ar technine įranga, programine įranga ar kitais būdais naudojimosi tokiais duomenimis apribojimą, sukėlusį didelę žalą, o šio straipsnio 2 d. numatyta baudžiamoji atsakomybė už tą pačią veiką informacinių sistemų, turinčių strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai, duomenims.

Pagrindinis šios nusikalstamos veikos objektas - elektroninių duomenų saugumas.

Nusikalstamos veikos, numatytos šio straipsnio 1 d. dalykas - bet kokie elektroniniai duomenys, o šio straipsnio 2 d. - tik strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniai duomenys. Elektroninio parašo įstatymo 2 straipsnyje elektroniniai duomenys apibrėžiami kaip visi duomenys, kurie tvarkomi informacinių technologijų priemonėmis[44].

LR BK 196 str. numatytos nusikalstamos veikos objektyvioji pusė gali pasireikšti vienu ar keliais iš šių alternatyvių veiksmų:

- neteisėtas elektroninių duomenų sunaikinimas;
- neteisėtas elektroninių duomenų sugadinimas;
- neteisėtas elektroninių duomenų pašalinimas;
- neteisėtas elektroninių duomenų pakeitimas;
- technine įranga, programine įranga ar kitais būdais naudojimosi elektroniniais duomenimis apribojimas.

Įvykdžius šiuos alternatyvius(-ų) nusikalstamus (-ą) veiksmus (-ą) tam, kad jie būtų kvalifikuojami kaip baigta nusikalstama veika, yra reikalinga, kad būtų įvykdytos šios trys sąlygos:

[44] Lietuvos Respublikos elektroninio parašo įstatymas. Valstybės žinios, 2000, Nr. 61-1827.

1. Šie veiksmai turi būti neteisėti. *Tai reiškia, kad asmuo, atlikdamas tokius veiksmus, nėra teisėtas elektroninių duomenų naudotojas - neturi teisėto duomenų savininko ar valdytojo leidimo naudotis ar dirbti su konkrečia informacija, arba toks naudojimasis ar darbas su elektroniniais duomenimis yra draudžiamas pagal teisės aktus (pvz., Valstybės ir tarnybos paslapčių įstatymas numato, kad įslaptinta informacija gali būti patikėta tik atitinkamus leidimus dirbti ar susipažinti su įslaptinta informacija turintiems asmenims). Neteisėtumas bus ir tuo atveju, kai asmeniui suteikiama ribota teisė naudotis ar dirbti su duomenimis (pvz. tik susipažinti, papildyti), tačiau jis viršydamas savo kompetenciją (suteiktus įgaliojimus) padaro veiksmus, kuriais tie duomenys sunaikinami, sugadinami, pašalinami ar pakeičiami*[45].

2. Turi kilti reali žala – turi būti sunaikinti, sugadinti, pašalinti ar pakeisti duomenys ar apribotas naudojimasis jais ir visais atvejais ši žala turi būti didelė.

3. Būtent dėl šių nusikalstančio asmens veiksmų (o ne pvz. programinės įrangos klaidos ir pan.) nukentėjusysis turi patirti didelę žalą, t.y. turi būti priežastinis ryšys tarp atliekamų veiksmų ir atsiradusių padarinių.

Atkreiptinas dėmesys, kad įstatymo leidėjas nėra pateikęs išaiškinimo, kokia žala jau yra laikoma didele. Tokiu atveju, teismui paliekama teisė kiekvienu konkrečiu atveju spęsti, ar padarytoji žala yra didelė, taigi didelės žalos nustatymo bendrieji principai ir jos vertinimo kriterijai turėtų susiformuoti iš teismų praktikos.

Panevėžio miesto apylinkės teismas, nagrinėdamas baudžiamąją bylą Nr. 1-187-389/2011, nustatė, kad R. Š. neteisėtai pakeitė kompiuteryje esančius elektroninius duomenis „..ir tokiu būdu iššvaistė jai patikėtą svetimą, UAB „D“ priklausantį turtą–2000 litrų dyzelino bendros 5957,40 Lt vertės, perleisdama jį nenustatytiems asmenims, ir tuo padarydama UAB „Deliuvis“ didelės žalos.“[46] Taigi, šiuo atveju teismas konstatavo, kad 5957,40 lt vertės žala jau gali būti laikoma didele ir nusikalstama veika yra kvalifikuotina pagal LR BK 196 str. 1 d.

Tuo tarpu Vilniaus miesto 2 apylinkės teismas, nagrinėdamas baudžiamąją bylą, kurioje V. Č. kaltinamas neteisėtai perėmęs, pasisavinęs ir laikęs neviešus elektroninius duomenis; neteisėtai įgijęs ir laikęs slaptažodžius, prisijungimo kodus, tiesiogiai skirtus daryti nusikalstamas veikas; neteisėtai prisijungęs prie informacinės sistemos, pažeisdamas informacinės sistemos apsaugos priemones; neteisėtai pakeitęs elektroninius duomenis, padarydamas nedidelės žalos, konstatavo, kad įvykdytais dviem neteisėtais elektroninių duomenų pakeitimais padarė VšĮ (duomenys neskelbtini) kolegijai bendrai nedidelę neturtinę 5000 litų žalą.[47]. Iš šios bylos pavyzdžio matome, kad kito teismo nuomone, 5000 lt vertės žala jau yra laikoma nedidele. Taigi, akivaizdu, kad neturint

[45] Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis. II tomas. Vilnius: VĮ „Registrų centras“, 2009, p. 419.
[46] Panevėžio miesto apylinkės teismo 2011 m. spalio 25 d. nuosprendis baudžiamojoje byloje Nr. 1-187-389/2011.
[47] Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. nuosprendis baudžiamojoje byloje Nr. 1-515-487/2009.

aiškiai apibrėžtų kriterijų takoskyra tarp didelės ir nedidelės žalos yra labai sunkiai nustatoma ir iš esmės priklauso nuo kiekvieno teismo individualaus vertinimo.

Kauno miesto apylinkės teismas nagrinėdamas baudžiamąją bylą, kurioje A. A., Lietuvos Respublikos pilietis, 11 klasių išsilavinimo, viengungis, Kauno vidurinės mokyklos moksleivis kaltinamas nusikalstamų veikų, numatytų Lietuvos Respublikos baudžiamojo kodekso 196 str. 1 d., 196 str. 3 d. padarymu, konstatavo, kad „kaltinamasis padarė Kodekso 196 str. 1 d. dispozicijoje nurodytą didelę (ji nėra apibrėžiama materialiniu dydžiu) žalą: iš civilinio ieškovo atstovų paaiškinimų matyti, kad sunaikintoji svetainė buvo sukurta dar 2004 metais, joje buvo daug informacijos, kurios atkurti nebėra galimybės.“[48]Šiuo atveju civilinio ieškovo atstovai gana detaliai pagrindė žalą, nurodydami kad *„Po įsilaužimo į (duomenys neskelbtini) vidurinės mokyklos svetainę ji buvo sunaikinta neatstatomai, nes svetainės aptarnautojas atnaujina svetainėje padarytus pakeitimus penktadieniais, ankstesnių duomenų neišsaugodamas. Svetainė (duomenys neskelbtini) buvo sukurta 2004 metais, svetainėje buvo patalpinta labai daug duomenų, apie 1000 nuotraukų ir kitos informacijos apie mokyklą, šie duomenys sunaikinti neatstatomai, juos reikia rinkti iš naujo, todėl po svetainės sunaikinimo mokyklai padaryta didelė žala. Mokykla nuolat dalyvaudavo mokyklų svetainių konkursuose, ne kartą yra juos laimėjusi. Naujos svetainės sukūrimas kainavo 10000 litų, tačiau už tai dar nėra sumokėta: su UAB „(duomenys neskelbtini)“, atlikusia svetainės atkūrimo darbus yra susitarta, kad 10000 litų dydžio sąskaita - faktūra bus apmokėta iki 2011-12-01.“*[49]

Akivaizdu, kad pagal teismų praktiką padaroma didelė žala gali būti tiek turtinė, tiek ir neturtinė (moralinė, socialinė ir pan.).

Tuo tarpu elektroninių duomenų sunaikinimo, sugadinimo, pašalinimo ar pakeitimo padarymo būdai nėra numatyti šioje sudėtyje.

Kalbant apie subjektyviąją tokios nusikalstamos veikos pusę, reikia pabrėžti, jog kaltės forma galima tik tyčia – tiek tiesioginė, tiek netiesioginė.

Subjektu pagal LR BK 196 str. gali būti pakaltinamas vyresnis nei 16 metų amžiaus fizinis asmuo, taip pat ir juridinis asmuo.

Sankcijoje už neteisėtą poveikį elektroniniams duomenims nustatytos šios alternatyvios bausmės - viešieji darbai arba bauda, arba laisvės atėmimas iki ketverių metų; už neteisėtą poveikį strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniams duomenims - bauda arba areštas, arba laisvės atėmimas iki šešerių metų.

[48] Kauno miesto apylinkės teismo 2011 m. spalio 25 d. nuosprendis baudžiamojoje byloje Nr.1-2092-246/2011.
[49] Kauno miesto apylinkės teismo 2011 m. spalio 25 d. nuosprendis baudžiamojoje byloje Nr.1-2092-246/2011.

Vadovaujantis BK 11 str. 4 dalimi nusikalstamos veikos, už kurias numatyta baudžiamoji atsakomybė pagal 196 str., priskirtinos apysunkių nusikaltimų grupei.

Kadangi įstatymų leidėjas nėra pateikęs 196 str. vartojamų sąvokų išaiškinimo, taip pat yra nustatęs, kad už straipsnyje numatytą nusikalstamą veiką galima taikyti įvairias alternatyvias sankcijas, tai didelę įtaką kaip šis straipsnis yra įgyvendinamas realiame gyvenime turi teismų praktika. Todėl žemiau pateikiama lentelė, rodanti per paskutinius penkerius metus, t.y. 2007 - 2011 metais, I instancijos teismuose gautų ir išnagrinėtų bylų pagal 196 str. statistiką.

1 Lentelė. 2007 - 2011 metais I instancijos teismuose gautos ir išnagrinėtos bylos pagal 196 str.

Metai	**Nebaigtų bylų likutis ataskaitinio laikotarpio pradžioje**	**Gauta bylų**	**Baigta bylų**	**Nebaigtų bylų likutis ataskaitinio laikotarpio pabaigoje**	**Bylų nagrinėjimo trukmė**		
					Iki 6 mėnesių	**Nuo 6 iki 12 mėnesių**	**12 mėnesių ir ilgiau**
2011	1	0	1	0	0	1	0
2010	0	1	0	1	0	0	0
2009	2	1	3	0	2	0	1
2008	0	2	0	2	0	0	0
2007	0	0	0	0	0	0	0

Šaltinis: Teismų statistika http://www.teismai.lt/lt/teismai/teismai-statistika

Kaip matyti iš teismuose išnagrinėtų bylų statistikos, į teismus pagal šį straipsnį patenka labai nedaug bylų, pats didžiausias „pikas“ buvo 2008 m. kai teisme buvo gautos „net“ dvi bylos. Labai abejotina, kad per metus laiko padaromos vos viena ar dvi tokio pobūdžio veikos, todėl matyt priežasčių reikėtų ieškoti kitur. Mūsų nuomone, galima daryti keletą prielaidų, kodėl bylos pagal šį straipsnį nepasiekia teismo. Viena iš jų – didelis tokių nusikalstamų veikų latentiškumas. Kita - tyrėjams, atliekantiems ikiteisminį tyrimą, yra nelengva įrodinėti, kad buvo padaryta didelė žala, ypač jei ji yra neturtinio pobūdžio, neturint nustatytų jokių aiškių tokios „didelės žalos“ vertinimų kriterijų. Pažymėtina, kad teismų praktika nagrinėjant tokio pobūdžio bylas dar tik formuojasi, todėl akivaizdu, kad turės praeiti dar pakankamai ilgas laiko tarpas kol bus suformuota bendra 196 str. straipsnio dispozicijoje pateiktų neapibrėžtų sąvokų (pvz. didelės žalos) samprata.

Mūsų nuomone, vis tik būtų tikslinga LR BK XXX skyrių papildyti dar vienu straipsniu, kuriame būtų pateiktas labai abstrakčios sąvokos „didelė žala“ išaiškinimas, atskleidžiant tiek turtinį, tiek ir neturtinį šios sąvokos aspektus. Tokiu būdu būtų išvengta šios sąvokos nevienodo

traktavimo problemos, o kartu ir veikos kvalifikavimo problemos. Juolab, kad tokia praktika pateikti sąvokos išaiškinimus pačiame LR BK yra taikoma, pvz. LR BK 190 str. yra išaiškinta turto vertė, taikoma XXVIII skyriaus nusikaltimams.

Rusijoje baudžiamoji atsakomybė už neteisėtą prieigą prie kompiuterinės informacijos, sukėlusią neigiamą poveikį šiai informacijai, numatyta pagal RF BK 272 str. „Neteisėta prieiga prie kompiuterinės informacijos“.

Pažymėtina, kad prie RF BK 272 str. yra pridedama grafa „Pastabos“, kurioje pateikiamas keleto naudojamų sąvokų išaiškinimas. Čia nurodyta, kad kompiuterinė informacija suprantama kaip informacija (žinutės, duomenys), pateikta elektroninių signalų pagalba, nepriklausomai nuo jų laikymo, perdirbimo ar perdavimo būdų.

RF BK 272 str. 1 d. numatyta baudžiamoji atsakomybė už neteisėtą prieigą prie įstatymo saugomos kompiuterinės informacijos, jeigu tai sukėlė kompiuterinės informacijos sunaikinimą, blokavimą, modifikavimą arba kopijavimą, o šio straipsnio 2 d. numatyta baudžiamoji atsakomybė už tą pačią veiką sukėlusią didelę žalą, arba padarytą iš savanaudiškų paskatų. Šio straipsnio 3 d. numatyta baudžiamoji atsakomybė už tuos pačius veiksmus, numatytus šio straipsnio 1 ir 2 dalyse, padarytus grupės iš anksto susitarusių asmenų arba organizuotos grupės arba asmens pasinaudojant savo tarnybine padėtimi, o šio straipsnio 4 d. numatyta baudžiamoji atsakomybė už tuos pačius veiksmus, numatytus šio straipsnio 1, 2 ir 3 dalyse, jei jie sukėlė sunkias pasekmes arba sudarė sąlygas jiems atsirasti.

Šios nusikalstamos veikos objektas – įstatymo saugomos kompiuterinės informacijos saugumas, iš esmės atitinka LR BK 196 str. numatytą nusikalstamos veikos objektą - elektroninių duomenų saugumas.

