View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Mykolas Romeris University Institutional Repository

MYKOLO ROMERIO UNIVERSITETAS

MOKSLAS • EKONOMIKA • SANGLAUDA

EUROPOS SĄJUNGA

Kuriame Lietuvos ateitį

Doc. dr. Darius Štitilis

ELEKTRONINIAI NUSIKALTIMAI

Metodinė priemonė

Mykolo Romerio universitetas

Vilnius,

2011

Metodinė priemonė išleista pagal projektą „Humanitarinių ir socialinių mokslų specialistų rengimo tobulinimas, skatinant ūkio plėtrą (HSM NKP studijos)“, projekto kodas Nr. VPI-2.2-ŠMM-09-V-01-012.

ISBN 978-9955-19-329-6

© Doc. dr. Darius Štitilis, 2011
© M. Romerio universitetas, 2011

TURINYS

PRATARMĖ 4
ĮVADAS 4
1. ELEKTRONINIS NUSIKALSTAMUMAS 5
1.1. Elektroninio nusikaltimo samprata 5
1.2. Elektroninių nusikaltimų žala ir latentiškumas 8
2. ELEKTRONINIŲ NUSIKALTIMŲ KLASIFIKACIJA, SUBJEKTAI IR ATLIKIMO BŪDAI 10
2.1. Elektroninių nusikaltimų klasifikacija 10
2.2. Elektroninių nusikaltimų subjektai 18
2.3. Elektroninių nusikaltimų atlikimo būdai 25
3. TEISINIAI ELEKTRONINIŲ NUSIKALTIMŲ ASPEKTAI 33
3.1. Elektroninių nusikaltimų reglamentavimas tarptautiniu ir ES mastu 33
3.1.1. Konvencija dėl elektroninių nusikaltimų 33
3.1.1.1. Konvencijos dėl elektroninių nusikaltimų nuostatos dėl materialinės teisės 35
3.1.1.2. Konvencijos dėl elektroninių nusikaltimų nuostatos dėl proceso teisės 39
3.1.1.3. Kitos Konvencijos dėl elektroninių nusikaltimų nuostatos 43
3.1.2. Konvencijos dėl elektroninių nusikaltimų papildomas protokolas 43
3.1.3. Tarptautinių organizacijų ir ES dokumentai dėl elektroninių nusikaltimų 45
3.2. Kai kurių užsienio valstybių baudžiamųjų įstatymų nuostatos dėl elektroninių nusikaltimų 56
3.2.1. Rusijos Federacija 56
3.2.2. Lenkija 62
3.2.3. Ukraina 64
3.2.4. Estija 67
3.2.5. Latvija 68
3.2.6. Jungtinė Karalystė 70
3.2.7. Jungtinės Amerikos Valstijos (JAV) 74
3.2.8. Kanada 77
3.2.9. Italija 79
3.2.10. Australija 80
3.2.11. Honkongas 82
3.3. Elektroninių nusikaltimų reglamentavimas Lietuvoje 83
4. ELEKTRONINIŲ NUSIKALTIMŲ PREVENCIJA 87
4.1. Elektroninių nusikaltimų tikimybė 88
4.2. Elektroninių nusikaltimų prevencijos priemonės 90
Literatūra 103
PRIEDAI 112

PRATARMĖ

Šio mokomojo leidinio tikslas – supažindinti su nauja nusikalstamumo rūšimi – elektroniniais nusikaltimais, jų keliama grėsme tiek valstybinėms įstaigoms, tiek verslui, tiek paprastiems piliečiams, ir aptarti tokių nusikaltimų prevencijos ypatumus.

Leidinyje atskleidžiamas naujo XXI amžiaus fenomeno – elektroninio nusikalstamumo – išskirtinumas iš tradicinių nusikaltimų, nagrinėjama tokių nusikaltimų sąvoka ir latentiškumas. Pateikiama elektroninių nusikaltimų klasifikacija, nagrinėjami šių nusikaltimų subjektai ir atlikimo būdai.

Leidinyje aptarti teisiniai elektroninių nusikaltimų aspektai, pristatoma Konvencija dėl elektroninių nusikaltimų, analizuojamas tokių nusikaltimų teisinis reglamentavimas Europos Sąjungoje, užsienio valstybėse ir Lietuvoje.

Labai svarbus šio leidinio elektroninių nusikaltimų prevencijos skyrius, kuriame analizuojama elektroninių nusikaltimų tikimybė bei tokių nusikaltimų prevencijos priemonės.

ĮVADAS

Technologijų vystymas sąlygojo ir įvairių nusikalstamo elgesio formų atsiradimą bei plitimą[1]. Todėl neišvengiamai susiduriama ir su didėjančiu nusikalstamų veikų, susijusių su šios erdvės panaudojimu, skaičiumi. Elektroninė erdvė suteikia naujų galimybių įvykdyti nusikaltimus, sudaro sąlygas naujiems nusikaltimų būdams atsirasti, be to, sudaro galimybes įvykdyti naujas veikas, iki tol nežinomas teisinėje praktikoje. Pastaruoju metu tokio tipo nusikaltimai – elektroniniai nusikaltimai – tapo realybe, o elektroninių nusikaltėlių pajamos pagal kai kuriuos vertinimus yra trečioje vietoje po pajamų iš prekybos narkotikais ir prekybos ginklais. 2010 metais Britų nacionalinėje saugumo strategijoje elektroniniai nusikaltimai buvo paminėti tarp pagrindinių Jungtinės Karalystės saugumo grėsmių, šalia terorizmo, karo ir gamtos nelaimių[2]. Būtent po 2009 m. rugsėjo 11-osios įvykių pradėta kalbėti, kad teroristiniai aktai gali būti vykdomi ir internetu[3].

Elektroniniai nusikaltimai gali paveikti tiek konkretų asmenį, tiek visą visuomenę kaip tokią[4]. Modernus gyvenimas šiais laikais neatsiejamas nuo elektroninės erdvės panaudojimo. Tačiau be teigiamų dalykų, ta pati elektroninė erdvė tampa didelės grėsmės šaltiniu.

Paminėtina, kad elektroninių nusikaltimų plitimui ir pasireiškimui fizinės valstybių sienos neturi jokios įtakos. Pvz., medžiagos su vaikų pornografija gamintojas gali būti Rusijoje, o tokią medžiagą su vaikų pornografija platinti Ispanijoje[5] ir dar daugelyje

[1] Higgins G. E. *Cybercrime: An Introduction to an Emerging Phenomen*. Library of Congress Cataloging, 2010, p. 1.
[2] UK loses over 43 bilion dollars a year to cybercrime. *In the World News* [interaktyvus]. 2011-02-18 [žiūrėta 2011-06-20].<http://www.intheworldnews.com/uk-loses-over-43-billion-dollars-a-year-to-cyber-crime/341153/>.
[3] Britz T. M. *Computer Forensics and Cyber Crime: An Introduction*. Pearson Education, 2009, p. 155.
[4] Brenner S.W. *Cybercrime. Criminal Threats from Cyberspace*. Library of Congress Cataloging, 2010, įžangos VII.
[5] Higgins G. E. *Cybercrime: An Introduction to an Emerging Phenomen*. Library of Congress Cataloging, 2010, p. 3.

kitų valstybių. Tai parodo, kad elektroniniai nusikaltimai gali būti įvykdomi bet kurioje pasaulio vietoje, nepaisant nusikaltėlio fizinės buvimo vietos. Globali elektroninių nusikaltimų prigimtis apsunkina tokių nusikaltimų tyrimą, sukelia problemas dėl jurisdikcijos bei padaro labai sudėtingą elektroninių įrodymų rinkimą.

1. ELEKTRONINIS NUSIKALSTAMUMAS

1.1. Elektroninio nusikaltimo samprata

Kuriant informacinę visuomenę, visose žmogaus veiklos srityse sparčiai plinta šiuolaikinės informacinės technologijos, kuriomis pasinaudojus tampa prieinama elektroninė erdvė. Todėl neišvengiamai susiduriama ir su didėjančiu nusikalstamų veikų, susijusių su šios erdvės panaudojimu, skaičiumi[6]. Elektroninė erdvė suteikia naujų galimybių įvykdyti nusikaltimus, sudaro sąlygas naujiems nusikaltimų būdams atsirasti, be to, sudaro galimybes įvykdyti naujas veikas, iki tol nežinomas teisinėje praktikoje.

Elektroninių nusikaltimų istorija siekia jau ne vieną dešimtmetį, tačiau dėl vieningos elektroninių nusikaltimų sampratos iki šiol vyksta mokslininkų bei praktikų diskusijos. Nors teisinės problemos, susijusios su pavojingomis veikomis panaudojant kompiuterius, pradėtos nagrinėti jau prieš kelis dešimtmečius, iki šiol nėra suformuota vieninga tokio nusikaltimo samprata. Reikia paminėti, jog dažnai apibūdinant elektroninius nusikaltimus vartojami skirtingi terminai, kurie tam tikrais atvejais gali būti ir sinonimai: kompiuteriniai nusikaltimai (angl. *computer crime*), su kompiuteriais nusiję nusikaltimai (angl. *computer-related crime*)[7], aukštų technologijų nusikaltimai (angl. *high-tech crime*) ir kt. 2001 m. priėmus Konvenciją dėl elektroninių nusikaltimų (toliau kai kur – Konvencija), vis dažniau vartojama elektroninio nusikaltimo sąvoka. Tačiau kelis dešimtmečius labai aktyviai buvo vartojama kompiuterinio nusikaltimo sąvoka.

Literatūroje nurodoma, jog *kompiuterinio nusikaltimo* terminas buvo pavartotas jau 60-70 metais, kai mokslinėje literatūroje pasirodė straipsniai šia tema. Vienas iš pirmųjų, susidomėjęs šia problema JAV, Donn Parker taip apibrėžė kompiuterinio nusikaltimo sąvoką: „visos tyčinės veikos, vienu ar kitu būdu susijusios su kompiuteriais, dėl kurių nukentėjęs patyrė ar galėjo patirti žalą, o nusikaltimo subjektas turėjo ar galėjo gauti iš to naudos“. Tačiau šis apibrėžimas neapima veikų, padarytų dėl neatsargumo arba nesiekiant naudos[8]. Taip pat samprata yra pernelyg plati ir apima tokias veikas kaip kompiuterio vagystė, o tai, daugelio autorių nuomone, neturėtų būti traktuojama kaip

[6] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 230.
[7] Sauliūnas D., et al. *Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004, p. 508.
8 Petrauskas R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 5.

kompiuterinis nusikaltimas. Dažnai kompiuteriniu nusikaltimu buvo laikoma veika, tiesiogiai susijusi su elektronine skaičiavimo mašina, įskaitant daug neteisėtų aktų, vykdomų arba elektroninių duomenų apdorojimo sistema, arba prieš ją[9].

1983 m. Ekonominio bendradarbiavimo ir vystymo organizacija sudarė ekspertų komitetą su kompiuteriais susijusių nusikaltimų problemai spręsti. Ši ekspertų grupė terminą „kompiuterinis nusikaltimas“ apibrėžė kaip bet kokį neteisėtą, neetišką ar nesankcionuotą elgesį, susijusį su automatiniu duomenų elektronine forma apdorojimu ir siuntimu. Tačiau šiame apibrėžime nepaminėta, kokios teisės šakos atžvilgiu minėtas elgesys yra neteisėtas.

Tai tik pirmieji bandymai apibrėžti kompiuterinius nusikaltimus. Per daugelį metų įvairios institucijos, mokslininkai bandė apibrėžti kompiuterinius nusikaltimus, tačiau vieningos nuomonės dėl kompiuterinių nusikaltimų sampratos nebuvo prieita. Netgi paminėtina, kad įvairios tarptautinės organizacijos sąmoningai neapbrėžinėja kompiuterinio nusikaltimo[10], nes mano, kad nuolat keičiantis technologijoms, toks apibrėžimas greitai taptų nebeaktualus.

Visgi, atsižvelgiant į nuomonių dėl kompiuterinio nusikaltimo sampratos įvairovę, išskirtinos dvi pagrindinės kompiuterinių nusikaltimų sampratos kryptys[11]:

- *siauraja prasme* kompiuteriniais nusikaltimais laikomos tik tos veikos, kurios nurodytos atskiruose baudžiamųjų įstatymų skirsniuose (pvz., Lietuvoje – XXIX sk. „Nusikaltimai informatikai“). Šioms veikoms būdingas bendras objektas (visuomeniniai santykiai informacijos apdorojimo procese) bei dalykas – kompiuterinė informacija;
- *plačiaja prasme* kompiuteriniais nusikaltimais laikomos baudžiamojo įstatymo nustatytos visuomenei pavojingos veikos, kai kompiuterinė informacija yra nusikaltimo dalykas arba kai kompiuteris panaudojamas kaip nusikaltimo priemonė. Kitais žodžiais tariant, pasikėsinimo dalykas yra informacija, apdorojama kompiuterinėje sistemoje, o kompiuteris yra nusikaltimo įrankis. Šių nusikaltimų objektas skiriasi. Todėl prie tokių veikų priskiriamos ir šios veikos: sukčiavimas panaudojant kompiuterius, autorių teisių pažeidimas, panaudojant kompiuterius ir kt. Paminėtina, jog kartais šios veikos vadinamos su kompiuteriais susijusiais nusikaltimais (angl. *computer-related crime*), nors pastarasis terminas turėtų apimti daugiau pavojingų veikų (pvz., šmeižtą panaudojant elektroninę erdvę).

Tačiau pastaruoju metu, 2001 metais priėmus Konvenciją dėl elektroninių nusikaltimų, kompiuterinių nusikaltimų terminą pakeitė elektroninių nusikaltimų (angl. cybercrime) terminas.

Visų pirma, reikėtų atkreipti dėmesį į patį terminą „elektroninis nusikaltimas“. Elektroninis nusikaltimas nėra tiksliausia sąvoka, apibūdinanti nusikaltimus, vykdomus

[9] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 231.
[10] Williams M. *Virtually criminal: Crime, deviance and regulation online*. New York: Routledge, 2006, p. 20.
[11] Kiškis M., Petrauskas R., Rootmskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 231.

panaudojant elektroninę erdvę[12]. Šie nusikaltimai būdingi ne elektronikos sričiai, elektronikos mokslui, o informatikos inžinerijai, kompiuterijos mokslams. Elektronika, elektroniniai signalai, elektroniniai įtaisai plačiai naudojami televizijoje, radiofonijoje, automobiliuose, pramonėje ir jų signalai analoginiai, tuo tarpu termino „cybercrime“ skiriamasis požymis – nusikaltimų dalykas – duomenys, informacija elektronine, skaitmenine (angl. *digital*) forma. Terminas „cybercrime“ simbolizuoja globaliai stipriai kompiuterizuotai interneto visuomenei būdingas nusikalstamas veikas. Jis kilęs iš termino „Cyber space“, kuris verčiamas „elektroninė erdvė“. Tačiau reikia paminėti, kad Lietuva ratifikavo Konvenciją dėl elektroninių nusikaltimų ir tokiu būdu *de jure* buvo įteisintas elektroninio nusikaltimo terminas.

Reikia pažymėti, kad iki šiol užsienio literatūroje elektroninio nusikaltimo samprata nėra išsamiai analizuota. Kai kurie autoriai nurodo, jog kol kas nėra universalios elektroninio nusikaltimo sampratos, tačiau teigia, kad elektroninio nusikaltimo samprata turėtų apimti ir tokius neteisėtus veiksmus naudojant kompiuterius, kaip neteisėta prieiga prie kompiuterinės sistemos, neteisėtas kompiuterinės informacijos perėmimas, neteisėto turinio medžiagos siuntimas ir kt. Taip pat manoma, kad elektroniniais nusikaltimais suprantami įvairūs veiksmai, tokie kaip poveikis kompiuterinei sistemai, su turiniu susiję pažeidimai (neteisėto ir žalingo turinio medžiagos panaudojimas) ir kiti.

Mokslininkas Goerge E. Higgins skiria kompiuterinius nusikaltimus ir elektroninius nusikaltimus. Kompiuteriniai nusikaltimai yra veikos, kurioms įvykdyti naudojamas kompiuteris ir kurios uždraustos baudžiamųjų įstatymų. Kompiuteriniai nusikaltimai gali būti skirstomi į tris grupes:

1) kai kompiuteris panaudojamas kaip nusikaltimo įvykdymo įrankis (pvz., neteisėtas garso failų siuntimasis);
2) kai kompiuteris yra kaip nusikaltimo objektas (pvz., neteisėtos prieigos atveju);
3) kai kompiuteris naudojamas kaip nelegalaus turinio saugykla (pvz., kai naudojamas saugoti medžiagai su vaikų pornografija)[13].

Elektroniniais nusikaltimais autorius laiko nusikaltimus, atliekamus per internetą (panaudojant bet kokios rūšies prieigą).

Pažymėtina, kad Konvencijoje dėl elektroninių nusikaltimų nėra pateikiama elektroninio nusikaltimo sąvoka. Tačiau atsižvelgiant į Konvencijoje dėl elektroninių nusikaltimų kriminalizuotinas veikas, apibrėžiant elektroninius nusikaltimus, ne tik reikėtų laikytis kompiuterinių nusikaltimų sampratos plačiąja prasme krypties, tačiau tokias veikas galima būtų tapatinti su veikomis, susijusiomis su kompiuterių panaudojimu (angl. *computer-related crime*), kurios apima gana platų nusikalstamų veikų spektrą. Galima konstatuoti, jog Konvencijoje dėl elektroninių nusikaltimų minimos veikos yra labai skirtingos (skirtumai objekte ir pan.), dėl to pateikti vieningą tokių veikų sampratą yra problemiška.