RF BK 272 str. bendrasis dalykas – įstatymo saugoma kompiuterinė informacija. Dėl sampratos, kas yra „įstatymo saugoma“ informacija Rusijos mokslininkų nuomonės išsiskiria. Dalis autorių šią sąvoką aiškina gana siaurai, kaip pavyzdžiui, М.М. Карелина, kuri nurodo, kad įstatymo saugoma informacija tai tokia informacija, kuriai specialiais įstatymais nustatyta teisinė apsauga (valstybinė, tarnybinė ir komercinė paslaptys, asmens duomenys ir kt.)[50]. Tuo tarpu kita dalis mokslininkų šią sąvoką aiškina daug plačiau, pavyzdžiui, Ю. В. Гаврилин, atskleisdamas šios sąvokos turinį, remiasi Konstitucija, Rusijos Federacijos civiliniu kodeksu, kitais teisės aktais ir nurodo, kad įstatymo saugoma gali būti tiek fizinių, tiek juridinių asmenų, tiek valstybinė informacija[51]. Mes pritartume pastarojo autoriaus nuomonei, nes labiau tikėtina prielaida, kad

[50] Карелина М.М. Преступления в сфере компьютерной информации. http://www.crime-research.ru/library/CodeRu.htm [2012-03-10]

[51] Преступления в сфере компьютерной информации: квалификация и доказывание: учебное пособие /под редакцией Ю. В. Гаврилина. Москва: Книжный мир, 2003, p. 16.

įstatymų leidėjas siekė apsaugoti visą informaciją, o ne tik tam tikrą dalį. Taigi, jeigu šią sąvoką aiškinsime plečiamai, tai šio nusikaltimo dalykas yra labiausiai panašus į LR BK 196 str. dalyką.

RF BK 272 str. numatyto nusikaltimo objektyvioji pusė gali būti apibrėžiama kaip neteisėta prieiga prie įstatymo saugomos kompiuterinės informacijos, jeigu tai sukėlė kompiuterinės informacijos sunaikinimą, blokavimą, modifikavimą arba kopijavimą. Mūsų nuomone, šio nusikaltimo objektyvioji pusė turi nemažai panašumų su LR BK 196 str. objektyviąja puse, kuri taip pat apima tokius veiksmus kaip elektroninių duomenų sunaikinimą, blokavimą ir modifikavimą, tik neapima vieno veiksmo – elektroninių duomenų kopijavimo. Tačiau už neviešų elektroninių duomenų kopijavimą baudžiamoji atsakomybė numatyta pagal kitą LR BK straipsnį – 198, kurį vėliau detaliau panagrinėsime savo darbe.

Iš RF BK 272 str. straipsnio dispozicijos matyti, kad tokio pobūdžio veika pripažįstama nusikalstama, jeigu ją realizuojant įvykdomos keturios esminės sąlygos:

1. prieiga prie kompiuterinės informacijos turi būti neteisėta (iš esmės tokia pati sąlyga yra numatyta LR BK 196 str.);

2. pasikėsinama ne į bet kokią kompiuterinę informaciją, bet tik į tą, kurią saugo įstatymas;

3. turi kilti neigiamos pasekmės – kompiuterinės informacijos sunaikinimas, blokavimas, modifikavimas arba kopijavimas;

4. būtent dėl šios nusikalstančio asmens veikos (o ne pvz. programinės įrangos klaidos ir pan.) buvo sunaikinta, blokuota, modifikuota ar nukopijuota kompiuterinė informacija, t.y. turi būti nustatytas priežastinis ryšys tarp atliekamų veiksmų ir atsiradusių padarinių (to taip pat reikalauja ir LR BK 196 str. dispozicija). „..paprastas laiko sutapimas neteisėtos prieigos ir kompiuterinės sistemos pažeidimo, kurį sukėlė kompiuterinės sistemos gedimas ar programinės įrangos klaidos neužtraukia baudžiamosios atsakomybės“.[52]

Kad nesant bent vieno iš šių keturių požymių, atitinkama veika negali būti pripažįstama nusikalstama pagal RF BK 272 str. patvirtina ir Rusijos teismų praktika. Jamalo-Nencų autonominio rajono teismas 2012 m. vasario 16 d. kasaciniu sprendimu konstatavo, kad „*pagrindas K. nuteisimui buvo tas, kad laikotarpiu nuo 2011 m. kovo 30 d. iki birželio 5 d. jis, siekdamas neteisėtos prieigos prie interneto tinklo, naudojo kitų vartotojų registracijos duomenis (vartotojo vardą ir slaptažodį), įvedęs juos į savo kompiuterio nustatymus. Dėl to į jo kompiuterio kietojo disko sisteminį bloką buvo perrašyti abonentų vardai, jų asmeninių sąskaitų numeriai, informacija apie duomenų srautus, sąskaitų apmokėjimus, registracijos duomenys (vartotojo vardai ir slaptažodžiai). Nusikaltimo, numatyto 272 str. 1 d. būtinu požymiu yra pasekmės, tokios kaip kompiuterinės informacijos sunaikinimas, blokavimas, kopijavimas arba modifikavimas. Be to,*

[52] В. Наумов Отечественное законодательство в борьбе с компьютерными преступлениями. http://www.hackzone.ru/articles/a5.html [2012-03-10]

tokios pasekmės turi būti neteisėtos prieigos prie įstatymo saugomos kompiuterinės informacijos rezultatas, t.y. tarp jų turi būti priežastinis ryšys. Be to, aprašomojoje-motyvacinėje dalyje teismas konstatavo tiktai neteisėtą kompiuterinės informacijos perrašymo į teisiamojo asmeninio kompiuterio kietąjį diską faktą. Bet nuosprendžio aprašomojoje - motyvacinėje dalyje nebuvo įvardinta, kad dėl K. veiksmų būtų kilusios kokios nors pasekmės, numatytos 272 str. 1 d. Dėl šios priežasties 2012 m. vasario 16 d. kasaciniu sprendimu buvo panaikintas miesto teismo nuosprendis, baudžiamoji byla grąžinta iš naujo nagrinėti.“[53]

Kadangi rusų mokslinėje literatūroje kyla daug diskusijų, kokia prieiga prie kompiuterinės informacijos turi būti laikoma neteisėta, šios sąvokos traktavimą aptarsime plačiau. Ю. Гульбин mano, kad „neteisėta prieiga prie informacijos yra tokia prieiga, kai pažeidžiamos galiojančios teisės normos, administraciniai aktai, įsakymai ar kiti teisės aktai, reglamentuojantys priėjimo prie informacijos santykius tarp asmenų (grupės asmenų)“.[54] Mūsų nuomone, neteisėtos prieigos nereikėtų susieti su norminių teisių aktų pažeidimu, nes tuomet neaišku kaip reikėtų traktuoti tokią prieigą prie duomenų, kurios nereglamentuoja norminiai teisės aktai, tačiau šių duomenų savininkas nėra suteikęs leidimo prieiti prie šių duomenų. Т.И. Ваулина mano, kad neteisėta prieiga reikėtų laikyti prieigą prie uždaros informacinės sistemos, kurią įvykdo asmuo, nesantis teisėtas šios informacijos savininkas arba neturintis leidimo dirbti su šia informacija“.[55] Tačiau šis apibrėžimas savo ruožtu sukelia dar papildomų klausimų - nėra aišku, kas tai yra „uždara informacinė sistema“. В. Наумов nuomone, „Neteisėta laikoma prieiga prie saugomos kompiuterinės informacijos, kurią atlieka asmuo, neturintis teisės gauti šios informaciją ir su ja dirbti (įskaitant ir kompiuterių sistemą)“.[56] О М.М. Карелина dar pabrėžia, kad „tokiai informacijai turi būti taikomos apsaugos priemonės, nustatant asmenis, galinčius prie jos prieiti.“[57] Mes pritartume šiam jungtiniam dviejų autorių pateikiamam apibrėžimui.

Štai ir Dzeržinskio miesto teismas, nagrinėdamas neteisėtos prieigos prie kompiuterinės informacijos bylą nustatė, kad Галушкин Д.А., laikotarpiu nuo 2010 m. rugpjūčio 10 d. iki 2010 m. spalio 4 d. dirbo ООО ТК ir jam tarnybinių pareigų atlikimui (dalykiniam susirašinėjimui) buvo suteiktas slaptažodis prisijungti prie įmonės pašto dėžutės. 2010 m. spalio 4 d. Галушкин Д.А. buvo atleistas iš pareigų. tačiau 2010 m. spalio 14 d. jis, suprasdamas, kad minėtas slaptažodis prisijungti prie įmonės pašto dėžutės jam buvo suteiktas išskirtinai darbo tikslais ir atleidus iš

[53] Актуальные кассационные определения по уголовным делам за период с 11 по 20 февраля 2012 года. http://oblsud.ynao.sudrf.ru/modules.php?name=press_dep&op=1&did=538 [2012-04-15]

[54] Гульбин Ю. Преступления в сфере компьютерной информации. http://www.lawmix.ru/comm/8288/ [2012-03-10]

[55] Уголовное право. Особенная часть / под редакцией И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов. Москва: норма, 1998, p.557.

[56] Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями. http://www.hackzone.ru/articles/a5.html [2012-03-10]

[57] Карелина М.М. Преступления в сфере компьютерной информации. http://www.crime-research.ru/library/CodeRu.htm [2012-03-10]

įmonės jam daugiau nepriklauso ir jis nebeturi teisės naudotis įmonės pašto dėžute, vis tiek prie jos prisijungė nusikalstamais tikslais. Teismas konstatavo, kad Галушкин Д.А. įvykdė neteisėtą prieigą prie kompiuterinės informacijos, nes prie įmonės pašto dėžutės prisijungė neteisėtai, t.y. neturėdamas kompiuterinės informacijos savininko OOO TK leidimo. Tuo pačiu Галушкин Д.А. sunaikino prieigos prie pašto dėžutės slaptažodį, kurį buvo nustatęs savininkas OOO TK ir užblokavo savininkui galimybę prisijungri prie savo pašto dėžutės.[58] Taigi šiuo atveju teismas taip pat konstatavo, kad neteisėta yra laikoma prieiga neturint kompiuterinės informacijos savininko leidimo ir pažeidžiant savininko nustatytas apsaugos priemones.

272 str. 2, 3 ir 4 dalyje yra numatytos sunkinančios aplinkybės, dėl kurių nusikaltimas yra laikomas sunkesnis, ko pasekoje už jį yra numatomos griežtesnės sankcijos, ir jas įstatymo leidėjas susieja su:

- Nusikaltimo subjektu:

  - nusikalstama veika padaroma grupės iš anksto susitarusių asmenų;

  - nusikalstama veika padaroma organizuotos grupės; Atkreiptinas dėmesys, kad pagal LR BK 60 str. jei veiką padarė bendrininkų ar organizuota grupė, tai visada laikoma sunkinančia aplinkybe skiriant bausmę, nepriklausomai nuo to, kokio pobūdžio nusikalstama veika yra įvykdoma.

  -nusikalstama veika padaroma asmens pasinaudojant savo tarnybine padėtimi.

- Nusikaltimo subjektyviąja puse:

  -nusikalstama veika padaroma iš savanaudiškų paskatų.

- Nusikaltimo padariniais:

  -nusikalstama veika sukėlė didelę žalą. Prie RF BK 272 str. pateiktose pastabose pateikiamas didelės žalos apibrėžimas, nurodant, kad didelė žala numatyta šiame straipsnyje laikoma žala, kurios suma viršija vieną milijoną rublių. Tuo tarpu LR BK 196 str. sąlyga, kad nusikalstama veika turi sukelti didelę žalą yra ne sunkinanti aplinkybė, o būtina sąlyga baudžiamajai atsakomybei pagal šį straipsnį kilti.

  -nusikalstama veika sukėlė sunkias pasekmes arba sudarė sąlygas jiems atsirasti. Sąvokos „sunkios pasekmės“ samprata RF BK nepateikiama, todėl teismams kiekvienu konkrečiu atveju tenka spręsti, ar nusikalstama veika yra sukeliamos sunkios pasekmės.

Tuo tarpu LR BK 196 str. nusikaltimą sunkinančios aplinkybės yra susiejamos tik su nusikaltimo dalyku, t.y. jeigu pasikėsinama į strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroninius duomenis. Rusijos įstatymų leidėjas nėra išskyręs dalyko vertingumo kaip kvalifikuojančio

[58]Приговор Дзержинского городского суда от 27 июля 2011 года Дело № (не определено). http://www.gcourts.ru/case/1446171 [2012-04-15]

požymio, kas, mūsų nuomone, gali būti traktuojama kaip teisinė spraga. Manome, kad informacija, į kurią kėsinamasi yra nelygiavertė ir už pasikėsinimą į visos valstybės funkcionavimui ir saugumui ypač svarbią bei reikšmingą informaciją, tikrai turėtų būti nustatyta griežtesnė atsakomybė negu už pasikėsinimą į vienam fiziniam asmeniui priklausančią informaciją.

Pažymėtina, kad skaitant mokslinę literatūrą ir nagrinėjant teismų praktiką vis dažniau galima pastebėti, kad elektroninius nusikaltimus padaro darbuotojai, pasinaudodami savo tarnybine padėtimi ir padarydami žalos būtent tai įstaigai, bankui ar kitai institucijai, kurioje dirba.

Pavyzdžiui, Panevėžio miesto apylinkės teismas, nagrinėdamas baudžiamąją byloje Nr. 1-187-389/2011, nustatė, kad *R. Š. dirbdama vadybininke ir būdama atsakinga už UAB „D“ degalinės Nr. 3 materialinius ir piniginius likučius, jų judėjimą ir ataskaitų sudarymą, laikotarpiu nuo 2007 m. gruodžio 12 d. iki 2008 m. vasario 1 d., kad 2000 litrų dyzelino trūkumas nepasimatytų mėnesio pabaigoje pildomose ataskaitose, neteisėtai pakeitė kompiuteryje esančius elektroninius duomenis, tai yra informacinę sistemą papildė naujais neegzistuojančiais elektroniniais duomenimis, o būtent: 2007 m. gruodžio 12 d., pagal krovinio važtaraštį Nr. 0002393 į degalinę Nr. 3 atvežtą 13293 litrus dyzelino 12:40:05 val. įvedė i kompiuterinę programą, po to, 09:13:54 val., suformavo neegzistuojantį dokumentą Nr. 00001, kuriuo iš programos išminusavo 3000 litrų dyzelino, 2007 m. gruodžio 14 d., 15:29:46 val., suformavo neegzistuojantį dokumentą DID Nr. 1111, kuriuo į programą įvedė 1000 litrų dyzelino, 2007 m. gruodžio 31 d., 23:25:02 val., suformavo neegzistuojantį dokumentą Nr. 00000345, kuriuo į programą įvedė 2000 litrų dyzelino, 2008 m. sausio 1 d., 01:31:35 val., suformavo neegzistuojantį dokumentą Nr. 00000345, kuriuo iš programos išminusavo 2000 litrų dyzelino, 2008 m. sausio 31 d., 20:43:38 val., suformavo neegzistuojantį dokumentą Nr. 002, kuriuo į programą įvedė 2000 litrų dyzelino, 2008 m. vasario 1 d., 06:09:29 val., suformavo neegzistuojantį dokumentą Nr.01/002, kuriuo iš programos išminusavo 2000 litrų dyzelino ir tokiu būdu iššvaistė jai patikėtą svetimą, UAB „D“ priklausantį turtą–2000 litrų dyzelino bendros 5957,40 Lt vertės, perleisdama jį nenustatytiems asmenims, ir tuo padarydama UAB „Deliuvis“ didelės žalos.*[59]

Iš šios bylos matome, kad nusikalstamą veiką įvykdęs asmuo yra susijęs su įstaiga darbo santykiais. Jeigu savo tarnybine padėtimi nusikalstamais tikslais pasinaudojęs kaltininkas atitiktų specialaus subjekto požymį – jis būtų valstybės tarnautojas ar jam prilygintas asmuo, tai tuomet būtų keliamas ir kaltininko veiksmų kvalifikavimo pagal LR BK 228 straipsnį „Piktnaudžiavimas“ (1 d. – „Valstybės tarnautojas ar jam prilygintas asmuo, piktnaudžiavęs tarnybine padėtimi arba viršijęs įgaliojimus, jeigu dėl to didelės žalos patyrė valstybė, tarptautinė viešoji organizacija, juridinis ar fizinis asmuo <...>. 2 d. Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką

[59] Panevėžio miesto apylinkės teismo nuosprendis 2011 m. spalio 25 d. baudžiamojoje byloje Nr. 1-187-389/2011

siekdamas turtinės ar kitokios asmeninės naudos, jeigu nebuvo kyšininkavimo požymių <...>[60]) klausimas. Tačiau aukščiau pateiktoje byloje kaltininkė su darbdaviu buvo susijusi darbo santykiais, grįstais darbo sutartimi, todėl jos piktnaudžiavimas tarnybine padėtimi negali būti inkriminuojamas pagal sutaptį su LR BK 228 straipsniu.