[12] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 232.
[13] Higgins G. E. Cybercrime: An Introduction to an Emerging Phenomen. Library of Congress Cataloging, 2010, p. 2.

1.2. Elektroninių nusikaltimų žala ir latentiškumas

Reikia pažymėti, kad susijusios su kompiuterinėmis technologijomis, nusikalstamos veikos yra ypač pavojingos tuo, kad oficiali teisėsaugos organų statistika neatspindi realios padėties. FBI Nacionalinės kompiuterinių nusikaltimų tyrimų grupės teigimu, 85–97 % tokių nusikaltimų neiškyla į viešumą. Kai kurių ekspertų vertinimu, elektroninių nusikaltimų latentiškumas JAV sudaro 80 proc., Jungtinėje Karalystėje – 85 proc., Vokietijoje – 75 proc., Rusijoje – net 90 proc. Taip pat jau 1995 m. atliktų JAV Gynybos departamento finansuotų tyrimų statistika buvo gana stulbinanti. Bandant įsibrauti į 8932 informacines sistemas, kurios dalyvavo tyrime, 7860 atvejai buvo sėkmingi. Tik 390 sistemų administratoriai (iš 7860) užfiksavo įsibrovimą, o tik 19 iš jų apie tai pranešė oficialioms instancijoms[14].

Kaip liudija statistika, pateikiama 2008 m. Kompiuterinių nusikaltimų ir saugumo apžvalgoje[15], atliktoje Kompiuterių saugumo instituto, iš 295 respondentų tik apie 27 proc. apie neteisėtą prisijungimą prie kompiuterio ar kompiuterių tinklo pranešė teisėsaugos institucijoms. 54 procentai respondentų tiesiog „užlopė padarytas spragas“. Taigi elektroniniai nusikaltimai yra vieni latentiškiausių iš visų nusikalstamumo rūšių[16].

Tokį didelį elektroninių nusikaltimų latentiškumą lemia keli faktoriai[17]:

1. Kompiuterių naudotojai dažnai neturi pakankamai žinių pastebėti tokiems nusikaltimams.
2. Aukos vengia informuoti apie aptiktus kompiuterinius nusikaltimus. Verslo srityje šis nenoras susijęs su dviem dalykais:
   - vienos aukos nenori atskleisti informacijos apie savo darbą, bijodamos viešumo arba prarasti gerą vardą;
   - kitos aukos bijo prarasti investuotoją, visuomenės pasitikėjimą.

Kompiuteriniai nusikaltimai kelia susirūpinimą ir dėl savo augimo tempų. Kompiuterinio saugumo instituto ir FTB atliktas tyrimas, kurio metu apklausta 250 organizacijų, parodė, kad apytikriai nuostoliai 1997 metais buvo 137 mln. JAV dolerių, t.y. 37 % daugiau nei 1996 metais. 2001 metais CERT surinkta informacija liudijo, jog įvyko 52 000 kompiuterių saugumo incidentai. Tai 140 proc. daugiau nei ankstesniais metais. Tuo tarpu 2009 metais, pagal „F-Secure“ ataskaitą, pasaulyje vien kenkimo programomis buvo užkrėsta daugiau nei 9 000 000 kompiuterių[18].

Literatūroje teigiama, kad yra glaudus ryšys tarp elekrtoninių nusikaltimų skaičiaus

[14] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 240.
[15] CSI computer crime survey 2008. [interaktyvus, žiūrėta 2011-06-28]. <http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf>.
[16] Kshetri N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, 2010, p. 64.
[17] Kiškis M., Petrauskas R., Rotomskis I.; Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 240.
[18] Ghosh S., Turrini E. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag, 2010, p. 27.

ir interneto paplitimo[19]. Taigi valstybėse, kuriose interneto, ypač plačiajuosčio ryšio, penetracija yra didžiausia, elektroninių nusikaltimų skaičius taip pat turėtų būti pakankamai didelis. Paminėtina, kad Lietuva šiuo metu šviesolaidį internetą diegia sparčiausiai Europoje[20].

Visgi, reikia pažymėti, kad dėl elektroninių nusikaltimų nėra patikimos statistikos[21], nes vieni statistiniai duomenys skiriasi nuo kitų. Todėl galima pateikti tik atitinkamus statistinės informacijos pavyzdžius, kurie, tikėtina, turės didesnę ar mažesnę paklaidą.

Naujausia elektroninių nusikaltimų statistika taip pat liudija didžiulius nuostolius, elektroninių nusikaltimų įvairovę bei didėjančią tokių veikų grėsmę. Pagal britų tyrimo kompanijos „mi2g“ duomenis, 2004 metais žala nuo elektroninių nusikaltimų sudarė 411 mlrd. JAV dolerių, kas beveik du kartus viršija žalą 2003 metais. 2005 m. Kompiuterinių nusikaltimų ir saugumo apžvalgoje, atliktoje Kompiuterių saugumo instituto, nurodoma, jog apklausti 639 respondentai (juridiniai asmenys) per 2005 metus patyrė daugiau kaip 130 mln. JAV dolerių nuostolius. Iš visų 693 apklaustų respondentų 2005 metais neteisėtą kompiuterinės sistemos naudojimą užfiksavo beveik 60 proc. Dažniausiai minima pavojinga veika – kompiuterių virusų platinimas. Labiausiai 2005 metais padidėjo pažeidimų, susijusių su belaide prieiga, skaičius.

Pagal Britanijos Elektroninio saugumo ir informacijos aprūpinimo tarnybos duomenis (studiją), 2010 metais Jungtinėje Karalystėje dėl elektroninių nusikaltimų buvo patirta 43,5 mln. dolerių žala[22].

Viena iš žymesnių bylų – R. T. Morris byla, susijusi su vadinamuoju internetiniu kirminu[23]. 23 metų studentas Morrisas nebuvo tipinis sistemlaužys. Šio studento tėvas dirbo kompiuterinio saugumo ekspertu Nacionaliniame kompiuterinio saugumo centre. Tačiau remiantis CFAA, Morrisas buvo nuteistas 3 metams lygtinai, 10 000 USD bauda bei 400 val. viešųjų darbų. Bausmė jam buvo skirta už kompiuterių programos – kirmino sukūrimą ir panaudojimą. Ši programa, anot Morriso, buvo skirta rinkti informacijai apie kompiuterius, įjungtus į pasaulinį kompiuterių tinklą, bei šių kompiuterių apsaugos priemones. Programa buvo sukurta 1998 metais, ja buvo siekiama atlikti jokios žalos nedarantį eksperimentą kompiuterių mokslo srityje. Tačiau, Morrisui nežinant, padaryta programinė klaida lėmė tai, kad programa pradėjo daugintis didžiuliais tempais. Programai patekus į internetą, po keleto valandų buvo užkrėsta apie 2 000 kompiuterių (sutrikdytas kompiuterių/kompiuterių tinklų darbas), dėl to padaryta 150 000 JAV dolerių žala vien JAV. Reikia paminėti, kad vertinimai, susiję su padaryta žala, skiriasi.

[19] Kshetri N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, 2010, p. 187.
[20] Navickytė L. Lietuva šviesolaidinį internetą Europoje diegia apsrčiausiai. *Diena* [interaktyvus]. 2010-02-25 [žiūrėta 2011-06-27]. < http://www.diena.lt/naujienos/mokslas-ir-it/lietuva-sviesolaidini-interneta-europoje-diegia-sparciausiai-papildyta-265149>.
[21] Kshetri N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, 2010, p. 29.
[22] UK loses over 43 bilion dollars a year to cybercrime. *In the World News* [interaktyvus]. 2011-02-18 [žiūrėta 2011-06-20].< http://www.intheworldnews.com/uk-loses-over-43-billion-dollars-a-year-to-cyber-crime/341153/>.
[23] Kiškis M.; Petrauskas R.; Rotomskis I.; Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 241.

J. McAfee, Kompiuterių virusų asociacijos pirmininkas, yra pareiškęs, kad Morriso kirmino padaryta žala siekia 96 mln. JAV dolerių.

Tai tik vienas iš daugelio precedentų, iškilusių į viešumą. Labai daug elektroninių nusikaltimų iš viso neiškyla į viešumą, kadangi ši nusikaltimų kategorija yra viena latentiškiausių, t.y. dažnai nepatenka į oficialią nusikaltimų statistiką. Elektroninių nusikaltimų kriminalizavimo prasme reikėtų paminėti, kad ilgą laiką atsakomybė už kai kuriuos elektroninius nusikaltimus, pvz., neteisėtą prieigą prie kompiuterinės informacijos, iš viso nebuvo nustatyta. Ir tik didžiulėmis pastangomis koordinuojant atskirų valstybių baudžiamuosius įstatymus, daugumai nacionalinių įstatymų leidėjų pavyko kriminalizuoti pagrindines elektroninių nusikaltimų rūšis. Tačiau iki šiol problemos kyla ne tik dėl netinkamo kai kurių elektroninių nusikaltimų kriminalizavimo nacionaliniuose baudžiamuosiuose įstatymuose, bet ir dėl kvalifikacijos ar techninės įrangos stokos tiriant elektroninius nusikaltimus bei elektroninių įrodymų įtvirtinimo problemų.