Atsižvelgiant į tai, kad vis daugiau elektroninių nusikaltimų yra padaroma darbuotojų, jiems piktnaudžiaujant užimamomis pareigomis, taip pat į tai, kad tokie asmenys, kurie dėl savo užimamų pareigų turi prieigą prie svarbių elektroninių duomenų, neretai gali padaryti daug didesnę žalą atitinkamai institucijai negu kiti asmenys, manytume, kad ir LR BK 196 str. būtų tikslinga nustatyti papildomą kvalifikuojantį požymį (kaip tai yra padaryta RF BK 272 str.) – jei nusikalstama veika padaroma asmens pasinaudojant savo tarnybine padėtimi. Mūsų nuomone, šiuo atveju sunkesnės bausmės nustatymas galėtų veikti prevenciškai, siekiant kuo labiau sumažinti atvejus, kai „įmonei/įstaigai kenkiama iš vidaus“.

RF BK 272 str. numatytos nusikalstamos veikos subjektyvioji pusė – tiesioginė tyčia, kai tuo tarpu LR BK 196 str. kaltės forma galima tiek tiesioginė, tiek ir netiesioginė tyčia.

RF BK 272 str. nereglamentuoja situacijos, kai neteisėta prieiga įvykdoma dėl neatsargumo, dėl to atsakomybė nekyla dėl didelės dalies veikų ir netgi dėl tų veikų, kurios iš tikrųjų buvo padarytos tyčia.[61]

RF BK 272 str. numatytos nusikalstamos veikos subjektas – pakaltinamas pilnametis fizinis asmuo. Tačiau skirtingai negu LR BK 196 str., RF BK 272 str. nėra nustatyta, kad baudžiamojon atsakomybėn gali būti traukiami ir juridiniai asmenys. Tuo atveju, jeigu neteisėtą veiką atlieka juridinio asmens atstovas, tai šiam fiziniam asmeniui tiesiogiai ir tenka atsakomybė.

RF BK 272 str. 1 d. sankcijoje nustatytos šios alternatyvios bausmės - bauda iki dviejų šimtų tūkstančių rublių arba gauto atlyginimo dydžio, arba kitokių nuteistojo pajamų, gautų iki aštuoniolikos mėnesių laikotarpyje, dydžio, arba pataisos darbai iki vienerių metų arba laisvės apribojimas iki dviejų metų arba priverčiamieji darbai iki dviejų metų arba laisvės atėmimas tam pačiam terminui. Lyginant sankcijas už pagrindinę nusikalstamos veikos sudėtį matyti, kad LR BK 196 str. yra numatyta dvigubai griežtesnė laisvės atėmimo bausmė.

RF BK 272 str. 2 d. - bauda nuo šimto tūkstančių iki trijų šimtų tūkstančių rublių arba gauto atlyginimo dydžio, arba kitokių nuteistojo pajamų, gautų laikotarpyje nuo vienų iki dvejų metų, dydžio arba pataisos darbai nuo vienerių iki dvejų metų arba laisvės apribojimas iki keturių metų arba priverčiamieji darbai iki keturių metų arba areštas iki šešių mėnesių arba laisvės atėmimas tam pačiam terminui, RF BK 272 str. 3 d. - bauda iki penkių šimtų tūkstančių rublių arba gauto

[60] Lietuvos Respublikos baudžiamasis kodeksas. Valstybės žinios, 2000, Nr. 89-2741; 2004, Nr. 25-760; 2007, Nr. 81-3309.

[61] Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями. http://www.hackzone.ru/articles/a5.html [2012-03-11]

atlyginimo dydžio, arba kitokių nuteistojo pajamų, gautų laikotarpyje iki trijų metų, dydžio kartu su teisės užimti tam tikras pareigas arba verstis tam tikra veikla iki trijų metų atėmimu, arba laisvės apribojimas iki keturių metų arba priverčiamieji darbai iki penkių metų arba laisvės atėmimas tam pačiam terminui. RF BK 272 str. 4 d. - laisvės atėmimu iki septynerių metų.

Palyginus sankcijas už šias kvalifikuotas nusikaltimo sudėtis su LR BK 196 str. numatytomis sankcijomis už kvalifikuotas nusikaltimo sudėtis, matome, kad RF BK 272 str. skirtingai negu atitinkamame LR BK str. yra numatyta „dvigubų bausmių“ galimybė (pvz. bauda kartu su teisės užimti tam tikras pareigas arba verstis tam tikra veikla atėmimu). Sankcijos lyginamuose straipsniuose savo dydžiu iš esmės ženkliai nesiskiria, tačiau už pavojingiausią nusikalstamą veiką, numatytą RF BK 272 str. gali būti skiriama tik laisvės atėmimo bausmė.

Manome, kad įvertinus tai, jog įvykdžius LR BK 196 str. 2 d. nustatytą nusikalstamą veiką yra padaroma žala tokiems esminiams valstybės interesams kaip viešasis saugumas, valstybės valdymas, valstybės ekonominiai, finansiniai interesai ir kt., ji turėtų būti netoleruojama ir už jos atlikimą turėtų būti baudžiama griežtai. Mūsų nuomone, LR BK 196 str. 2 d. numatyta alternatyvi sankcija – bauda, yra pernelyg švelni ir neadekvati padaromam nusikaltimui, tuo tarpu RF BK 272 str. 4 d. numatyta sankcija yra gerokai labiau atgrasanti. Atsižvelgiant į tai, kas išdėstyta siūlytume LR BK 196 str. 2 d. sankcijoje panaikinti galimybę skirti baudą.

Vadovaujantis RF BK 15 str. 2 d. nusikalstamos veikos, už kurias numatyta baudžiamoji atsakomybė pagal 272 str. 1 d. priskirtinos nesunkių nusikaltimų grupei, o vadovaujantis RF BK 15 str. 3 d., nusikalstamos veikos, už kurias numatyta baudžiamoji atsakomybė pagal 272 str. 2 d. priskirtinos apysunkių nusikaltimų grupei.

Be to, atkreiptinas dėmesys, kad RF BK 272 str. 2 d. matyt padaryta korektūros klaida, nes labai keistai atrodo, kad už nusikaltimą, atliktą sunkinančiomis aplinkybėmis, gali būti skiriamas laisvės atėmimas iki 6 mėnesių, kai tuo tarpu pagal pagrindinę nusikaltimo sudėtį – iki dviejų metų.

Apibendrinus kas išdėstyta, mūsų nuomone, RF BK 272 str. savo prigimtimi yra labiausiai panašus į LR BK 196 str.

Deja, atsižvelgiant į tai, kad RF BK 272 str. pakeitimai buvo padaryti vos prieš keletą mėnesių, negalime pateikti palyginimui statistikos, kiek per paskutinius penkerius metus, t.y. 2007 - 2011 metais, Rusijos I instancijos teismuose buvo gauta ir išnagrinėta bylų pagal atitinkamą straipsnį.

3.2. Baudžiamoji atsakomybė už neteisėtą perėmimą

Lietuvoje baudžiamoji atsakomybė už neteisėtą elektroninių duomenų perėmimą gali kilti pagal LR BK 198 str. “Neteisėtas elektroninių duomenų perėmimas ir panaudojimas”.

LR BK 198 str. 1 d. numatoma baudžiamoji atsakomybė už neteisėtą neviešų elektroninių duomenų stebėjimą, fiksavimą, perėmimą, įgijimą, laikymą, pasisavinimą, paskleidimą ar kitokį panaudojimą, o LR BK 198 str. 2 d. numatoma baudžiamoji atsakomybė už neteisėtą neviešų elektroninių duomenų, turinčių strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai stebėjimą, fiksavimą, perėmimą, įgijimą, laikymą, pasisavinimą, paskleidimą ar kitokį panaudojimą. Šios nusikalstamos veikos objektas - neviešų elektroninių duomenų konfidencialumas, o bendrasis dalykas – nevieši elektroniniai duomenys. Vilniaus apygardos teismo baudžiamųjų bylų skyriaus teisėjų kolegija, apeliacine tvarka nagrinėdama baudžiamąją bylą pagal nuteistojo T. S. ir Vilniaus miesto apylinkės prokuratūros prokuroro apeliacinius skundus dėl Vilniaus miesto 2 apylinkės teismo 2011 m. liepos 1 d. nuosprendžio pažymėjo, kad elektroniniai duomenys yra „įvardijami, kaip duomenys, tvarkomi informacinių technologijų priemonėmis ir yra sukurti elektronine forma arba perkelti į tokią formą. Taip pat elektroniniai duomenys įvardijami ir kaip ženklų seka, skirta perduoti informacijai, naudojant informacines technologijas.”[62]

Tuo tarpu nevieši duomenys, tai tokie duomenys, kurie skirti ne visiems, visuotinai nenaudojami. Tokių neviešų duomenų įgijimas ir naudojimas siejamas su tam tikrais apribojimais, specialiais reikalavimais ar procedūromis, kurie gali būti nustatyti įstatymuose ar kituose teisės aktuose, įmonių, įstaigų, organizacijų vidaus dokumentuose, taip pat tuo atveju, kai asmuo tikisi privataus jų perdavimo[63].

LR BK 198 str. numatytos nusikalstamos veikos objektyvioji pusė gali pasireikšti vienu ar keliais iš šių alternatyvių veiksmų:

- neteisėtas neviešų elektroninių duomenų stebėjimas;
- neteisėtas neviešų elektroninių duomenų fiksavimas;
- neteisėtas neviešų elektroninių duomenų perėmimas;
- neteisėtas neviešų elektroninių duomenų įgijimas;
- neteisėtas neviešų elektroninių duomenų laikymas;
- neteisėtas neviešų elektroninių duomenų pasisavinimas;
- neteisėtas neviešų elektroninių duomenų paskleidimas;
- neteisėtas kitoks neviešų elektroninių duomenų panaudojimas.

Vilniaus apygardos teismas, nagrinėdamas baudžiamąją bylą pagal nuteistojo T. S. ir Vilniaus miesto apylinkės prokuratūros prokuroro apeliacinius skundus dėl Vilniaus miesto 2 apylinkės

[62] Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje Nr. 1A-977/2011.
[63] Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis. II tomas. Vilnius: VĮ „Registrų centras“, 2009, p. 430.

teismo 2011 m. liepos 1 d. nuosprendžio pažymėjo, kad „kitoks elektroninių duomenų panaudojimas yra tokių duomenų pritaikymas, pavartojimas kokiam nors tikslui. Tai gali būti tiek kaltininko, tiek kitų asmenų chuliganiškiems, savanaudiškiems ar kitokiems interesams tenkinti. Neteisėto elektroninių duomenų perėmimo ir panaudojimo objektyvieji požymiai įstatymo dispozicijoje suformuluoti kaip alternatyvūs, todėl baudžiamajai atsakomybei kilti pakanka, kad būtų padaryta bent viena iš šių veikų."[64]

Įvykdžius šiuos alternatyvius(-ų) nusikalstamus (-ą) veiksmus (-ą) tam, kad jie būtų kvalifikuojami kaip baigta nusikalstama veika, yra reikalinga, kad būtų įvykdytos šios dvi sąlygos:

1. Šie veiksmai turi būti neteisėti; Vilniaus apygardos teismo baudžiamųjų bylų skyriaus teisėjų kolegija, apeliacine tvarka nagrinėdama jau aukščiau paminėtą baudžiamąją bylą konstatavo, kad *esminė aplinkybė, daranti T. S. veiksmus nusikalstamais - tai elektroninių duomenų pasisavinimas neturint tam teisės. Byloje nustatyta, kad T. S., neturėdamas teisėto elektroninės bankininkystės sąskaitų generatoriaus duomenų valdytojo - UAB „VSG " (duomenys pakeisti) leidimo, t.y. neteisėtai, savanaudiškiems interesams tenkinti, turimo elektroninės bankininkystės sąskaitų generatoriaus duomenų pagalba savavališkai prisijungė prie UAB „VSG" (duomenys pakeisti) sąskaitos ir iš šios sąskaitos į savo sąskaitą bei savo vadovaujamos bendrovės sąskaitas atliko piniginių lėšų pervedimus, t.y. nagrinėjamu atveju elektroninių duomenų panaudojimo objektyvusis požymis buvo realizuotas pasitelkiant kodų generatorių, kurio pagalba buvo pervestos lėšos į T. S. sąskaitą. Tokiu būdu, pirmos instancijos teismo išvada, kad „T. S. nepadarė veikos, turinčios nusikaltimo, numatyto LR BK 198 str. 1 d., požymių" yra nepagrįsta ir neatitinkanti realių faktinių aplinkybių.*[65]

2. Turi būti pasikėsinama ne į bet kokius elektroninius duomenis, bet tik į tuos, kurie yra nevieši, t.y. nėra skirti visuotiniam naudojimui.

Atkreiptinas dėmesys, kad tam, kad būtų konstatuotas nusikalstamos veikos baigtumas pagal 198 str. , nereikalinga, kad kiltų reali didelė žala ir būtų nustatytas priežastinis ryšys tarp veikos ir neigiamų pasekmių, kaip kad buvo reikalaujama prieš tai aptartame straipsnyje – pakanka atlikti straipsnio dispozicijoje išvardintus veiksmus(-ą).

Kalbant apie subjektyviąją tokios nusikalstamos veikos pusę, reikia pabrėžti, jog galima kaltės forma tik tiesioginė tyčia.

Šios nusikalstamos veikos subjektas - asmuo, kuriam iki nusikaltimo padarymo buvo suėję šešiolika metų. Toks asmuo taip pat turi būti pakaltinamas. Be to, už šiuos nusikaltimus atsako taip pat ir juridinis asmuo pagal LR BK 20 str. nustatytas juridinio asmens baudžiamosios atsakomybės sąlygas.

---

[64] Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje Nr. 1A-977/2011.
[65] Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje Nr. 1A-977/2011.

Nusikalstamos veikos, už kurias numatyta baudžiamoji atsakomybė pagal 198 str., vadovaujantis BK 11 str. 4 dalimi priskirtinos apysunkių nusikaltimų grupei.

LR BK 198 str. 1 d. sankcijoje alternatyviai numatytos šios bausmės - bauda arba laisvės atėmimas iki ketverių metų; LR BK 198 str. 2 d. numatyta vienintelė galima bausmė - laisvės atėmimas iki šešerių metų.

Išanalizavus žemiau pateikiamą 2 lentelę ir palyginus su kitomis pateikiamomis darbe, matome, kad tai vienas iš pagrindinių ir dažniausių straipsnių, numatančių atsakomybę už elektroninius nusikaltimus, pagal kurį bylos patenka į teismą.

2 Lentelė. 2007 – 2011 metais I instancijos teismuose gautos ir išnagrinėtos bylos pagal 198 str.

Metai	**Nebaigtų bylų likutis ataskaitinio laikotarpio pradžioje**	**Gauta bylų**	**Baigta bylų**	**Nebaigtų bylų likutis ataskaitinio laikotarpio pabaigoje**	**Bylų nagrinėjimo trukmė**		
					Iki 6 mėnesių	**Nuo 6 iki 12 mėnesių**	**12 mėnesių ir ilgiau**
2011	1	5	5	1	4	1	0
2010	0	5	4	1	4	0	0
2009	0	5	5	0	5	0	0
2008	0	3	2	1	2	0	0
2007	0	3	2	1	2	0	0

Šaltinis: Teismų statistika http://www.teismai.lt/lt/teismai/teismai-statistika

Rusijos BK nėra išskirta atskiro straipsnio, numatančio atsakomybę už sąmoningą ir neteisėtą neviešų elektroninių duomenų perdavimą į kompiuterinę sistemą, iš jos ar jos viduje. Tik jau mūsų nagrinėtame RF BK 272 str. numatyta baudžiamoji atsakomybė už neteisėtą prieigą prie įstatymo saugomos kompiuterinės informacijos, jeigu tai sukėlė kompiuterinės informacijos kopijavimą. Specialiojoje literatūroje nurodoma, kad Rusijos mokslininkų tarpe egzistuoja du požiūriai, kas tai yra kompiuterinės informacijos kopijavimas. Pirmojo (siauresniojo) požiūrio šalininkai laikosi nuomonės, kad kopijavimas – tai yra perėmimas kompiuterinės informacijos iš vieno kompiuterio į kitą kompiuterį ar kokią kitą laikmeną (pvz. nukopijavimas į diskelį). Antrojo (platesnio) požiūrio šalininkai laikosi nuomonės, kad kopijavimas - tai yra informacijos perėmimas iš elektroninės saugojimo priemonės į bet kurią kitą (pvz. perrašant ranka, nufotografuojant ir pan.).[66] Mes

[66] Мазуров В. А. Компьютерные преступления: классификация и способы противодействия. Москва: Логос, 2002, p.107.

pritartume pirmojo požiūrio šalininkams, nes, mūsų nuomone, pagal antrąjį požiūrį yra apimamos daug platesnis nusikalstamų veikų spektras negu tik elektroniniai nusikaltimai.

3.3. Baudžiamoji atsakomybė už neteisėtą prieigą prie informacinės sistemos ir poveikį jai

Lietuvoje baudžiamoji atsakomybė už neteisėtą prieigą prie informacinių sistemų nustatyta LR BK 198(1) str. „Neteisėtas prisijungimas prie informacinės sistemos“.

LR BK 198(1) str. 1 d. numatoma baudžiamoji atsakomybė už neteisėtą prisijungimą prie informacinės sistemos pažeidžiant informacinės sistemos apsaugos priemones, LR BK 198(1) str. 2 d. numatoma baudžiamoji atsakomybė už neteisėtą prisijungimą prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos.

Pagrindinis neteisėto prisijungimo prie informacinės sistemos nusikaltimo objektas yra informacinių sistemų bei jose esančių elektroninių duomenų saugumas (konfidencialumas), o dalykas yra informacinė sistema.

LR BK 198(1) str. numatyto nusikaltimo objektyvioji pusė gali būti apibrėžiama kaip neteisėtas prisijungimas prie informacinės sistemos pažeidžiant informacinės sistemos apsaugos priemones.

Kaip matyti iš straipsnio dispozicijos, tokio pobūdžio veika pripažįstama nusikalstama, jeigu ją realizuojant įvykdomos dvi esminės sąlygos:

1. prie informacinės sistemos prisijungiama neteisėtai, t.y. neturint informacinės sistemos savininko ar teisėto valdytojo leidimo atlikti tokius veiksmus;

2. nusikalstama veika padaroma ne bet kaip, o konkrečiu straipsnio dispozicijoje numatytu būdu – prie informacinės sistemos prisijungiama pažeidžiant informacinės sistemos apsaugos priemones.

Kad turi būti įvykdytos šios dvi esminės sąlygos patvirtina ir teismų praktika. Vilniaus miesto 1 apylinkės teismas, konstatavo, kad yra visiškai įrodyta, kad T.Č. padarė nusikalstamą veiką, numatytą LR BK 198 str. 1 d., nes „*T.Č. laikotarpiu nuo 2010 m. spalio 13 d. iki 2010 m. gruodžio 8 d., AB SEB banko patalpose, per jo darbo vietoje esantį kompiuterį „DELL Optiplex 745“, nenustatyta programine įranga, nustatęs ir vėliau (ikiteisminio tyrimo nenustatytu laiku) savavališkai pakeitęs prisijungimo prie AB SEB banko tarnybinėse stotyse administruojamos neviešos informacinės sistemos administratoriaus slaptažodį, 2011 m. balandžio 13 d. 12 val. 01 min. neteisėtai, t.y. neturėdamas šios informacinės sistemos savininko ar teisėto valdytojo leidimo*

jungtis prie šios informacinės sistemos, tyčia, pažeisdamas šios sistemos apsaugos priemones, prisijungė prie šios banko informacinės sistemos kaip neribotą prieigos teisę turintis vartotojas.“[67]

Kalbant apie subjektyviąją tokios nusikalstamos veikos pusę, reikia pabrėžti, jog kaltės forma galima tik tiesioginė tyčia. Asmuo suvokia, kad neteisėtai prisijungia prie informacinės sistemos pažeisdamas jos apsaugos priemones ir nori taip daryti.

Šios nusikalstamos veikos subjektas – pakaltinamas fizinis asmuo, kuriam iki nusikaltimo padarymo buvo suėję šešiolika metų. Be to, už šiuos nusikaltimus atsako taip pat ir juridinis asmuo pagal LR BK 20 str. nustatytas juridinio asmens baudžiamosios atsakomybės sąlygas.

Nusikalstamos veikos, už kurias numatyta baudžiamoji atsakomybė pagal 198^{1} str., vadovaujantis BK 11 str. 3 dalimi priskirtinos nesunkių nusikaltimų grupei.

LR BK $198^{(1)}$ str. 1 d. sankcijoje numatyta, kad už neteisėtą prisijungimą prie informacinės sistemos gali būti skiriamos šios alternatyvios bausmės: viešieji darbai arba bauda, arba areštas, arba laisvės atėmimas iki vienerių metų; o LR BK $198^{(1)}$ str. 2 d. sankcijoje numatyta, kad už neteisėtą prisijungimą prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos gali būti skiriama - bauda arba areštas, arba laisvės atėmimas iki trejų metų.

Kaip matyt iš 3 lentelės, nuo 2009 m. į teismus patenka stabilus ir net didėjantis bylų pagal LR BK $198^{(1)}$ str. skaičius, taigi galima daryti išvadą, kad šis straipsnis realiai pritaikomas praktikoje ir tokiu atveju jį taip pat galima priskirti prie vieno iš dažniausių straipsnių, pagal kurį pritaikoma baudžiamoji atsakomybė už elektroninius nusikaltimus.

3 Lentelė. 2007 - 2011 metais I instancijos teismuose gautos ir išnagrinėtos bylos pagal $198^{(1)}$ str.

Metai	**Nebaigtų bylų likutis ataskaitinio laikotarpio pradžioje**	**Gauta bylų**	**Baigta bylų**	**Nebaigtų bylų likutis ataskaitinio laikotarpio pabaigoje**	**Bylų nagrinėjimo trukmė**		
					Iki 6 mėnesių	**Nuo 6 iki 12 mėnesių**	**12 mėnesių ir ilgiau**
2011	1	7	6	2	6	0	0
2010	0	5	4	1	4	0	0
2009	1	5	6	0	5	0	1
2008	0	0	0	0	0	0	0
2007	0	0	0	0	0	0	0

Šaltinis: Teismų statistika http://www.teismai.lt/lt/teismai/teismai-statistika

[67] Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje Nr. 1-1430-276/2011

Pažymėtina, kad pagal RF BK kompiuterinė informacija turi būti suprantama kaip informacija (žinutės, duomenys), pateikta elektroninių signalų pagalba, nepriklausomai nuo jų laikymo, perdirbimo ar perdavimo būdų, todėl manome, kad ši sąvoka neapima „informacinių sistemų„ sąvokos. Tokiu atveju galima daryti išvadą, kad RF BK nėra nustatyta baudžiamoji atsakomybė už neteisėtą prisijungimą prie informacinės sistemos.

Lietuvoje baudžiamoji atsakomybė už neteisėtą poveikį informacinei sistemai gali kilti pagal LR BK 197 str. "Neteisėtas poveikis informacinei sistemai".

LR BK 197 str. 1 d. numatyta baudžiamoji atsakomybė už neteisėtą informacinės sistemos darbo sutrikdymą ar nutraukimą, sukėlusį didelę žalą, o šio straipsnio 2 d. numatyta baudžiamoji atsakomybė už tą pačią veiką informacinėms sistemoms, turinčioms strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai.

Nusikalstamos veikos objektas - informacinių sistemų tvarkingas funkcionavimas ar valdymas.

Nusikalstamos veikos, numatytos šio straipsnio 1 d., dalykas - bet kokia informacinė sistema, o šio straipsnio 2 d. - tik strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos. Įstatymų leidėjas nėra pateikęs informacinės sistemos sąvokos. *Informacinė sistema - techninių ir programinių priemonių visuma, naudojama informacijai kurti, siųsti, priimti, išsaugoti ar kitaip tvarkyti elektroniniu būdu. Tai itin plati sąvoka, kuri praktiškai apima tiek patį kompiuterį, tiek kompiuterių sistemas ar kompiuterinius tinklus. <...> Įstatymų leidėjas BK pasirinko plačiausią įmanomą informacinės sistemos apibrėžimą, t. y. technologiškai neutralų, neatsižvelgiant į konkrečiu laiko momentu egzistuojančias informacines technologijas ar jų įvairovę*[68].

LR BK 197 str. numatytos nusikalstamos veikos objektyvioji pusė gali pasireikšti šiais alternatyviais veiksmais:

- neteisėtas (t.y. asmuo teisėto informacinės sistemos savininko ar valdytojo nėra įgaliotas atlikti nurodytų veiksmų) informacinės sistemos darbo sutrikdymas;
- neteisėtas informacinės sistemos darbo nutraukimas.

Kiekvienu iš šių atvejų būtina, kad kiltų padariniai - informacinės sistemos darbo sutrikimas ar nutrūkimas ir tai sukeltų realią didelę žalą. Be to, analogiškai kaip ir LR BK 196 str. nusikalstama veika gali pasireikšti tik aktyviais (-iu) veiksmais (-u) (veikimu) ir šie (-is) veiksmai (-as) privalo būti neteisėti. Taip pat būtina, kad būtų nustatytas priežastinis ryšys tarp atliktų

[68] Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis. II tomas. Vilnius, VĮ „Registrų centras", 2009, p.426.

draudžiamų veiksmų ir atsiradusios didelės žalos. Didelės žalos sampratos problema jau buvo aptarta analizuojant LR BK 196 str., todėl daugiau nebesikartosime.

Šios nusikalstamos veikos subjektyviajai pusei būdinga kaltės forma yra tyčia, tiek tiesioginė, tiek netiesioginė.

Šios nusikalstamos veikos subjektas – pakaltinamas fizinis asmuo, kuriam iki nusikaltimo padarymo buvo suėję šešiolika metų. Be to, už šiuos nusikaltimus atsako taip pat ir juridinis asmuo pagal LR BK 20 str. nustatytas juridinio asmens baudžiamosios atsakomybės sąlygas.

Sankcijoje už neteisėtą poveikį informacinei sistemai nustatytos šios alternatyvios bausmės - bauda, arba areštas arba laisvės atėmimas iki ketverių metų; už neteisėtą poveikį strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiai informacinei sistemai - bauda arba areštas, arba laisvės atėmimas iki šešerių metų.

Atkreiptinas dėmesys, kad tiek 197 str. 2 d., tiek LR BK $198^{(1)}$ str. 2 d. numatyto nusikaltimo pavojingumą didina specialus nusikaltimo dalykas – informacinė sistema, turinti strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansinei sistemai. Manome, kad įvertinus tai, jog įvykdžius tiek 197 str. 2 d., tiek LR BK $198^{(1)}$ str. 2 d. nustatytą nusikalstamą veiką yra padaroma žala tokiems esminiams valstybės interesams kaip viešasis saugumas, valstybės valdymas, valstybės ekonominiai, finansiniai interesai ir kt., ji turėtų būti netoleruojama. Siekiant užtikrinti maksimalų taikomų sankcijų veiksmingumą, proporcingumą ir atgrasomumą už minėtos nusikalstamos veikos atlikimą turėtų būti baudžiama griežtai. Mūsų nuomone, tiek 197 str. 2 d., tiek LR BK $198^{(1)}$ str. 2 d. šiuo metu numatyta alternatyvi sankcija – bauda, yra pernelyg švelni ir neadekvati padaromam nusikaltimui, todėl siūlytume tiek 197 str. 2 d., tiek LR BK $198^{(1)}$ str. 2 d sankcijoje panaikinti galimybę skirti baudą.

Kadangi analogiškai kaip ir aukščiau aptarto LR BK 196 str. atveju, taip ir nagrinėjamo LR BK 197 str. atveju įstatymų leidėjas nėra pateikęs vartojamų sąvokų išaiškinimo, taip pat yra nustatęs, kad už straipsnyje numatytą nusikalstamą veiką gali būti taikomos alternatyvios sankcijos, tai didelę įtaką kaip šis straipsnis yra įgyvendinamas realiame gyvenime turi teismų praktika. Žemiau pateikiame lentelę apie 2007 - 2011 metais I instancijos teismuose gautas ir išnagrinėtas bylas pagal LR BK 197 str.