2. ELEKTRONINIŲ NUSIKALTIMŲ KLASIFIKACIJA, SUBJEKTAI IR ATLIKIMO BŪDAI

2.1. Elektroninių nusikaltimų klasifikacija

Viena iš pirmųjų elektroninių nusikaltimų klasifikacijų pateikta 1989 metais. Šiais metais Europos Tarybos Ministrų kabinetas priėmė rekomendaciją R89(9) Europos Sąjungos šalių vyriausybėms, kurioje siūloma peržiūrint ar kuriant įstatymus atsižvelgti į Europos komiteto nusikaltimų problemoms tirti skirtą pranešimą apie su kompiuteriais susijusius nusikaltimus[24]. Šiame pranešime pateikiami du sąrašai veikų, susijusių su tokiais nusikaltimais. Europos Sąjungos šalims leidžiama savarankiškai spręsti, kaip ir kiek pasinaudoti šiuo pasiūlymu. „Minimaliame sąraše“ išvardytos 8 pavojingesnės veikos, susijusios su kompiuterinėmis technologijomis. Papildomas sąrašas apima keturias mažiau pavojingas veikas, kurios įtraukiamos į įstatymų leidybą, bet nėra privalomos. Šie sąrašai reikalingi suvienodinant ES šalių teisines sistemas kompiuterių nusikaltimų atžvilgiu. Šios veikos nėra kompiuteriniai nusikaltimai teisine prasme, o tik veikos, kurias valstybėms rekomenduojama fiksuoti savo nacionaliniuose teisiniuose aktuose kaip pažeidimus ir nebūtinai kaip kriminalines veikas.

[24] Computer-related crime. Council of Europe. Recomendation No. R(89)9, adopted by Committee of Ministers of the Council of Europe on 13 September 1989 [interaktyvus]. Strasbourg, 1990 [žiūrėta 2011-06-21]. <http://www.oas.org/juridico/english/89-9&final%20Report.pdf>.

Minimalus sąrašas

1. Sukčiavimas naudojant kompiuterį (Computer-related fraud).
2. Klastojimas naudojant kompiuterį (Computer forgery).
3. Elektroninių duomenų ar programų sunaikinimas ar sugadinimas (Damage to computer data or computer programs).
4. Sabotažas naudojant kompiuterį (Computer sabotage).
5. Neteisėta prieiga prie kompiuterinių sistemų (Unauthorised access).
6. Neteisėtas informacijos perėmimas kompiuterinėse sistemose (Unauthorised interception).
7. Neteisėtas apsaugotų kompiuterių programų dauginimas ir platinimas (Unauthorised reproduction of a protected computer program).
8. Neteisėtas kompiuterių lustų (mikroschemų) topografijų dauginimas ir platinimas (Unauthorised reproduction of a topography).

Neprivalomas sąrašas

1. Kompiuterių duomenų ar programų pakeitimas (Alteration of computer data or computer programs).
2. Špionažas naudojant kompiuterį (Computer espionage).
3. Neteisėtas kompiuterio naudojimas (laiko vagystė) (Unauthorised use of computer).
4. Neteisėtas apsaugotų kompiuterių programų naudojimas (Unauthorised use of a protected computer program).

1995 metų INTERPOLO rekomendacijose „Computers and crime“ (čia pateikiamas tik minimalus sąrašas), Europos Tarybos rekomendacijose pateiktos šios pavojingos veikos, panaudojant kompiuterį (kurios aiškinamos toliau):

1. *Sukčiavimas naudojant kompiuterį.* Kompiuterių duomenų ar programų įvedimas, pakeitimas, ištrynimas ar kitoks trukdymas duomenų apdorojimo procesui, kas paveikia šio proceso galutinį rezultatą, padarydamas žalą kito asmens nuosavybei, norint neteisėtai gauti materialinę naudą sau ar kitam asmeniui.
2. *Klastojimas naudojant kompiuterį.* Kompiuterių duomenų ar programų įvedimas, pakeitimas, ištrynimas ar kitoks trukdymas duomenų apdorojimo procesui, kai šių veiksmų tikslas yra toks pats, kaip ir įstatymuose, numatančiuose atsakomybę už klastojimą.
3. *Kompiuterių duomenų ar sunaikinimas arba sugadinimas.* Kompiuterių duomenų ar programų ištrynimas, sunaikinimas, sugadinimas, neturint tam teisės.
4. *Sabotažas naudojant kompiuterį.* Kompiuterių duomenų ar programų įvedimas, pakeitimas, ištrynimas ar įsikišimas, trukdymas kompiuterių sistemoms, norint surikdyti kompiuterių ar telekomunikacijų sistemos darbą.

5. *Neteisėta prieiga prie kompiuterių sistemų.* Priėjimas, neturint teisės, prie kompiuterių sistemos ar tinklo, pažeidžiant saugumo priemones.
6. *Neteisėtas informacijos perėmimas kompiuterių sistemose.* Perėmimas, atliktas techniškai, legaliai nenumatytais būdais, kompiuterių tinklo viduje ar iš išorės.

Jungtinių tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalgoje pateikiama tokia kompiuterinių nusikaltimų klasifikacija[25]:

1. manipuliavimas panaudojant kompiuterį (kompiuterinis sukčiavimas);
2. klastojimas panaudojant kompiuterį;
3. kompiuterių duomenų ir programų sunaikinimas ir modifikavimas (sabotažas);
4. neteisėta prieiga prie kompiuterių duomenų;
5. neteisėtas kompiuterių programų platinimas.

Manipuliavimas panaudojant kompiuterį (kompiuterinis sukčiavimas)

Tai manipuliavimas įvedimu, išvedimu bei įvedimas kompiuterių programų, kurios tampa duomenų praradimo ar sugadinimo priežastimi, siekiant materialinės naudos sau, dėl ko būna patirti ekonominiai nuostoliai.

Manipuliavimas įvedimu yra dažniausiai pasitaikantis, nes tai lengva įvykdyti ir sunku susekti. Šiuo būdu į kompiuterių sistemą gali būti įvesti neteisingi duomenys. Tai nereikalauja ypatingų kompiuterinių žinių ir gali būti įvykdyta bet ko, kas turi prieigą prie kompiuterių sistemų duomenų apdorojimo funkcijų.

Manipuliacija programomis, kurią sunku aptikti, reikalauja specialių kompiuterinių žinių. Čia įeina kompiuterių sistemoje esančių programų pakeitimas arba naujų programų įvedimas. Dažniausiai naudojamas asmenų, turinčių specialių kompiuterinių žinių, metodas yra Trojos arklys, kompiuterinės instrukcijos, slaptai įvedamos į kompiuterių programą. Trojos arklys gali būti užprogramuotas save sunaikinti, nepaliekant jokių jo egzistavimo požymių, išskyrus padarytą žalą.

Manipuliavimas išvedimu yra vykdomas paveikiant kompiuterių sistemų išvedimo procedūras. Aiškus pavyzdys yra grynųjų pinigų automato apgavimas, atliekamas įvestimis falsifikuojant komandas kompiuteriui. Dažniausiai šioje apgavystėje naudojamos vogtos bankų kortelės. Taip pat yra tam tikras sukčiavimas, kurio metu vykdomos manipuliacijos, kai gaunama nauda iš automatizuotų kompiuterinių procedūrų pakartojimo. Tokios manipuliacijos vadinamos „saliamio“ technika, kai labai nedidelė finansinio pervedimo dalis pervedama į kitą sąskaitą.

Klastojimas panaudojant kompiuterį

Tai kompiuterine forma saugomų duomenų pakeitimas, sugadinimas ar sunaikinimas. Vykdymo motyvai ir tikslai gali būti įvairūs. Nuo sukčiavimo skiriasi tuo, jog nesiekiama

[25] International review of criminal policy – United Nations Manual on the prevention and control of compute-related crime. Jungtinių tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalga [interaktyvus, žiūrėta 2011-06-21]< http://www.uncjin.org/Documents/irpc4344.pdf>.

tiesioginės materialinės naudos. Prie šio tipo nusikaltimų gali būti priskirtina ir neteisėta (nesąžininga) konkurencija. Vykdant kompiuterinius klastojimus organizacijose, kurių apskaita kompiuterizuota, gali būti slepiami mokesčiai.

Nauja apgavikiškų klastojimų karta pasirodė, kai atsirado galimybė daryti spalvotas lazerines kopijas. Lazeriniai spausdintuvai turi dideles aukštos kokybės kopijavimo galimybes, gali atspausdinti pakeistus ar net naujai sukurtus dokumentus, kuriuos atskirti nuo originalų be eksperto pagalbos gana sunku.

Kompiuterių duomenų ir programų sunaikinimas ar modifikavimas (kompiuterinis sabotažas)

Tai kompiuterių programų, duomenų, kompiuterinės technikos sugadinimas ar sunaikinimas bei techninio personalo veiklos apribojimas, trukdant jiems dirbti su kompiuterių resursais. Taip pat programų, skirtų sugadinti ar sunaikinti kitoms kompiuterių programoms bei duomenims (kompiuterių virusų, loginių bombų ir pan.) kūrimas, platinimas bei įvedimas.

Kompiuterinio sabotažo tikslas – sugadinti kompiuterių programas, sunaikinti kompiuterių duomenis. Nusikaltimas gali būti vykdomas dėl karinių, politinių motyvų, konkurencinėje kovoje, kerštaujant arba iš chuliganiškų paskatų. Duomenis galima sugadinti per labai trumpą laiką, panaudojant kompiuterių programas (standartines ir specialiai sukurtas), taip pat elektromagnetinių bangų ar radiacijos pagalba.

Šios kategorijos kriminalinės veikos apima ir tiesioginį, ir slaptą neteisėtą prieigą prie kompiuterių sistemos, įvedant naujas programas, žinomas kaip virusus, logines bombas, kirminus. Neteisėta duomenų modifikacija ar išnaikinimas per internetą, kuris sutrikdo normalų kompiuterių sistemos darbą, dažnai minima kaip kompiuterinis sabotažas. Pavyzdžiui, 1987 m. Londone atleistas vienos firmos darbuotojas nesėkmingai bandė sužlugdyti firmos kompiuterių sistemą, programoje patalpindamas loginę bombą, kuri po tam tikro laiko visiškai ją sunaikintų.

Neteisėta prieiga prie kompiuterių duomenų

Neteisėta prieiga funkciškai yra nuosavybės ribų peržengimo analogas[26]. Tai prieiga prie kompiuterių duomenų, prie kurių neturima teisės prieiti, įveikiant apsaugines sistemas, kai yra pažeidžiamas kompiuterinės informacijos slaptumas[27]. Prieigos prie kompiuterių duomenų šiuo atveju nereikėtų suprasti kaip fizinės. Motyvai gauti neteisėtą prieigą gali būti įvairūs: tai hakerių noras pasirodyti ir kt. Neteisėta prieiga prie duomenų, kurie yra valstybės ar firmos komercinė paslaptis, visose valstybėse yra baudžiama. Žmogaus, neturinčio įgaliojimų prieiti prie kompiuterių sistemos, tyčinė ir nepateisinama prieiga dažnai konstatuojama kaip kriminalinis elgesys. Neteisėta prieiga sukuria galimybę padaryti žalą duomenims, sutrikdyti kompiuterių sistemos darbą. Neteisėta prieiga gali būti vykdoma kompiuterių tinklų pagalba. Norint gauti prieigą, gali būti pasinaudota silpnomis apsaugos vietomis. Dažniausiai hakeriai apsimeta teisėtais vartotojais. Tai gali atsitikti ten, kur naudojamasi bendrais slaptažodžiais.

[26] Brenner S. W. *Cybercrime. Criminal Threats from Cyberspace*. Library of Congress Cataloging, 2010, p. 121.
[27] Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai. *Jurisprudencija*, 2003, 47(39), p. 61.

Slaptažodis dažnai minimas kaip priemonė, užkertanti kelią neteisėtai prieigai[28]. Tačiau šiuolaikinis hakeris tam tikrais metodais gali lengvai apeiti šią apsaugą. Jeigu hakeris sugeba nulaužti prieigos leidimo slaptažodį, gali patalpinti Trojos arklį, kad surinktų kitų teisėtų vartotojų slaptažodžius. Šią programą sunku aptikti. Vėliau per nuotolinę prieigą hakeris gali gauti daugumą slaptažodžių. Slaptažodžių apsaugą galima apeiti ir kitais būdais, pavyzdžiui, panaudojant slaptažodžių nulaužimo programas. Nulaužimo programomis hakeriai keičiasi internetu.

Neteisėtas kompiuterių programų platinimas

Tai programinės įrangos, kurią gali naudoti tik ją sukūrusi ar įsigijusi organizacija, pasisavinimas ir platinimas. Ši veika gali atnešti ekonominę žalą teisėtiems savininkams. Programinės įrangos piratavimas yra labai paplitęs Rytų Europos ir buvusios Sovietų Sąjungos šalyse.

Paminėtina prof. *U. Sieber* 1998 metais pateikta elektroninių nusikaltimų (tuo metu – kompiuterinių nusikaltimų/su kompiuteriais susijusių nusikaltimų) formų klasifikacija[29]:

- ➤ privatumo pažeidimai;
- ➤ ekonominiai pažeidimai (įsilaužimas į kompiuterį; špionažas panaudojant kompiuterį; neteisėtas programinės įrangos kopijavimas; sabotažas panaudojant kompiuterį; sukčiavimas panaudojant kompiuterį);
- ➤ pažeidimai, susiję su neteisėtu ir žalingu turiniu (medžiagos, susijusios su pornografija, platinimas ar pan.);
- ➤ kiti pažeidimai.

Skirstant elektroninius nusikaltimus, galima pasiremti ir viena iš paskutiniųjų tokių nusikaltimų klasifikacijų, pateiktų Konvencijoje dėl elektroninių nusikaltimų – elektroniniai nusikaltimai pagal įstatymo saugomą interesą skirstomi į:

- ➤ nusikaltimus, pažeidžiančius kompiuterinės informacijos ir kompiuterių sistemų konfidencialumą, vientisumą bei prieinamumą (neteisėta prieiga, neteisėtas perėmimas, įsikišimas į duomenų apdorojimo procesą, įsikišimas į kompiuterių sistemos darbą);
- ➤ nusikaltimus, susijusius su kompiuterių panaudojimu (klastojimas panaudojant kompiuterius; sukčiavimas panaudojant kompiuterius);
- ➤ nusikaltimus, susijusius su turiniu (medžiagos su vaikų pornografija panaudojimas);
- ➤ pažeidimus, susijusius su autorių teisėmis ar gretutinėmis teisėmis.

Šios elektroninių nusikaltimų rūšys atitinkamai skirstomos ir į tam tikrus porūšius:

[28] Štitilis D. Neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimas. *Informacijos mokslai*, 2003, 26, p. 82.
[29] Sieber U. *Computer Crime and Criminal Information Law – The New Trends in International Risks and Information Society* [interaktyvus, žiūrėta 2011-06-21]. <http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html>.

Nusikaltimai, pažeidžiantys kompiuterinės informacijos ir kompiuterių sistemų konfidencialumą,vientisumą bei prieinamumą

Viena iš žinomiausių veikų – neteisėta prieiga (angl. *hacking*). Neteisėta prieiga prie kompiuterių programų ar duomenų elektronine forma laikytina tokia veika, kuri pažeidžia laikomos informacijos slaptumą bei konfidencialumą (t.y. kyla realios žalos grėsmė), o dėl neteisėtos prieigos vykdomas špionažas, neteisėtai kopijuojami autorių teisėmis apsaugoti kūriniai, sabotažas, sukčiavimas panaudojant kompiuterius ir pan. laikytini savarankiškomis pavojingomis veikomis.

Baudžiamosios atsakomybės už neteisėtą prieigą problema kilo jau 1985 metais, kai Vienoje kompiuterių mokslo srities studentas įsilaužė į keleto finansų institucijų kompiuterių sistemas, tačiau nepadarė jokios žalos. Apie šiuos veiksmus buvo pranešta Vienos teisėsaugos institucijoms. Tačiau tyrimas buvo sustabdytas, nes nebuvo padaryta jokios žalos, o studento motyvacija buvo pavadinta „intelektualiu iššūkiu“. Byloje *R v Gold* taip pat buvo pademonstruota baudžiamųjų įstatymų nuostatų, susijusių su neteisėta prieiga, būtinybė. Jungtinėje Karalystėje tyrimas prasidėjo dėl to, jog sistemlaužiai be leidimo įsilaužė į „British Telecom“ kompiuterių tinklą ir pakeitė tam tikrus duomenis. Kaltinamieji teigė, kad buvo įsilaužta turint tikslą „išryškinti saugumo spragas“ kompiuterių sistemoje „British Telecom“. Sistemlaužiai buvo apkaltinti remiantis 1981 m. Klastojimo įstatymu, nes buvo sudarytas klaidingas dokumentas, vėliau buvo nuteisti. Tačiau apeliacinėje instancijoje teismo sprendimas buvo panaikintas, teigiant, jog šių asmenų veiksmuose nebuvo jokio nusikaltimo sudėties. Tokiu būdu buvo pademonstruotas egzistuojančių įstatymų netobulumas.