4 Lentelė. 2007 - 2011 metais I instancijos teismuose gautos ir išnagrinėtos bylos pagal 197 str.

Metai	Nebaigtų bylų likutis ataskaitinio laikotarpio pradžioje	Gauta bylų	Baigta bylų	Nebaigtų bylų likutis ataskaitinio laikotarpio pabaigoje	Bylų nagrinėjimo trukmė		
					Iki 6 mėnesių	Nuo 6 iki 12 mėnesių	12 mėnesių ir ilgiau
2011	0	3	2	1	2	0	0
2010	0	1	1	0	1	0	0
2009	0	0	0	0	0	0	0
2008	0	0	0	0	0	0	0
2007	0	0	0	0	0	0	0

Šaltinis: Teismų statistika http://www.teismai.lt/lt/teismai/teismai-statistika

Akivaizdu, kad situacija su bylų pagal LR BK 197 str. patekimu į teismą yra labai bloga – trejus metus nei viena tokio pobūdžio byla nebuvo nagrinėjama I instancijos teisme, o per paskutiniuosius dvejus metus iš viso tik keturios bylos buvo nagrinėjamos šiuose teismuose. Prielaidos dėl ko taip gali būti jau buvo aptartos šio darbo 3.1. skyriuje, todėl nesikartosime. Neabejotinai galima daryti išvadą, kad teismų praktika nagrinėjant bylas pagal LR BK 197 str. dar tik formuojasi, todėl akivaizdu, kad turės praeiti dar pakankamai ilgas laiko tarpas kol bus suformuota bendra praktika, kuria galės remtis tiek ikiteisminio tyrimai pareigūnai, tiek kiti teismai, nagrinėjantys panašaus pobūdžio bylas.

Kaip jau minėjome nagrinėdami neteisėtos prieigos prie informacinių sistemų kriminalizavimą, pagal RF BK kompiuterinė informacija turi būti suprantama kaip informacija (žinutės, duomenys), pateikta elektroninių signalų pagalba, nepriklausomai nuo jų laikymo, perdirbimo ar perdavimo būdų, todėl manome, kad ši sąvoka neapima „informacinių sistemų„ sąvokos. Taigi, galime teigti, kad RF BK taip pat nėra nustatyta baudžiamoji atsakomybė ir už neteisėtą poveikį informacinei sistemai (žinoma, kartais pažeidžiant kompiuterių sistemos naudojimo taisykles gali būti sutrikdomas ir informacinės sistemos darbas, tačiau tai nėra būtina sąlyga).

Mūsų nuomone, informacinių sistemų tvarkingas funkcionavimas yra ypač svarbus norint užtikrinti sėkmingą bet kurios įstaigos, įmonės funkcijų vykdymą, taip pat garantuoti, kad nebus pažeidžiami nei informacinių sistemų, nei jos vartotojų interesai. Pvz. sutrikdžius ar nutraukus informacinės sistemos darbą, bet kuris duomenų bankas gali pateikti atitinkamus jame saugomus duomenis ženkliai iškraipytus, ko pasekoje gali ženkliai nukentėti fizinių ar juridinių asmenų reputacija, jų finansiniai interesai, netgi valstybės viešasis saugumas (pareigūnai paleidžia sunkų

nusikaltimą padariusį asmenį, nes prisijungus prie duomenų banko nerodoma, kad tokiam asmeniui yra paskelbta paieška) ir pan. Taigi, nusikalstančio asmens padarytas poveikis informacinei sistemai gali sutrikdyti ne tik tinkamą informacinės sistemos funkcijų, kurioms yra sukurta, atlikimą, bet taip pat sukelti ir tolimesnius neigiamus padarinius jų savininkams ir vartotojams.

Tuo tarpu nusikalstamo prisijungimo prie informacinių sistemų pasekoje neretai yra susipažįstama su informacijos turiniu, kas netgi gali sąlygoti sėkmingo verslo sužlugdymą arba tokio prisijungimo pasekoje yra padaromi ir kiti nusikaltimai, pvz. pasisavinami nevieši elektroniniai duomenys.

Taigi, apibendrinant tai, kas išdėstyta galima teigti, kad prisijungimas prie informacinių sistemų ir poveikis joms yra visuomenei pavojingos veikos, sukeliančios neigiamus padarinius, todėl, mūsų nuomone, RF BK 28 skyrių būtų tikslinga papildyti straipsniais kriminalizuojančiais minėtas veikas. Be to, tokią nuomonę pagrindžia ir tarptautinių dokumentų nuostatos, rekomenduojančios kriminalizuoti tiek neteisėtą prisijungimą prie informacinės sistemos, tiek ir neteisėtą poveikį informacinei sistemai, taip pat ir anksčiau darbe pateikta Lietuvos I instancijos teismuose nagrinėjamų bylų statistika (198$^{(1)}$ str. galima priskirti prie vieno iš dažniausių straipsnių, pagal kurį pritaikoma baudžiamoji atsakomybė už elektroninius nusikaltimus).

3.4. Baudžiamoji atsakomybė už netinkamą įtaisų naudojimą

Lietuvoje baudžiamoji atsakomybė už netinkamą įtaisų naudojimą yra nustatyta LR BK 198$^{(2)}$ str. „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis“.

LR BK 198$^{(2)}$ str. numatyta baudžiamoji atsakomybė už neteisėtą įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų, tiesiogiai skirtų daryti nusikalstamas veikas, gaminimą, gabenimą, pardavimą ar kitokį platinimą arba jų įgijimą ar laikymą turint tikslą daryti nusikalstamas veikas.

Šiame straipsnyje numatytos nusikalstamos veikos objektas yra elektroninių duomenų ir informacinių sistemų saugumas, asmens privataus gyvenimo neliečiamumas, asmenų turtinės teisės ir turtiniai interesai, finansų sistema ir pan.

Nusikalstamos veikos dalykas - įrenginiai ar programinė įranga, taip pat slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys, tiesiogiai skirti ar pritaikyti nusikalstamoms veikoms daryti. *Įrenginiai yra įrengtas sudėtingas mechanizmas. Šiais įrenginiais gali būti įvairūs informacijos šifravimui, dešifravimui, kopijavimui, skenavimui, prisijungimui prie kompiuterio ar kompiuterinio tinklo ar kitokiems veiksmams atlikti skirti elektroniniai prietaisai ar įtaisai. Programinė įranga - įvairūs kompiuterių virusai („Trojos arkliai", loginės „bombos", „kirminai" ir*

kt.), taip pat informacijos šifravimui (dešifravimui), skenavimui, rinkimui, kopijavimui, kompiuterinių tinklų stebėjimui ir panašiems veiksmams skirtos programos. Slaptažodžiai, prisijungimo kodai ir kitokie panašūs duomenys - visi duomenys, įgalinantys atlikti veiksmus, kuriuos atitinkama informacinė sistema atpažįsta kaip savus ir autentifikuoja asmenį kaip teisėtą sistemos vartotoją.“[69]

Nusikalstamos veikos objektyvioji pusė gali pasireikšti šiais alternatyviais veiksmais: įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų, tiesiogiai skirtų nusikalstamoms veikoms daryti neteisėtu gaminimu, gabenimu, pardavimu ar kitokiu platinimu, taip pat jų įgijimu ar laikymu turint tą patį tikslą. Padarius bent vieną iš šių veiksmų taikoma baudžiamoji atsakomybė.

Iš LR BK 198$^{(2)}$ straipsnio dispozicijos matyti, kad tokio pobūdžio veika pripažįstama nusikalstama, jeigu ją realizuojant įvykdomos dvi esminės sąlygos:

1.turi būti disponuojama tokiais įrenginiais ar programine įranga, slaptažodžiais, prisijungimo kodais ar kitokiais panašiais duomenimis, kurie yra tiesiogiai skirti ar pritaikyti nusikalstamoms veikoms daryti;

2.disponavimas turi būti neteisėtas.

Pažymėtina, kad pagal šį straipsnį nėra baudžiama už gaminimą ar kitokį disponavimą įrenginiais ar programine įranga, taip pat slaptažodžiais, prisijungimo kodais ar kitokiais panašiais duomenimis, skirtais sankcionuotam duomenų panaudojimui ar sankcionuotam informacinių sistemų tikrinimui ar jų apsaugai.

Atkreiptinas dėmesys, kad pagal šį straipsnį taip pat nebūtina, kad tokios produkcijos pagalba būtų realiai padarytos nusikalstamos veikos, ar tokių nusikalstamų veikų pasekoje kiltų kokios nors socialiai ar materialiai neigiamos pasekmės. Taip pat nebūtina, kad atitinkamą produkciją pagaminęs asmuo, pats šios produkcijos pagalba ir vykdytų nusikalstamas veikas. Baudžiamajai atsakomybei kilti užtenka vien neteisėto įrenginių ar programinės įrangos, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų, tiesiogiai skirtų daryti nusikalstamas veikas, disponavimo fakto.

Štai Vilniaus mieto apylinkės teismas pripažino J.P. kaltu pagal LR BK 198^2 str. 1 d. ir skyrė jam 10 MGL (1300 lt) dydžio baudą už tai, kad jis personaliniu kompiuteriu sukūrė netikrą AB bankas „X" internetas bankininkystės paslaugos „X.net“ puslapį, skirtą fiksuoti šio banko klientų prisijungimų prie elektroninės bankininkystės paslaugos tarnybinės stoties kodus ir slaptažodžius, o vėliau - persiųsti juos internetu į sukurtas elektroninio pašto dėžutes ir taip pagamino programinę įrangą, skirtą nusikaltimams daryti, o būtent vykdyti nusikalstamas veikas,

[69] Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis. II tomas. Vilnius, VĮ „Registrų centras“ 2009, p.438.

numatytas LR BK 198[1] str., 214 str., 215 str. ir 182 str. Vėliau jis minėtą netikrą AB bankas „X" interneto puslapį internetu persiuntė M.J. ir taip neteisėtai jam perdavė programinę įrangą, skirtą nusikaltimams daryti.[70] Taigi, nors J.P. pats ir nevykdė nusikalstamų veikų naudodamasis savo neteisėtai sukurta programine įranga, tačiau vien už tokios įrangos pagaminimą ir perdavimą kitam asmeniui jo veikla yra kvalifikuojama pagal LR BK 198[2] str.

Šio nusikaltimo subjektyviajai pusei būdinga kaltės forma yra tiesioginė tyčia.

Šios nusikalstamos veikos subjektas – pakaltinamas fizinis asmuo, kuriam iki nusikaltimo padarymo buvo suėję šešiolika metų. Be to, už šiuos nusikaltimus atsako taip pat ir juridinis asmuo pagal LR BK 20 str. nustatytas juridinio asmens baudžiamosios atsakomybės sąlygas.

Nusikalstamos veikos, už kurias numatyta baudžiamoji atsakomybė pagal 198[1] ir 198[2] str. vadovaujantis BK 11 str. 3 dalimi priskirtini nesunkių nusikaltimų grupei.

Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo, kodais ir kitokiais duomenimis gali būti baudžiamas viena iš šių alternatyvių bausmių - viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki trejų metų.

Pažiūrėjus į 5 lentelę, galima daryti išvadą, kad realiai bylos pagal šį straipsnį Lietuvos teismus pradėjo pasiekti tik 2009 metais, kai buvo gautas 8 bylos. Tačiau 2011 m. ir vėl I instancijos teisme nebuvo gauta nei viena byla pagal šį straipsnį.

5 Lentelė. 2007 - 2011 metais I instancijos teismuose gautos ir išnagrinėtos bylos pagal 198[(2)] str.

Metai	**Nebaigtų bylų likutis ataskaitinio laikotarpio pradžioje**	**Gauta bylų**	**Baigta bylų**	**Nebaigtų bylų likutis ataskaitinio laikotarpio pabaigoje**	**Bylų nagrinėjimo trukmė**		
					Iki 6 mėnesių	**Nuo 6 iki 12 mėnesių**	**12 mėnesių ir ilgiau**
2011	1	0	1	0	0	0	1
2010	1	2	2	1	2	0	0
2009	0	8	7	1	7	0	0
2008	0	0	0	0	0	0	0
2007	0	0	0	0	0	0	0

Šaltinis: Teismų statistika http://www.teismai.lt/lt/teismai/teismai-statistika

[70] Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. baudžiamasis įsakymas baudžiamojoje byloje N1-1470-88/2009.

Mūsų nuomone, į LR BK 198(2) pagal pavadinimą labiausiai yra panašus RF BK 273 straipsnis „Kenkėjiškų kompiuterinių programų sukūrimas, naudojimas ar platinimas“, taigi detaliau panagrinėsime, ar iš tiesų šie straipsniai yra tarpusavyje panašūs ir, ar juose abiejuose nustatyta baudžiamoji atsakomybė už netinkamą įtaisų naudojimą.

RF BK 273 str. 1 d. numatyta baudžiamoji atsakomybė už kompiuterinių programų arba kitos kompiuterinės informacijos sukūrimą, platinimą arba naudojimą, kurios skirtos neteisėtam kompiuterinės informacijos sunaikinimui, blokavimui, modifikavimui, kopijavimui arba kompiuterinės informacijos apsaugos neutralizavimui, RF BK 273 str. 2 d. numatyta baudžiamoji atsakomybė už tą pačią veiką, padarytą grupės iš anksto susitarusių asmenų arba organizuotos grupės arba asmens pasinaudojant savo tarnybine padėtimi, sukėlusią didelę žalą arba padarytą iš savanaudiškų paskatų, o šio straipsnio 3 d. numatyta baudžiamoji atsakomybė už tuos pačius veiksmus, numatytus šio straipsnio 1 ir 2 dalyse, jei jie sukėlė sunkias pasekmes arba sudarė sąlygas jiems atsirasti.

Šios nusikalstamos veikos objektas – kompiuterinės informacijos saugumas, neliečiamumas ir pan., taigi, mūsų nuomone, RF BK 273 str. objektas yra siauresnis lyginant su LR BK 198(2) str., nes jis fokusuotas tik į nusikalstamas veikas prieš kompiuterinės informacijos saugumą, kai tuo tarpu LR BK 198(2) str. objektas apima ne tik elektroninių duomenų, bet ir informacinių sistemų saugumą, taip pat ir asmens privataus gyvenimo neliečiamumą, asmenų turtines teises, finansų sistemą ir pan.

RF BK 273 str. bendrasis dalykas – kenkėjiškos kompiuterinės programos ar kita kompiuterinė informacija, skirta neteisėtam kompiuterinės informacijos sunaikinimui, blokavimui, modifikavimui, kopijavimui arba kompiuterinės informacijos apsaugos neutralizavimui.

Specialiojoje literatūroje išsiskiria mokslininkų nuomonės, kas tai yra „kenkėjiškos kompiuterinės programos“. Išsiskiria nemaža dalis autorių, kurie tapatina sąvokas „kenkėjiškos programos“ ir „kompiuteriniai virusai“.

С. В. Полубинская ir С. В. Бородулин nurodo, kad RF BK 273 str. „..kalbama apie taip vadinamų kompiuterinių virusų kūrimą ir platinimą, sukuriant atitinkamas kompiuterines programas, o taip pat atliekant pakeitimus jau esančiose kompiuterinėse programose“. Mūsų nuomone, su tokiu požiūriu sutikti negalima, nes šiuolaikiniame pasaulyje egzistuoja daug daugiau įvairių kenkėjiškų programų, o ne tik „virusai“, taigi sulyginant sąvokas „kenkėjiškos programos“ ir „virusai“ yra pernelyg susiaurinamas RF BK 273 str. numatytos nusikalstamos veikos dalykas.

А. Г. Волеводз nurodo, kad sąvoka, „kenkėjiškos programos“ suprantama kaip programos, specialiai sukurtos sutrikdyti normalų kompiuterinių programų (be kurių negalimas tolimesnis elektroninių skaičiavimo mašinų, sistemų ir tinklų funkcionavimas) funkcionavimą.[71]

[71] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: Юрлитинформ, 2002, p. 73.

Ю.И. Ляпунов и А.В. Пушкин nurodo, kad kenkėjiška programa suprantama kaip specialiai parašyta (sukurta) programa, kurią naudojant galima atlikti nesankcionuotus veiksmus ir to pasekoje padaryti žalą informacijos savininkui arba valdytojui, o taip pat kitiems asmenims sunaikinant, blokuojant, modifikuojant ar kopijuojant informaciją[72]. Mes pritartume būtent šių autorių išsakomai pozicijai.

Labiausiai paplitusiomis kenkimo programomis laikomos: kompiuterių virusai, „Trojos arkliai“, „loginės bombos“ ir kt.[73].

Lieka neaišku, ką įstatymo leidėjas norėjo pasakyti sąvoka „kita kompiuterinė informacija“ – ar ši sąvoka galėtų kaip Lietuvos atveju, apimti slaptažodžius, prisijungimo kodus ir pan.? Šis klausimas kol kas dar lieka atviras, kadangi naujoji RF BK 273 str. straipsnio redakcija galioja vos keletą mėnesių dar nėra nei teismų praktikos, nei mokslininkų komentarų, kuriais remiantis būtų galima teikti šios sąvokos išaiškinimą.

Nusikalstamos veikos objektyvioji pusė gali pasireikšti šiais alternatyviais veiksmais:

- kompiuterinių programų arba kitos kompiuterinės informacijos, skirtos neteisėtam kompiuterinės informacijos sunaikinimui, blokavimui, modifikavimui, kopijavimui arba kompiuterinės informacijos apsaugos neutralizavimui, sukūrimas;
- kompiuterinių programų arba kitos kompiuterinės informacijos, skirtos neteisėtam kompiuterinės informacijos sunaikinimui, blokavimui, modifikavimui, kopijavimui arba kompiuterinės informacijos apsaugos neutralizavimui platinimas;
- kompiuterinių programų arba kitos kompiuterinės informacijos, skirtos neteisėtam kompiuterinės informacijos sunaikinimui, blokavimui, modifikavimui, kopijavimui arba kompiuterinės informacijos apsaugos neutralizavimui, naudojimas.

Pirmieji du veiksmai, kuriais gali pasireikšti objektyvioji pusė, yra ganėtinai panašūs į veiksmus, kuriais gali pasireikšti LR BK $198^{(2)}$ str. objektyvioji pusė. Tačiau trečiasis veiksmas, kuriuo gali pasireikšti RF BK 273 str. objektyvioji pusė, yra visiškai skirtingas nuo LR BK $198^{(2)}$ str. objektyviosios pusės, - numatoma atsakomybė už kompiuterinių programų arba kitos kompiuterinės informacijos, skirtos neteisėtam kompiuterinės informacijos sunaikinimui, blokavimui, modifikavimui, kopijavimui arba kompiuterinės informacijos apsaugos neutralizavimui naudojimą. Pvz. neretai dažnas kompiuterio naudotojas gauna virusais užterštus laiškus, kuriuos, neturėdamas jokių piktų kėslų ir net nežinodamas apie jų kenksmingumą, persiunčia kitiems ir tokiu būdu jau naudoja kenkėjišką programą. Ar toks asmuo gali būti traukiamas baudžiamojon atsakomybėn? Skaitant RF BK 273 str. dispoziciją pažodžiui atrodytų, kad atsakymas turėtų būti -

[72] Уголовное право. Особенная часть / под редакцией Н.И. Ветрова, Ю.И. Ляпунова. Москва, 1998, p. 554.
[73] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: Юрлитинформ, 2002, p. 73.

taip. Tokiu atveju, tenka suabejoti, ar tikrai tinkamai yra sukonstruota šio straipsnio dispozicija, nes vadovaujantis tokia logika, vos ne kiekvienas kompiuterio naudotojas gali būti traukiamas baudžiamojon atsakomybėn. Mūsų nuomone, šiuo atveju daug geriau yra sukonstruota LR BK $198^{(2)}$ str. dispozicija, pagal kurią baudžiamoji atsakomybė kyla tik už tikslingą neteisėtą kenkėjiškų programų ir kitų kompiuterinių duomenų gaminimą, gabenimą, pardavimą ar kitokį platinimą, taip pat jų įgijimą ir laikymą.

Iš RF BK 273 str. straipsnio dispozicijos matyti, kad tokio pobūdžio veika pripažįstama nusikalstama, jeigu ją realizuojant įvykdomos dvi esminės sąlygos (iš esmės tokios pačios, kokios yra numatytos ir LR BK $198^{(2)}$ str. dispozicijoje):

1. turi būti disponuojama tokiomis kompiuterinėmis programomis arba kita kompiuterine informacija, kurie yra tiesiogiai skirta nusikalstamoms veikoms daryti;

2. disponavimas turi būti neteisėtas, t.y. turi būti įvykdytas nesankcionuotas kompiuterinės informacijos sunaikinimas, blokavimas, modifikavimas, kopijavimas arba kompiuterinės informacijos apsaugos neutralizavimas.

Pažymėtina, kad pagal šį straipsnį, taip pat kaip ir pagal LR BK $198^{(2)}$ str., nereikalaujama, kad kiltų realūs neigiami padariniai, užtenka ir kenkėjiškų kompiuterinių programų arba kitos kompiuterinės informacijos sukūrimo ar disponavimo fakto.

RF BK 273 str. nusikaltimo subjektyvioji pusė – tik tiesioginė tyčia, lygiai taip pat kaip ir LR BK $198^{(2)}$ str. atveju.

RF BK 273 str. 2 ir 3 dalyje yra numatytos sunkinančios aplinkybės, dėl kurių nusikaltimas yra laikomas sunkesniu, ko pasekoje už jį yra numatomos griežtesnės sankcijos, ir jas įstatymo leidėjas susieja su:

- Nusikaltimo subjektu ir nusikaltimo padariniais arba nusikaltimo subjektyviąja puse (būtinos abi sąlygos):

  -nusikalstama veika padaroma grupės iš anksto susitarusių asmenų;

  -nusikalstama veika padaroma organizuotos grupės. Pagal LR BK 60 str. jei veiką padarė bendrininkų ar organizuota grupė, tai skiriant bausmę visada laikoma sunkinančia aplinkybe;

  -nusikalstama veika padaroma asmens pasinaudojant savo tarnybine padėtimi;

  -nusikalstama veika sukėlė didelę žalą;

  -nusikalstama veika padarytą iš savanaudiškų paskatų.

- Vien su nusikaltimo padariniais:

  -nusikalstama veika sukėlė sunkias pasekmes arba sudarė sąlygas joms atsirasti.

Tuo tarpu LR BK $198^{(2)}$ str. nenumatyta jokių sunkinančių aplinkybių. Manytume, kad ir LR BK $198^{(2)}$ str. būtų tikslinga nustatyti papildomą kvalifikuojantį požymį (kaip tai yra padaryta RF

BK 273 str.) – jei nusikalstama veika padaroma asmens pasinaudojant savo tarnybine padėtimi. Detalesnis pagrindimas, kodėl tai reikėtų padaryti jau buvo pateiktas šio darbo 3.1. poskyryje nagrinėjant baudžiamosios atsakomybės už neteisėtą prieigą prie elektroninių duomenų ir poveikį jiems klausimą, todėl šioje dalyje nesikartosime.

RF BK 273 str. numatytos nusikalstamos veikos subjektas – pakaltinamas pilnametis fizinis asmuo. Tačiau skirtingai negu LR BK 198(2) str., RF BK 272 str. nėra nustatyta, kad baudžiamojon atsakomybėn gali būti traukiami ir juridiniai asmenys. Tuo atveju, jeigu neteisėtą veiką atlieka juridinio asmens atstovas, tai šiam fiziniam asmeniui tiesiogiai ir tenka atsakomybė.

Vadovaujantis RF BK 15 str. 2 d. nusikalstamos veikos, už kurias numatyta baudžiamoji atsakomybė pagal 273 str. 1 d., 2 d. ir 3 d., priskirtinos apysunkių nusikaltimų grupei.

RF BK 273 str. 1 d. sankcijoje nustatytos šios alternatyvios bausmės - laisvės apribojimas iki keturių metų arba priverčiamieji darbai iki keturių metų arba laisvės atėmimas tam pačiam terminui su bauda iki dviejų šimtų tūkstančių rublių arba gauto atlyginimo dydžio, arba kitokių nuteistojo pajamų, gautų iki aštuoniolikos mėnesių laikotarpyje, dydžio, RF BK 273 str. 2 d. - laisvės apribojimas iki keturių metų arba priverčiamieji darbai iki penkių metų kartu su teisės užimti tam tikras pareigas ar verstis tam tikra veikla iki trijų metų atėmimu ar be atėmimo arba laisvės atėmimas iki penkių metų su bauda nuo vieno šimto tūkstančių iki dviejų šimtų tūkstančių rublių ar gauto atlyginimo dydžio ar kitokių nuteistojo pajamų, gautų nuo dvejų iki trejų metų laikotarpyje, dydžio arba be baudos, su teisės užimti tam tikras pareigas arba verstis tam tikra veikla iki trijų metų atėmimu, arba be atėmimo, RF BK 273 str. 3 d. - laisvės atėmimas iki septynerių metų. Palyginus su LR BK 198(2) str. numatyta sankcija, galima daryti išvadą, kad Rusijoje už šį nusikaltimą yra numatytos griežtesnės bausmės (pvz. Rusijoje maksimali laisvės atėmimo bausmė gali būti septyneri metai, o Lietuvoje – treji metai), be to, RF BK 273 str. skirtingai negu atitinkamo LR BK straipsnyje yra numatyta „dvigubų bausmių“ galimybė (pvz. laisvės atėmimas ir bauda).

3.5. Baudžiamoji atsakomybė už eksploatacijos ar prisijungimo taisyklių pažeidimus

LR BK nėra nustatyta baudžiamoji atsakomybė už nusikalstamos veikos, susijusios su eksploatacijos ar prisijungimo taisyklių pažeidimu, padarymą. Tačiau baudžiamoji atsakomybė už eksploatacijos ar prisijungimo taisyklių pažeidimus gali kilti pagal RF BK 274 str. „Kompiuterinės informacijos ir informacinės-telekomunikacijos tinklų saugojimo, perdirbimo ar perdavimo taisyklių pažeidimas“.

RF BK 274 str. 1 d. numatyta baudžiamoji atsakomybė už saugomos kompiuterinės informacijos arba informacinės-telekomunikacijos tinklų ir galinio įrenginio saugojimo, perdirbimo ar perdavimo priemonių eksploatacijos taisyklių pažeidimą, o taip pat prisijungimo prie informacinių-telekomunikacijos tinklų taisyklių pažeidimą, dėl ko buvo sunaikinta, blokuota,

modifikuota ar nukopijuota kompiuterinė informacija taip pat padarant didelę žalą, RF BK 274 str. 2 d. numatyta baudžiamoji atsakomybė už tą pačią veiką, jei ji sukėlė sunkias pasekmes arba sudarė sąlygas jiems atsirasti.

RF BK 274 str. objektas – saugus ir taisyklingas saugomos kompiuterinės informacijos arba informacinės-telekomunikacijos tinklų ir galinio įrenginio saugojimo, perdirbimo ar perdavimo priemonių eksploatavimas, o taip pat saugus ir taisyklingas prisijungimas prie informacinių-telekomunikacijos tinklų.

Šios nusikalstamos veikos dalykas - saugomos kompiuterinės informacijos arba informacinės-telekomunikacijos tinklų ir galinio įrenginio saugojimo, perdirbimo ar perdavimo priemonių eksploatacijos taisyklės, o taip pat prisijungimo prie informacinių-telekomunikacijos tinklų taisyklės.

RF BK 274 str. objektyvinė pusė pasireiškia veiksmais, pažeidžiančiais saugomos kompiuterinės informacijos arba informacinės-telekomunikacijos tinklų ir galinio įrenginio saugojimo, perdirbimo ar perdavimo priemonių eksploatacijos taisykles, o taip pat prisijungimo prie informacinių-telekomunikacijos tinklų taisykles.

Iš RF BK 274 str. dispozicijos matyti, kad tokia veika pripažįstama nusikalstama, jeigu ją realizuojant įvykdomos šios esminės sąlygos:

1. kyla neigiamos pasekmės – kompiuterinė informacija turi būti sunaikinta, blokuota, modifikuota ar nukopijuota ir dėl to būtinai turi kilti didelė žala;

2. turi būti nustatytas priežastinis ryšys, kad būtent dėl nusikalstančio asmens atliktos nusikalstamos veikos kilo būtinos neigiamos pasekmės.

RF BK 274 str. numatytos nusikalstamos veikos subjektas – pakaltinamas pilnametis fizinis asmuo.

Vadovaujantis RF BK 15 str. 2 d. nusikalstamos veikos, už kurias numatyta baudžiamoji atsakomybė pagal 274 str. 1 d. ir 274 str. 2 d., priskirtinos apysunkių nusikaltimų grupei.

RF BK 274 str. 1 d. sankcijoje nustatytos šios alternatyvios bausmės - bauda iki penkių šimtų tūkstančių rublių arba gauto atlyginimo dydžio, arba kitokių nuteistojo pajamų, gautų laikotarpyje iki aštuoniolikos mėnesių arba pataisos darbai nuo šešių mėnesių iki vienų metų arba laisvės apribojimas iki dvejų metų arba priverčiamieji darbai iki dvejų metų arba laisvės atėmimas tam pačiam terminui, RF BK 274 str. 1 d. - priverčiamieji darbai iki penkių metų arba laisvės atėmimas tam pačiam terminui.

Mūsų nuomone, RF BK 274 str. iš esmės skiriasi nuo LR BK XXX skyriuje įtvirtintų straipsnių. Jis yra blanketinė norma, kuri nukreipia į konkrečias taisykles, kai tuo tarpu LR BK nagrinėjamame skyriuje tokių straipsnių nėra. Tačiau iš kitos pusės manome, kad pažeidžiant saugomos kompiuterinės informacijos arba informacinės-telekomunikacijos tinklų ir galinio

įrenginio saugojimo, perdirbimo ar perdavimo priemonių eksploatacijos taisykles, o taip pat prisijungimo prie informacinių-telekomunikacijos tinklų taisykles, iš esmės dažniausiai yra įvykdomas neteisėtas prisijungimas prie informacinės sistemos arba neteisėtas poveikis šiai sistemai.

Apibendrindami tai, kas išdėstyta galime daryti išvadą, kad iš esmės tiek Lietuvoje, tiek Rusijoje didžioji dalis elektroninių nusikaltimų, už kuriuos numatyta baudžiamoji atsakomybė atitinkamos valstybės baudžiamuosiuose kodeksuose, priskiriami apysunkių nusikaltimų grupei, ir tik keletas iš jų – nesunkių nusikaltimų grupei.