Įsikišimą į kompiuterinės informacijos apdorojimo procesą galima vadinti neteisėtos prieigos tąsa. Tokia veika gali pasireikšti neteisėtu kompiuterinės informacijos ištrynimu, sunaikinimu, sugadinimu ar pakeitimu. Manoma, jog kompiuterių programos ir kompiuterinė informacija turi būti apsaugota nuo tokio kėsinimosi, kaip ir materialūs objektai, siekiant užtikrinti kompiuterinės informacijos integralumą bei kompiuterių programų ar kompiuterinės informacijos tinkamą naudojimą (funkcionavimą). Kompiuterinės informacijos vagystę (tam tikra dalimi sietiną su špionažu panaudojant kompiuterį) taip pat galima įvardyti kaip neteisėtos prieigos tąsą. Šiandieninės informacinės technologijos, ypač kompiuterių tinklai, suteikia didžiulių galimybių akimirksniu nukopijuoti bet kokį informacijos kiekį. Kai kurie autoriai tokią veiką laiko savarankiška pavojinga veika, užtraukiančia baudžiamąją atsakomybę.

Su kompiuterinės informacijos vagyste susijusi ir veika perimant kompiuterinę informaciją, kai ji siunčiama elektronine erdve. Prieš keletą metų perėmimo (angl. *Interception*) veika dažniausiai būdavo tapatinama su telefoninių pokalbių perėmimu. Tačiau *M. Mohrenschlager* teigia, kad vystantis technologijoms ir komunikacijoms, telekomunikacijoms ir kompiuterių sistemoms susiliejant į bendrą visumą, apsaugos reikalauja ir kiti kompiuterinės informacijos tipai, siunčiami elektronine erdve.

Sabotažu panaudojant kompiuterius vadinama veika, kai į kompiuterių sistemą įvedant kenkimo programas (ar padarant kompiuterių programose pakeitimus) neteisėtai

sunaikinama, pakeičiama ar ištrinama kompiuterinė informacija, siekiant sutrikdyti kompiuterių sistemos darbą. Duomenų, saugomų elektronine forma, koncentruotumas, įmonių, organizacijų bei fizinių asmenų priklausomumas nuo informacijos, laikomos elektronine forma, sabotažą panaudojant kompiuterius daro labai pavojinga veika. Visuomenė įvairiose gyvenimo srityse (medicinos tarnybų, transporto veikla ir pan.) tampa vis labiau priklausoma nuo kompiuterių sistemų, kurios dažnai sujungtos su kompiuterių tinklais (elektronine erdve). Todėl netgi nedidelis šių sistemų funkcionavimo sutrikimas, atsiradęs dėl veikos panaudojant elektroninę erdvę, gali sukelti pavojų žmonių sveikatai ar gyvybei. Atsiradus elektroninei erdvei, populiariausi metodai padaryti žalą – specialių programų, kurios gali ištrinti didelius duomenų kiekius per trumpą laiką, panaudojimas. Tokios programos gali būti kompiuterių virusai, Trojos arkliai ir kt. Daugiausia problemų kelia kompiuterių virusų ir kirminų paplitimas. Kompiuterių virusai – tai programos, kurios platinasi elektroninėje erdvėje bei kompiuterių sistemose ir greičiausiai po tam tikro laiko padaro žalą.

Pastaruoju metu akcentuojamas *kompiuterių sistemos darbo sutrikdymas*, kai kompiuterių sistema internetu atakuojama dideliu kiekiu žinučių (angl. *a distributed denial of service (DDoS) attack*). Šiuo būdu sutrikdomas kompiuterių sistemos darbas, nors neteisėta prieiga prie sistemos ir neatliekama. Literatūroje DDoS atakos suprantamos kaip kruopščiai atlikti veiksmai, kuriais siekiama teisėtus vartotojus atkirsti nuo tinklo resursų[30]. DDoS atakos dažnai neatsiejamis nuo botnetų[31] panaudojimo[32]. Tokiais veiksmais buvo sutrikdytas „CNN“, „Yahoo!“, „E-Bay“ bei kitų interneto svetainių darbas, dėl to buvo patirta milžiniškų finansinių nuostolių. Teisminėje praktikoje yra ne viena byla, kai buvo nuteisti tokias veikas įvykdę asmenys. Pavyzdžiui, 2002 m. pradžioje, remiantis Federaliniu sukčiavimo bei piktnaudžiavimo panaudojant kompiuterį įstatymu, buvo nuteistas Bret McDanel. Šis asmuo buvo pripažintas kaltu, nes piktavališkai siuntė tūkstančius elektroninių žinučių į centrinį kompiuterį, kurio operatorius buvo „Tornado Development“. Tokiu būdu šis centrinis kompiuteris buvo perpildytas, dėl to sutriko jo darbas. Bret McDanel buvo nuteistas laisvės atėmimu penkeriems metams.

Kaip viena iš didžiausių DDoS atakų paminėtini 2007 metų Estijos įvykiai, kai botnetas, kurį sudarė apie 1 milijonas kompiuterių, buvo panaudotas atakuoti Estijos kompiuteriams ir kompiuterių tinklams, dėl to buvo sutriktydas šalies valstybinių institucijų, parlamento bei daugumos bankų darbas[33]. Estija manė, kad Rusija pradėjo elektroninį karą[34]. Tačiau pakankamai įrodymų tam nėra iki šiol. Beje, kai kurie autoriai Estijos įvykius pristato vadovaudamiesi elektroninio terorizmo samprata.

Paminėtų veikų įvykdymas dažnai susijęs su tam tikrų įrankių/priemonių turėjimu. M. Mohrenschlager nurodo, kad praktikoje egzistuoja ištisos nelegalios slaptažodžių bei prieigos kodų rinkos elektroninėje erdvėje. Todėl viena iš įvardijamų internetinių

[30] Ghosh S., Turrini E. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag, 2010, p. 40.
[31] Virusų pagalba iš išorės neteisėtais tikslais valdomi kompiuterių tinklai (grupė atskirų kompiuterių).
[32] Graham J. *Cyber Fraud: Tactics, Techniques and Procedures*. Taylor&Francis Group, 2009, p. 316.
[33] Kshetri N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, 2010; p. 7.
[34] Brenner S. W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. – Oxford University Press, 2009, p. 10.

nusikaltimų rūšių – neteisėtos prieigos priemonių bei įrenginių platinimas, gaminimas ir kt. Šio tipo veikų pavojingumas buvo pažymėtas jau 1994 m. Kriminalinės policijos tarptautinėje apžvalgoje dėl kompiuterinių nusikaltimų, kur nurodyta, jog veikos pavojingumas sietinas su galimybe padaryti žalą.

Kenkimo programų sukūrimas, naudojimas ir platinimas taip pat laikomas pavojinga veika. Literatūroje nurodoma, kad kenkimo programų sukūrimo, naudojimo bei platinimo pavojingumas visuomenei pasireiškia tuo, kad tokios programos gali pačiu netikėčiausiu momentu sutrikdyti kompiuterių sistemos darbą, dėl ko gali kilti žalingų pasekmių. Atsiradus elektroninei erdvei, kenkimo programų grėsmė padidėjo, nes, pavyzdžiui, paskleidus virusą internete, dėl šio tinklo globalumo jis gali padaryti daug žalos. Kenkimo programomis laikomos kompiuterių programos, turinčios virusų (kompiuterių virusai), ar tam tikrų nurodymų (pvz., loginės bombos, Trojos arkliai, asinchroninės atakos, liukai), ar turinčios specifinių savybių įvykdyti neteisėtus arba nusikalstamus veiksmus (grobti pinigus iš bankų sąskaitų ir kt.). Šios programos turi savybę persikelti kompiuterių tinklu iš vienos kompiuterių sistemos į kitą, patekti į kompiuterių sistemą, taip pat daugintis kaip virusinės ligos.

Su kompiuterių panaudojimu susiję nusikaltimai

Technologinė revoliucija padidino galimybes įvykdyti tokius ekonominius nusikaltimus kaip sukčiavimas. Šiandien daugelis didelių kompanijų prijungtos prie interneto ar kitų kompiuterių tinklų, o jų kompiuterių sistemose esančios bei administruojamos vertybės tapo dažnu taikiniu. Sukčiavimas panaudojant kompiuterį apibrėžiamas kaip piniginių lėšų ar kito turto grobimas panaudojant kompiuterį. Ši veika apima nurodymus kompiuteriui pervesti pinigus į banko sąskaitą ar pan. Anot *D. Baibridge,* veikas atliekant sukčiavimą, susijusį su kompiuteriais, galima suskirstyti į dvi pagrindines grupes: sukčiavimą, susijusį su duomenimis, ir sukčiavimą, susijusį su kompiuterių programomis. Literatūroje nurodoma, jog terminas „sukčiavimas panaudojant kompiuterį“ tam tikrais atvejais gali būti klaidinantis, nes juo apibrėžiamos veikos gali užtraukti baudžiamąją atsakomybę ir pagal kitus straipsnius, ne vien tik pagal straipsnius, nustatančius atsakomybę už tradicinį sukčiavimą. Sukčiavimas panaudojant kompiuterius gali pasireikšti turto ar paslaugų gavimu apgaule ir kt. *U. Sieber* taip pat nurodo, jog pastaruoju metu sukčiavimas panaudojant kompiuterius apibrėžia įvairias veikas ekonominių nusikaltimų srityje bei tai, kad elektroninė erdvė suteikia ypač dideles galimybes įvykdyti tokio tipo nusikaltimus. Taigi iškeliamas tikslas kriminalizuoti sukčiavimo veikas elektroninėje erdvėje, manipuliuojant kompiuterine informacija ar kompiuterių programomis, siekiant materialinės naudos.