Atlikus Lietuvos ir Rusijos baudžiamųjų kodeksų normų, reglamentuojančių atskirų elektroninių nusikaltimų sudėtis, analizę galima daryti išvadą, kad iš esmės tiek LR BK, tiek RF BK yra numatyta baudžiamoji atsakomybė už neteisėtą prieigą prie elektroninių duomenų, kenkėjiškų programų disponavimą, tačiau RF BK nėra numatyta tiesioginė baudžiamoji atsakomybė už neteisėtą prisijungimą prie informacinės sistemos ar neteisėtą poveikį informacinei sistemai, o LR BK – už kompiuterių sistemos naudojimo taisyklių pažeidimus.

Nors abiejose lyginamose valstybėse elektroninių nusikaltimų subjektu gali būti pakaltinamas fizinis asmuo, kuriam iki nusikaltimo padarymo buvo suėję šešiolika metų, tačiau Lietuvoje, skirtingai negu Rusijoje, baudžiamojon atsakomybėn gali būti traukiami ir juridiniai asmenys. Sankcijos už elektroninius nusikaltimus savo dydžiu ženkliai nesiskiria, tačiau už pavojingiausias nusikalstamas veikas, numatytas nagrinėtuose RF BK straipsniuose, gali būti skiriama tik laisvės atėmimo bausmė. Manome, kad įvertinus tai, jog įvykdžius tiek 196 str. 2 d., tiek 197 str. 2 d., tiek LR BK 198$^{(1)}$ str. 2 d. nustatytą nusikalstamą veiką yra padaroma žala tokiems esminiams valstybės interesams kaip viešasis saugumas, valstybės valdymas, valstybės ekonominiai, finansiniai interesai ir kt., ji turėtų būti netoleruojama, o siekiant užtikrinti maksimalų taikomų sankcijų veiksmingumą, proporcingumą ir atgrasomumą už minėtos nusikalstamos veikos atlikimą turėtų būti baudžiama griežtai. Mūsų nuomone, tiek 196 str. 2 d. , tiek 197 str. 2 d., tiek LR BK 198$^{(1)}$ str. 2 d šiuo metu numatyta alternatyvi sankcija – bauda, yra pernelyg švelni ir neadekvati padaromai nusikalstamai veikai, todėl siūlytume šių straipsnių dalių sankcijose panaikinti galimybę skirti baudą.

RF BK skirtingai negu LR BK yra numatyta daugiau galimų alternatyvių bausmių, taip pat yra numatyta „dvigubų bausmių“ galimybė (pvz. bauda kartu su laisvės atėmimu). Mūsų nuomone, sankcijoje neturėtų būti numatyta tokia didelė galimų alternatyvių bausmių įvairovė, nes tai praplečia korupcijos galimybes ikiteisminio tyrimo ir teisminio nagrinėjimo metu bei sudaro sąlygas, kad už iš esmės tapatų elektroninį nusikaltimą būtų skiriamos ženkliai skirtingos bausmės.

Pažymėtina, kad skirtingai negu LR BK pačiame RF BK yra pateiktas „kompiuterinės informacijos“ ir „didelės žalos“ sąvokų išaiškinimas, tokiu būdu išsprendžiant šių sąvokų nevienodo traktavimo problemą, o kartu ir veikos kvalifikavimo problemą. Mūsų nuomone, ir LR

BK XXX skyrių papildyti dar vienu straipsniu, kuriame būtų pateiktas labai abstrakčios sąvokos „didelė žala“ išaiškinimas, atskleidžiant tiek turtinį, tiek ir neturtinį šios sąvokos aspektus. Tokiu būdu būtų išvengta šios sąvokos nevienodo traktavimo problemos , o kartu ir veikos kvalifikavimo problemos. Juolab, kad tokia praktika pateikti sąvokos išaiškinimus pačiame LR BK yra taikoma, pvz. LR BK 190 str. yra išaiškinta turto vertė, taikoma XXVIII skyriaus nusikaltimams.

Išanalizavus per paskutinius penkerius metus, t.y. 2007 - 2011 metais, I instancijos teismuose gautų ir išnagrinėtų bylų pagal 196 str.-198[2] str. statistiką, matome, kad realiai Lietuvoje pagrindiniai ir dažniausi straipsniai, pagal kuriuos bylos patenka į teismą yra 198 ir 198[1] str. Deja, atsižvelgiant į tai, kad RF BK 28 skyriaus pakeitimai buvo padaryti vos prieš keletą mėnesių, negalime pateikti palyginimui statistikos, kiek per paskutinius penkerius metus, t.y. 2007 - 2011 metais, Rusijos I instancijos teismuose buvo gauta ir išnagrinėta bylų pagal atitinkamus straipsnius.

IŠVADOS IR PASIŪLYMAI

1. Teisinėje literatūroje ir teisės aktuose trūksta aiškaus vieningo elektroninių nusikaltimų apibrėžimo, o Lietuvos Respublikos ir Rusijos Federacijos baudžiamuosiuose įstatymuose tokia sąvoka iš viso nepateikiama, todėl tai skatina įvairių elektroninių nusikaltimų sąvokos interpretacijų atsiradimą. Nesant vieningos elektroninių nusikaltimų sampratos gali būti apsunkinamas tokių nusikalstamų veikų susekimas, tyrimas ir baudžiamasis persekiojimas tarptautiniu lygiu, elektroninių nusikaltimų sampratos įvairovė taip pat gali neigiamai veikti šių nusikaltimų plitimą. Manytume, kad baudžiamosios teisės doktrinoje, atlikus gilią analizę, būtų galima pabandyti sumodeliuoti kuo tikslesnį „elektroninio nusikaltimo“ apibrėžimą arba bent jau apsispręsti, kurios iš teisinėje literatūroje mokslininkų pateikiamų elektroninių nusikaltimų sampratos krypties reikėtų laikytis, apibrėžiant elektroninius nusikaltimus.

2. Atlikus pagrindinių tarptautinių ir regioninių dokumentų įgyvendinimo Lietuvoje ir Rusijos Federacijoje analizę, nustatyta, kad elektroninių nusikaltimų reglamentavimui Lietuvos Respublikoje įtaką daro tiek tarptautinis, tiek regioninis teisinis reglamentavimas, tuo tarpu elektroninių nusikaltimų reglamentavimui Rusijos Federacijoje jokios tarptautinės ir regioninės iniciatyvos įtakos neturi. Atsižvelgiant į tai, kad Rusijos mokslininkų tarpe vis dažniau pripažįstama Europos Tarybos konvencijos dėl elektroninių nusikaltimų, kaip ypač svarbaus tarptautinio mechanizmo, reikšmė suvienodinant valstybių įstatymus elektroninių nusikaltimų srityje ir į tai, kad Rusijos Federacijoje jau buvo padaryti pirmieji žingsniai siekiant prisijungti prie Konvencijos, tikėtina, kad Rusijos Federacija vis tik laikui bėgant prisijungs prie Konvencijos.

3. Atitinkamų teisės aktų Lietuvos Respublikos ir Rusijos Federacijos elektroninės informacijos saugos srityje analizė parodė, kad šiuo metu abiejose valstybėse yra priimti strateginiai dokumentai, kurie apibrėžia planuojamą valstybės politiką šioje srityje. Lietuvos programoje nustatyti pakankamai konkretūs ir ambicingi, kai kurie galbūt realiai netgi sunkiai įgyvendinami, tikslai, uždaviniai ir programos vertinimo kriterijai, tuo tarpu Rusijos doktrinoje nurodytų tikslų ir prioritetinių priemonių formuluotės yra ganėtinai deklaratyvios ir nekonkrečios, taip pat skirtingai negu Lietuvos programoje nenustatyta jokių vertinimo kriterijų, pagal kuriuos galima būtų spręsti, ar ši Rusijos doktrina yra sėkmingai įgyvendinama. Mūsų nuomone, siekiant formuoti ir įgyvendinti veiksmingą politiką elektroninės informacijos saugos srityje, Lietuvos programoje (kaip šiuo metu yra padaryta Rusijos doktrinoje) reikėtų aiškiai išskirti konkrečių institucijų (tiek valstybinių, tiek savivaldos institucijų) kompetencijas elektroninės informacijos saugos srityje, taip pat turėtų būti padaryta gilesnė esamos būklės analizė, įvardinant galimas grėsmes, dėl kurių atitinkami tikslai ir uždaviniai gali būti nepasiekti.

4. Abiejose lyginamose valstybėse yra daug įstatymų, kuriuose yra įtvirtintos pavienės nuostatos reglamentuojančios elektroninės informacijos saugos santykius, tačiau Rusijos Federacijoje yra priimtas vienas pagrindinis įstatymas, reguliuojantis elektroninės informacijos saugos sritį, kai tuo tarpu Lietuvoje dar iki šiol nėra priimtas įstatymas, kuriuo visapusiškai ir nuosekliai būtų reglamentuoti visuomeniniai santykiai, susiję su elektroninės informacijos sauga, nors koncepcija dėl šio įstatymo priėmimo buvo patvirtinta jau daugiau kaip prieš penkerius metus. Mūsų nuomone, siekiant užtikrinti visapusišką ir veiksmingą elektroninės informacijos saugą, būtina kiek įmanoma greičiau patvirtinti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymą, neatidėliojant jo priėmimo dar keletui metui kaip buvo nuolat daroma iki šiol.

5. Tiek Lietuvos Respublikoje, tiek Rusijos Federacijoje didžioji dalis elektroninių nusikaltimų, už kuriuos numatyta baudžiamoji atsakomybė atitinkamos valstybės baudžiamuosiuose kodeksuose, priskiriami apysunkių nusikaltimų grupei, ir tik keletas iš jų – nesunkių nusikaltimų grupei.

6. Atlikus Lietuvos Respublikos ir Rusijos Federacijos kodekse nustatytų elektroninių nusikaltimų sudėties atskirų požymių turinio analizę nustatyta, kad iš esmės tiek LR BK, tiek RF BK yra numatyta baudžiamoji atsakomybė už neteisėtą prieigą prie elektroninių duomenų ir poveikį jiems, kenkėjiškų programų disponavimą, tačiau RF BK nėra numatyta tiesioginė baudžiamoji atsakomybė už neteisėtą prisijungimą prie informacinės sistemos ar neteisėtą poveikį informacinei sistemai, o LR BK – už kompiuterių sistemos naudojimo taisyklių pažeidimus.

7. Abiejose lyginamose valstybėse elektroninių nusikaltimų subjektu gali būti pakaltinamas fizinis asmuo, kuriam iki nusikaltimo padarymo buvo suėję šešiolika metų, tačiau Lietuvoje, skirtingai negu Rusijoje, baudžiamojon atsakomybėn gali būti traukiami ir juridiniai asmenys. Atsižvelgiant į tai, kad vis daugiau elektroninių nusikaltimų yra padaroma darbuotojų, jiems piktnaudžiaujant užimamomis pareigomis, taip pat į tai, kad tokie asmenys, kurie dėl savo užimamų pareigų turi prieigą prie svarbių elektroninių duomenų, neretai gali padaryti daug didesnę žalą atitinkamai institucijai negu kiti asmenys, manytume, kad ir LR BK XXX skyriaus straipsniuose būtų tikslinga nustatyti griežtesnę atsakomybę specialiajam subjektui – asmeniui, nusikalstamą veiką padarančiam pasinaudojant savo tarnybine padėtimi, kaip tai yra padaryta RF BK 28 skyriaus dviejuose straipsniuose.

8. Atlikus LR BK ir RF BK nustatytų elektroninių nusikaltimų sankcijų lyginamąją analizę nustatyta, kad abiejose nagrinėtose valstybėse sankcijos už elektroninius nusikaltimus savo dydžiu ženkliai nesiskiria, tačiau už pavojingiausias nusikalstamas veikas, numatytas nagrinėtuose RF BK straipsniuose, gali būti skiriama tik laisvės atėmimo bausmė. Manome, kad įvertinus tai, jog įvykdžius tiek LR BK 196 str. 2 d., tiek LR BK 197 str. 2 d., tiek LR BK $198^{(1)}$ str. 2 d. nustatytą

nusikalstamą veiką yra padaroma žala tokiems esminiams valstybės interesams kaip viešasis saugumas, valstybės valdymas, valstybės ekonominiai, finansiniai interesai ir kt. ir siekiant užtikrinti maksimalų taikomų sankcijų veiksmingumą, proporcingumą bei atgrasomumą, už minėtų nusikalstamų veikų atlikimą turėtų būti baudžiama griežtai. Mūsų nuomone, tiek 196 str. 2 d., tiek 197 str. 2 d., tiek LR BK $198^{(1)}$ str. 2 d šiuo metu numatyta alternatyvi sankcija – bauda, yra pernelyg švelni ir neadekvati padaromai nusikalstamai veikai, todėl siūlytume šių straipsnių dalių sankcijose panaikinti galimybę skirti baudą.

Taip pat nustatyta, kad RF BK skirtingai negu LR BK yra numatyta daugiau galimų alternatyvių bausmių, taip pat yra numatyta „dvigubų bausmių“ galimybė (pvz. bauda kartu su laisvės atėmimu). Mūsų nuomone, sankcijoje neturėtų būti numatyta tokia didelė galimų alternatyvių bausmių įvairovė, nes tai praplečia korupcijos galimybes ikiteisminio tyrimo ir teisminio nagrinėjimo metu bei sudaro sąlygas, kad už iš esmės tapatų elektroninį nusikaltimą būtų skiriamos ženkliai skirtingos bausmės.

9. RF BK, skirtingai negu LR BK, yra pateiktas nagrinėjamų straipsnių dispozicijose vartojamų sąvokų „kompiuterinė informacija“ ir „didelė žala“ išaiškinimas. Mūsų nuomone, reikėtų ir LR BK XXX skyrių papildyti dar vienu straipsniu, kuriame būtų pateiktas labai abstrakčios sąvokos „didelė žala“ išaiškinimas, atskleidžiant tiek turtinį, tiek ir neturtinį šios sąvokos aspektus ir tokiu būdu būtų išvengiant šios sąvokos nevienodo traktavimo problemos, o kartu ir veikos kvalifikavimo problemos.

10. Išanalizavus per paskutinius penkerius metus, t.y. 2007 - 2011 metais, I instancijos teismuose gautų ir išnagrinėtų bylų pagal 196 str.- 198^{2} str. statistiką nustatyta, kad į teismus patenka labai nedaug bylų, realiai Lietuvoje pagrindiniai ir dažniausi straipsniai, pagal kuriuos bylos patenka į teismą yra 198 str. ir 198^{1} str. Deja, atsižvelgiant į tai, kad RF BK 28 skyrius buvo iš esmės pakeistas vos prieš keletą mėnesių, negalime pateikti palyginimui statistikos, kiek per paskutinius penkerius metus, t.y. 2007 - 2011 metais, Rusijos I instancijos teismuose buvo gauta ir išnagrinėta bylų pagal atitinkamus RF BK straipsnius.

LITERATŪRA

Knygos:

1. Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации. Красноярск, 2002. http://pu.boom.ru/book/index.html.

2. Brenner. S. W. Cybercrime. Criminal Threats from Cyberspace. Library of Congress Cataloging, 2010.

3. Civilka M., Lamanauskas T., Nosinaitė G., Sauliūnas D., Štitilis D., Toliušis S., Ulevičius L. Informacinių technologijų teisė. Vilnius: Teisės Institutas, 2004.