Elektroninės erdvės atsiradimas atvėrė kelią ir klastojimo veikoms. Kompiuterinės informacijos klastojimas gali turėti tokių pačių pasekmių, kaip ir tradicinis klastojimas. Klastojimas, susijęs su kompiuteriais, apima neteisėtą kompiuterinės informacijos sukūrimą ar jau sukurtos pakeitimą, dėl to ši informacija įgyja kitokią reikšmę. Todėl turi būti apsaugotas kompiuterinės informacijos patikimumas ir saugumas, siekiant užkirsti kelią neigiamoms teisinių santykių tarp asmenų pasekmėms.

Nusikaltimai, susiję su turiniu

Interneto vystymasis paskatino neteisėto ir žalingo turinio medžiagos plitimą elektroninėje erdvėje. Literatūroje nurodoma, kad tai yra labiausiai auganti nusikaltimų elektroninėje erdvėje sritis. Pornografinio turinio medžiagos internete platinimas, rasistinių nuostatų skleidimas kelia klausimus dėl baudžiamosios teisės vaidmens vertinant šias veikas. *U. Sieber* taip pat mini problemas, susijusias su rasistinėmis nuostatomis, šmeižtu ar grasinimais elektroninėje erdvėje. Paminėtina, kad pavojingos veikos, susijusios su pornografinio turinio medžiagos naudojimu, rasistinėmis nuostatomis, šmeižtu ar grasinimais elektroninėje erdvėje, sukelia teisinės atsakomybės problemas daugiau dėl teisinių ir kultūrinių tradicijų skirtumų įvairiose valstybėse, todėl šiame darbe minimos problemos nebus nagrinėjamos. Šiuo metu didžiausias dėmesys yra skiriamas vaikų pornografijos elektroninėje erdvėje problemai. Įstatymų, susijusių su vaikų pornografija, kūrimo problemą akcentuoja ir Europos Komisija. Tokiu būdu siekiama apsaugoti vaikus nuo seksualinio išnaudojimo. Dėl interneto paplitimo šiuo metu elektroninė erdvė tapo pagrindine priemone, kurios pagalba platinama tokio pobūdžio medžiaga. Todėl ši nauja pavojingos veikos forma turi būti nurodyta baudžiamuosiuose įstatymuose.

Pažeidimai, susiję su autorių teisėmis ir gretutinėmis teisėmis

Intelektualios nuosavybės teisių pažeidimai, ypač autorių teisių pažeidimai, yra vieni iš labiausiai internete paplitusių pavojingų veikų, darančių didžiulę žalą autorių teisių turėtojams. Apsaugotų darbų dauginimas ir platinimas internete be autorių teisių savininko leidimo yra ypač dažnas. Literatūroje teigiama, kad šiandien dėl interneto įtakos daugiausiai neteisėtai platinami kompiuterių programos ir kiti autorių teisėmis apsaugoti kūriniai. Tokiais apsaugotais darbais laikomi literatūros darbai, fotografijos, muzikos kūriniai, audiovizualiniai kūriniai ir kiti, kurie gali būti platinami panaudojant FTP serverius, elektroninį paštą, elektronines skelbimų lentas ir kt. Didžiulės darbų kopijavimo bei platinimo galimybės, kurias suteikia elektroninė erdvė, verčia įstatymo leidėjus baudžiamuosiuose įstatymuose nustatyti normas, uždraudžiančias tokias veikas. Trumpai paminėtina, kokios autorių teisės gali būti pažeidžiamos elektroninėje erdvėje. M. Racicot, M. S.Hayes teigia, kad internete gali būti pažeidžiamos net kelios autoriaus teisės. Gali būti pažeidžiama autoriaus teisė viešai demonstruoti, atgaminti kūrinį ir kt. Be to, pavojingos veikos gali pasireikšti informacijos apie autorių teisių valdymą sunaikinimu ar pakeitimu, autorių teisių techninių apsaugos priemonių pašalinimu ir pan.

2.2. Elektroninių nusikaltimų subjektai

Informacinės technologijos suteikia unikalias galimybes žmonėms, turintiems kriminalinių tikslų. Formuojasi organizuotos elektorninių nusikaltėlių grupės, kurias sudaro nariai iš viso pasaulio.

Elektroniniai nusikaltėliai, beje, yra pelnę didesnį visuomenės palankumą negu tradiciniai. Nuomonė, kad elektroninis nusikaltėlis yra mažiau pavojingas, neteisinga. Manoma, kad ateities grėsmė bus beveik proporcinga informacinių technologijų privalumams[35].

Kodėl reikia žinoti, kas yra elektroninių nusikaltimų subjektai? Atskirų kategorijų tipinių nusikaltimų išskyrimas, šių žmonių pagrindinių bruožų žinojimas leidžia optimaliai išskirti ratą žmonių, tarp kurių reikėtų ieškoti nusikaltėlio. Tai taip pat leidžia nustatyti konkretaus nusikaltėlio išaiškinimo būdus.

Daugelis elektroninių nusikaltimų tyrinėtojų šios rūšies nusikaltimų atsiradimą sieja vadinamųjų hakerių atsiradimu. Tačiau hakeris – ne vienintelė elektroninio nusikaltėlio rūšis. Nors į elektroninius nusikaltėlius reikėtų žiūrėti kaip į vieną visumą, tačiau pagal tam tikrus požymius išryškėja jų rūšys. Kaip matyti iš istorijos, elektroninius nusikaltimus vykdo įvairūs žmonės: studentai, mėgėjai, teroristai, nusikalstamų grupuočių nariai. Bet skiriasi jų padarytų nusikaltimų pobūdis. Asmuo, kuris patenka į kompiuterį neturėdamas nusikalstamų ketinimų, skiriasi nuo finansų institucijos darbuotojo, vagiančio pinigus iš klientų sąskaitų. Labai prieštaringai vertinami tipiški elektroninių nusikaltėlių įgūdžiai[36].

Elektroniniai nusikaltėliai yra iš skirtingų visuomenės sluoksnių. Jų amžius vidutininškai svyruoja nuo 6-7 iki 60 ir daugiau metų, įgūdžių lygis – nuo naujoko iki profesionalo.

Nors ankstesni tyrimai rodė, kad didžiausią grėsmę kelia darbuotojai (t.y. vidiniai nusikaltėliai), vėlesnės tendencijos parodė, kad labai išaugo nusikaltėlių iš išorės dalis. Todėl elektroniniai nusikaltimai jau nebegali būti taip dažnai vadinami vidiniais nusikaltimais. Manytina, kad išorinių nusikaltimų skaičiaus didėjimą, lyginant su bendru elektroninių nusikaltimų skaičiumi, lėmė sparti interneto plėtra ir penetracija. Ir nors įvairūs tyrimai dėl to, koks procentas elektroninių nusikaltimų įvykdomi iš vidaus ir iš išorės, skiriasi, manytina, kad tokie skirtingi duomenys yra dėl elektroninių nusikaltimų latentiškumo.

Egzistuoja daug („tyčinių“) elektroninių nusikaltėlių skirstymo būdų. Pateiktinas prof. S. Brenner siūlomas elektroninių nusikaltėlių skirstymas. Nusikaltėlių, vykdančių elektroninius nusikaltimus, rūšys pateikiamos atsžvelgiant į dažniausiai vykdomus elektroninius nusikaltimus (pvz., neteisėtą prieigą, sukčiavimą). Prof. Brenner elektroninius nusikaltėius skirsto į šias grupes[37]:

1. hakerius;
2. vidinius nusikaltėlius;
3. sukčiautojus;
4. persekiotojus (angl. *Stalkers*).

[35] Petrauskas R., Štitilis, D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 15.
[36] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 242.
37 Brenner S. W. *Cybercrime. Criminal Threats from Cyberspace*. Library of Congress Cataloging, 2010, p.121.

Hakeris – nauja kategorija, atsiradusi XX a.[38] Dažnas nusikaltimas elektroninėje erdvėje prasideda nuo neteisėtos prieigos. Pirmuosius hakerius galima net pavadinti „sportininkais-studentais“, nes jie neteisėtą prieigą traktuodavo kaip intelektualų iššūkį. Taigi pirmieji hakeriai į kompiuterių sistemas įsilaužda vo norėdami pasilinksminti, bet ne dėl finansinės naudos[39]. Šiuo metu šio tipo nusikaltėlių mažėja (dėl tos priežasties, kad vis mažiau įsilaužimų į kompiuterių sistemas vykdoma vien dėl sportinio intereso).