4. Дремлюга Р.И. Интернет преступность. Владивосток: Издательство Дальневосточного университета, 2008. http://www.telecomlaw.ru/monograph/Internet_crime_Dremlyga.pdf

5. Higgins George E. Cybercrime: an introduction to an emerging phenomenom. New York: McGraw-Hill, 2010.

6. Kiškis M., Štitilis D., Rotomskis I., Petrauskas R. Teisės informatika ir informatikos teisė: vadovėlis. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006.

7. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis. II tomas. Vilnius, VĮ „Registrų centras“, 2009.

8. Мазуров В. А. Компьютерные преступления: классификация и способы противодействия. Москва: Логос, 2002.

9. Piesliakas V. Lietuvos baudžiamoji teisė. Pirmoji knyga. Vilnius: Justitia, 2006.

10. Преступления в сфере компьютерной информации: квалификация и доказывание: учебное пособие /под редакцией Ю. В. Гаврилина. Москва: Книжный мир,2003.

11. Рассолов И.М. Право и Интернет. http://tawkataw.ucoz.ru/_ld/1/105_pravo_i_interne.pdf

12. Российское уголовное право. Особенная часть /под редакцией В.П. Кудрявцева, А.В. Наумова. Москва: Юрист, 1997.

13. Štitilis D. Elektroniniai nusikaltimai: metodinė priemonė. Vilnius: Mykolo Romerio universitetas, 2011.

14. Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации: научно-практическое пособие. Москва: ЛексЭст, 2004.

15. Вехов В. Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. Москва, 2000. www.cyberpol.ru/public/osobennosti_rassled.doc

16. Вехов В.Б. Компьютерные преступления: способы совершения методики расследования. Москва, 1996. http://www.pravo.vuzlib.net/book_z404_page_1.html

17. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: Юрлитинформ, 2002.

18. Уголовное право. Особенная часть / под редакцией Н.И. Ветрова, Ю.И. Ляпунова. Москва, 1998.

19. Серго А. Интернет и Право. Москва: "Бестселлер", 2003. http://internet-law.ru/book/index1.htm

20. Уголовное право. Особенная часть / под редакцией И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов. Москва: норма, 1998.

21. Уголовное право. Особенная часть / под редакцией Н.И. Ветрова, Ю.И. Ляпунова. Москва, 1998.

Straipsniai:

22. Гульбин Ю. Преступления в сфере компьютерной информации. http://www.lawmix.ru/comm/8288/

23. Карелина М.М. Преступления в сфере компьютерной информации. http://www.crime-research.ru/library/CodeRu.htm

24. Petrauskas R., Štitilis D. Lietuvos Respublikos baudžiamasis kodeksas nusikaltimų elektroninėje erdvėje konvencijos kontekste. Jurisprudencija, Vilnius, 2002, t. 24 (16).

24. Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. Vilnius: Lietuvos teisės akademijos Leidybos centras, 2000.

25. Мазуров В. А. П. Преступность в сфере высоких технологий: Понятие, общая характеристика,тенденции.
http://www.lib.tsu.ru/mminfo/000063105/300%28I%29/image/300_1_151-154.pdf

26. Мосин О.В. Компьютерная преступность в России. Как с ней бороться? – 2008 г. – Юридический портал «Правопорядок» . http://www.oprave.ru/statii/Informacionnoe-texts02.html

27. Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями. http://www.hackzone.ru/articles/a5.html

28. Полякова Т. А. Проблемы совершенствования правового регулирования противодействия использованию информационных технологий в преступных целях. Доклад на VII Международной конференции “Право и Интернет”. http://www.ifap.ru/pi/07/

29. Štitilis, D.; Paškauskas, Ž. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. Jurisprudencija, 2007, 2 (92).

30. Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai. Jurisprudencija, 2003, 47 (39).
31. Štitilis D., Pakutinskas P., Dauparaitė I., Laurinaitis M. Teisinė aplinka siekiant išvengti tapatybės vagystės elektroninėje erdvėje: JAV ir Lietuvos teisės aktų lyginamoji analizė. Socialinės technologijos, 2011, 1 (1).
32. Волчинская Е. К. Роль государства в обеспечении информационной безопасности. rniiis.ru/articlesip409/volchinskaya.doc
33. Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Автореферат. Москва, 2007. http://www.russianlaw.net/files/law/doc/a212.pdf

Teisės aktai:
34. Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui - Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme {SEK(2007) 641} {SEK(2007) 642}
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:LT:NOT
35. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ {SEC(2009) 399} {SEC (2009) 400} KOM (2009) 149 galutinis. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:HTML
36. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“. KOM (2011) 163 galutinis. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:LT:HTML
37. Komisijos ataskaita Tarybai parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas 12 straipsnį. KOM (2008) 0448 galutinis */
http://eur-law.eu/LT/Komisijos-ataskaita-Tarybai-parengta-2005-m-vasario-24,480987,d
38. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004, Nr. 36-1188.
39. Konvencijos dėl elektroninių nusikaltimų Papildomas protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo. Valstybės žinios, 2006, Nr. 75-2850.
40. Lietuvos Respublikos baudžiamasis kodeksas. Valstybės žinios, 2000, Nr. 89-2741; 2004, Nr. 25-760; 2007, Nr. 81-3309.
41. Lietuvos Respublikos elektroninio parašo įstatymas. Valstybės žinios, 2000, Nr. 61-1827.

42. Lietuvos Respublikos elektroninių ryšių įstatymas. Valstybės žinios, 2004, Nr. 69-2382.

43. Lietuvos Respublikos įstatymas dėl konvencijos dėl elektroninių nusikaltimų ratifikavimo. Valstybės žinios, 2004, Nr. 36- 1178.

44. Lietuvos Respublikos įstatymas dėl konvencijos dėl elektroninių nusikaltimų Papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo ratifikavimo. Valstybės žinios, 2006, Nr. 75- 2848.

45. Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“. Valstybės žinios, 2006, Nr.134-5081.

46. Lietuvos Respublikos Vyriausybės 2009 m. vasario 25 d. nutarimas Nr. 189 “Dėl Lietuvos Respublikos Vyriausybės 2008–2012 metų programos įgyvendinimo priemonių patvirtinimo”. Valstybės žinios, 2009, Nr. 33-1268.

47. Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 “Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo”. Valstybės žinios. 2011, Nr. 83-4033; 2011, Nr.106 (atitaisymas).

48. Tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:LT:HTML

49. Aiškinamasis raštas „Dėl Lietuvos Respublikos įstatymo „Dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo”, Lietuvos Respublikos baudžiamojo kodekso (Žin., 2000, 89-2741) 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 str. pakeitimo ir papildymo bei Kodekso papildymo 198^1 ir 198^2 str. įstatymo ir Lietuvos Respublikos baudžiamojo proceso kodekso (Žin., 2002, 37-1341) 154 str. papildymo įstatymo projektų. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=223058

50. Доктрина информационной безопасности Российской Федерации http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

51. Федеральный закон „Об информации, информационных технологиях и о защите информации“. http://www.rg.ru/2006/07/29/informacia-dok.html

52. Распоряжение Президента РФ от 15 ноября 2005 г. N 557-рп "О подписании Конвенции о киберпреступности". http://www.lawrussia.ru/texts/legal_712/doc712a781x217.htm

53. Распоряжение Президента РФ от 22 марта 2008 г. N 144-рп "О признании утратившим силу распоряжения Президента РФ от 15 ноября 2005 г. N 557-рп "О подписании Конвенции о киберпреступности". http://news-city.info/akty/lawbook-36/tekst-ey-civil-moskwa.htm

54. Уголовный кодекс Российской Федерации. http://www.interlaw.ru/law/docs/10008000-045.htm

55. Council of Europe. Computer-related crime. Recommendation No. R(89)9, adopted by Committee of Ministers of the Council of Europe on 13 September 1989 // Strasbourg, 1990. http://cm.coe.int/ta/rec/1989/89r9.htm
56. 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=COM:2000:0890:FIN:EN:PDF

Teismų praktika:
57. Panevėžio miesto apylinkės teismo nuosprendis 2011 m. spalio 25 d. baudžiamojoje byloje Nr. 1-187-389/2011
58. Kauno miesto apylinkės teismo 2011 m. spalio 25 d. nuosprendis baudžiamojoje byloje Nr.1-2092-246/2011
59. Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje Nr. 1A-977/2011.
60. Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje Nr. 1-1430-276/2011
61. Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. baudžiamasis įsakymas baudžiamojoje byloje N1-1470-88/2009
62. Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. baudžiamoji byla Nr. 1-515-487/2009
63. Актуальные кассационные определения по уголовным делам за период с 11 по 20 февраля 2012 года. http://oblsud.ynao.sudrf.ru/modules.php?name=press_dep&op=1&did=538
64. Приговор Дзержинского городского суда от 27 июля 2011 года Дело № (не определено). http://www.gcourts.ru/case/1446171

Interneto šaltiniai:
65. Teismų statistika http://www.teismai.lt/lt/teismai/teismai-statistika/
66.http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
67.http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG

Klišauskas V. Elektroninių nusikaltimų reglamentavimas Rusijoje ir Lietuvoje: lyginamieji aspektai / Naujų technologijų teisės magistro baigiamasis darbas. Vadovas doc. dr. Darius Štitilis. – Vilnius: Mykolo Romerio universitetas, Socialinės informatikos fakultetas, 2012. – 68 p.

SANTRAUKA

Elektroninis nusikalstamumas tapo pasauliniu reiškiniu, darančiu vis daugiau žalos atskiriems piliečiams, organizacijoms, visai visuomenei, valstybei. Dauguma pasaulio valstybių elektroninius nusikaltimus pagal jų pavojingumą ir pelningumą netgi prilygina tokioms nusikalstamoms veikoms kaip terorizmas ir prekyba narkotikais. Todėl elektroninių nusikaltimų teisinio reglamentavimo problema yra viena iš pačių aktualiausių visame pasaulyje, tame tarpe ir Lietuvoje, ir mūsų kaimynystėje esančioje Rusijoje. Iki šiol elektroninių nusikaltimų nagrinėjimas Lietuvos mokslinėje literatūroje yra pakankamai ribotas. Literatūros šaltiniuose nepavyko surasti palyginimo tarp elektroninių nusikaltimų reglamentavimo praktikos Rusijos Federacijoje ir Lietuvos Respublikoje.

Pagrindinis darbo tikslas – išanalizuoti ir tarpusavyje palyginti elektroninių nusikaltimų reglamentavimą Rusijos Federacijoje ir Lietuvos Respublikoje.

Darbą sudaro trys dalys. Pirmojoje dalyje aptariama elektroninių nusikaltimų samprata. Akcentuojama, kad teisinėje literatūroje ir teisės aktuose trūksta aiškaus vieningo elektroninių nusikaltimų apibrėžimo.

Antrojoje darbo dalyje lyginamuoju aspektu nagrinėjama pagrindinių tarptautinių ir regioninių dokumentų įgyvendinimo Lietuvos Respublikoje ir Rusijos Federacijoje praktika, elektroninių nusikaltimų teisinio reglamentavimo klausimai Lietuvos Respublikoje ir Rusijos Federacijoje. Pabrėžiama, kad elektroninių nusikaltimų reglamentavimui Lietuvos Respublikoje įtaką daro tiek tarptautinis, tiek regioninis teisinis reglamentavimas., tuo tarpu elektroninių nusikaltimų reglamentavimui Rusijos Federacijoje jokios tarptautinės ir regioninės iniciatyvos įtakos neturi. Nustatyta, kad šiuo metu abiejose valstybėse yra priimti strateginiai dokumentai, kurie apibrėžia planuojamą valstybės politiką šioje srityje, tačiau Lietuvoje trūksta įstatymo, kuriuo visapusiškai ir nuosekliai būtų reglamentuoti visuomeniniai santykiai, susiję su elektroninės informacijos sauga.

Trečiojoje dalyje analizuojamos ir tarpusavyje lyginamos Lietuvos Respublikos ir Rusijos Federacijos baudžiamųjų kodeksų nuostatos, numatančios atsakomybę už elektroninius nusikaltimus. Nustatyta, kad iš esmės tiek LR BK, tiek RF BK yra numatyta baudžiamoji atsakomybė už neteisėtą prieigą prie elektroninių duomenų ir poveikį jiems, kenkėjiškų programų disponavimą, tačiau RF BK nėra numatyta tiesioginė baudžiamoji atsakomybė už neteisėtą

prisijungimą prie informacinės sistemos ar neteisėtą poveikį informacinei sistemai, o LR BK – už kompiuterių sistemos naudojimo taisyklių pažeidimus.

Darbe, pasitelkiant dokumentų analizės, lyginamąjį bei apibendrinimo metodus, analizuojami Lietuvos ir Rusijos mokslininkų darbai, šių valstybių nacionaliniai teisės aktai dėl elektroninių nusikaltimų, Lietuvos teismuose išnagrinėtų bylų statistika pagal atitinkamus baudžiamojo kodekso straipsnius.

Klišauskas V. Cybercrime reglamentation in Russia and Lithuania: comparative aspects / New technologies law Master thesis. – Adviser - Docent Dr. Darius Štitilis. – Vilnius: Mykolo Romerio University, Faculty of Social Informatics, 2012. – 68 p.

SUMMARY

Cybercrime has become a global phenomenon, which is causing more harm to individual citizens, organizations, society and the state. Most countries in the world compare cybercrime with such offences as terrorism and drug trafficking due to its risks and profitability. Therefore, the legal regulation of cybercrime is one of the most relevant problems in the world, including Lithuania and our neighboring country Russia. So far cybercrime analysis in scientific literature has been rather limited. We have not succeeded in finding a comparison between the regulatory practices of cybercrime in the Russian Federation and the Republic of Lithuania in any of the references.

The main goal of the thesis paper is to analyze and compare the regulation of cybercrime in the Russian Federation and the Republic of Lithuania.

The paper consists of three parts. The first part deals with the concept of cybercrime. It is emphasized that the legal sources and laws lack a clear unified definition of cybercrime.

The second part analyses the main international and regional instruments implemented in practice by the Republic of Lithuania and the Russian Federation, the issues of legal regulation of cybercrime in the Republic of Lithuania and the Russian Federation. It is emphasized that the regulation of cybercrime in Lithuania is influenced by both the international and regional legal framework, while cybercrime regulation in the Russian Federation is not affected by international and regional initiatives. It was determined that recently strategic documents which define the proposed national policy in this area have been enacted in two countries, but there is a lack of law in the Lithuanian legal system which would comprehensively and consistently regulate public relations related to electronic information security.

The third part analyzes and compares criminal code provisions of the Republic of Lithuania and the Russian Federation that criminalize cybercrime. It was determined that in general both the Criminal Code of the Republic of Lithuania and the Criminal Code of the Russian Federation foresee criminal liability for unauthorized access to electronic data, the impact on it, and malware disposition, but the Criminal Code of the Russian Federation does not provide direct criminal liability for unauthorized access to the information system or illegal influence on information system. The Criminal Code of the Republic of Lithuania does not provide direct criminal liability for the violations of rules related to the use of computer systems.

Using the methods of document analysis, comparative and summative methods, scientific

works of Lithuanian and Russian scientists, the respective national legislation on cybercrime, relevant statistics of the Lithuanian court cases according to respective Criminal Code articles have been analyzed in the thesis paper.