Vidinės atakos tapo labai didele grėsme kompiuterių saugumui. Mokslininkai vidinius nusikaltėlius apibūdina kaip individus, kurie būdami informacinių sistemų autorizuotais vartotojais (ar tokiais buvę), netikėtai padaro žalą. Tyrimai rodo, kad yra tam tikrų skirtumų tarp vidinių nusikaltėlių bankų ir finansų sektoriuje ir nusikaltėlių, dirbančių su kritine infrastruktūra. Pirmuoju atveju, tokių nusikaltėlių vykdomi elektroniniai nusikaltimai nėra labai sudėtingi ir kompleksiniai, dažniausiai panaudojamos ne techninės pažeidžiamos vietos (organizacijos politika ir kt.). Pagrindinis tokių nusikaltėlių tikslas dažniausiai būna finansinė nauda, bet ne žala organizacijai. Tuo tarpu, kritinės infrastruktūros atveju, kaip rodo tyrimai, 86 proc. elektroninių nusikaltimų padaro techniniai darbuotojai (sistemos administratoriai ir pan.). 84 proc. atvejų pagrindinis tokių nusikaltėlių motyvas – kerštas. Tokie nusikaltėliai organizacijai paprastai padaro labai daug žalos.

Sukčiavimas – vienas iš tų nusikaltimų, kurie atsiradus elektroninei erdvei, gali būti įvykdomi ir elektroninės erdvės pagalba. Tokie nusikaltėliai dažnai veikia iš kitos valstybės (pvz., Nigerijos sukčiavimo atvejai). Elektroninė erdvė suteikia galimybes tokiems nusikaltėliams savo aukas pasiekti praktiškai visame pasaulyje (t.y. ten, kur veikia interneto ryšys). Tarptautinis nusikaltimų pobūdis gerokai apsunkina tokių nusikaltėlių išaiškinimą.

Elektroninės erdvės persekiotojai elektroninius nusikaltimus vykdo veikiami labai įvairių motyvų. Vieni iš dažniausių elektroninio persekiojimo atvejų, kai persekiojamas buvęs partneris. Nors dažni atvejai, kai persekiotojas savo aukos gali ir nepažinoti.

Knygoje „Computer crime“[40] nusikaltėliai skirstomi į šias grupes:

1. hakerius;
2. „tipinius nusikaltėlius“;
3. vandalus.

Šios kategorijos tam tikrais atvejais persikerta. Geriausiai juos atskirti pagal motyvus. Hakeriai dažniausiai nori tik patekti į kompiuterių sistemą, nusikaltėlių pagrindinis motyvas – nauda, pinigai, o vandalai dažniausiai nori padaryti žalą.

1. Hakeriai

Šie žmonės labai gerai išmano kompiuterių programų bei kompiuterių tinklų kūrimo procesus, jų spragas. Labai didelė jų dalis yra kompiuterių technikos fanatai, nuolat ieškantys silpnų kompiuterių įrangos vietų, kurių nežino net patys įrangos kūrėjai. Dėl

[38] Higgins G. E. *Cybercrime: An Introduction to an Emerging Phenomen*. Library of Congress Cataloging, 2010, p. 129.
[39] Brenner S. W. *Cybercrime. Criminal Threats from Cyberspace*. Library of Congress Cataloging, 2010, p.121.
[40] Icove D. *Computer Crime: a Crimefighter`s Handbook*. O'Reilly Media, 2005, p. 62

šios priežasties tokie nusikaltimai vadinami „baltųjų apykaklių“ nusikaltimais. Šio tipo nusikaltimams įvykdyti nereikia didelių raumenų ar ginklų, jie vykdomi intelekto pagalba: įsibrauti į banką per atstumą gali asmuo, neturintis kojų, tačiau gerai išmanantis kompiuterių techniką ir turintis prieigą prie kompiuterių tinklo.

Bet kokios kategorijos nusikaltėliai gali padaryti tą patį, ką hakeriai, tačiau hakerių grupė unikali. Istoriškai savo „profesija“ jie susiviliojo iš nuobodulio arba norėdami pademonstruoti intelektualinius sugebėjimus. Jie gali veikti ištisą naktį, nes dažniausiai dieną būna mokykloje arba dirba.

Dauguma šių nusikaltėlių yra paaugliai. Nepaisant jų amžiaus, jie sėkmingai gali įsiveržti į bet kokio tipo kompiuterių sistemas – bankų, kompanijų, gamyklų, karines. 1989 metais keturiolikametis, panaudodamas asmeninį kompiuterį, įsilaužė į JAV karinių pajėgų navigacinę palydovų sistemą. Vėliau tiriant bylą buvo išsiaiškinta, kad įsilaužėlio karjerą jis pradėjo aštuonerių.

Kai kurie hakeriai veikia grupėmis, bet yra ir vienišių. Nepaisant jų protinių sugebėjimų, dauguma jų prastai mokosi mokykloje arba jos visai nelanko. Kai kurie, be bičiulių hakerių, turi mažai draugų. Su kitais hakeriais dažniau bendrauja ne būdami kartu, o per kompiuterių, socialinius tinklus. Susikūrusios hakerių grupės siekia būti neformalios.

Angliškai žodis „hacker“– reiškia juvelyrą, žmogų, kuris kruopščiai atlieka savo darbą. Analogiškai kompiuterių hakeris – tai žmogus, sugebantis juvelyriškai dirbti kompiuteriu. Kitais žodžiais tariant, tai žmogus, sugebantis padaryti tai, ko nesugebėtų padaryti paprastas vartotojas.

Pagal priklausomybę hakerius galima skirstyti į dvi grupes:

- vidinius darbuotojus;
- „svetimšalius“.

Taip pat hakeriai skirstomi į dar dvi pagrindines grupes:

- diletantus;
- profesionalus.

Diletantai paprastai būna jauni žmonės (17-25 m.), besimėgaujantys kompiuteriais, savo intelektualinėmis galimybėmis, padedančiomis įveikti kliūtis, kurių negali įveikti paprasti vartotojai.

Hakeris-diletantas paprastai siekia šių tikslų:

1) prasibrauti į sistemą, norėdamas nustatyti jos paskirtį;
2) gauti prieigą prie žaidimų;
3) pakeisti ir ištrinti duomenis, taip pat tyčia palikti savo pėdsakus.

Dauguma diletantų nepavojingi firmos ar organizacijos kompiuterių sistemai. Vieniems rūpi paprasčiausiai prisijungti prie kompiuterių tinklo, nes legaliai tai padaryti

trūksta lėšų, kiti skaito informaciją iš duomenų banko. Jiems įdomu surasti ir ištaisyti programines klaidas, sumaniai panaudoti tokias klaidas ar programos darbo šalutinius efektus. Tikėtina, kad jie yra didelės dalies virusų ir Trojos arklių autoriai[41].

Dažnai vien dėl malonumo ir asmeninio pasitenkinimo tokie hakeriai prasiskverbia į įvairių operacinių sistemų, turinčių daugiapakopę apsaugą, apsaugos sistemas. Šių hakerių motyvai paprasti: nori arba gauti prieigą prie žaidimų, arba pasirodyti. Pastarasis variantas daug rimtesnis, nes jie gali palikti sistemoje įsilaužimo žymes, sugadinant kokius nors failus arba paprasčiausiai palikti žinučių. Pavojingi bet kokie įsilaužimai į kompiuterių sistemą. Įsilaužėlis gauna prieigą prie vartotojų failų, kuriuose gali būti konfidenciali informacija. Kiekvienas pakankamai kvalifikuotas hakeris supranta, kad jį sugauti labai sunku. Patrauktas atsakomybėn, toks asmuo neretai atsiperka nedidelėmis baudomis.

Daug pavojingesni hakeriai-profesionalai, kurie aktyviai panaudoja savo žinias, kad padarytų žalą kitiems ar gautų asmeninės naudos. Veikti jie gali savo iniciatyva, taip pat kaip nusikalstamos grupuotės nariai arba vykdydami nurodymus. Dažniausiai hakeriai-profesionalai nusitaiko į bankus, draudimo kompanijas, įvairias firmas.

Hakeriai-profesionalai skirstomi į šias grupes:

1) nusikaltėlių grupuotes, siekiančias politinių tikslų;
2) asmenis, besistengiančius gauti informaciją pramoninio špionažo tikslais;
3) asmenų grupuotes, susiformavusias pasipelnymo tikslais.

Dvi paskutinės grupės beveik nesiskiria nuo „tipinių nusikaltėlių“. Hakeriai-profesionalai – tai pereinamoji grandis tarp hakerių ir „tipinių nusikaltėlių“. Kai hakerio pagrindinė veikla tampa susijusi su naudos gavimu, jis tampa nusikaltėliu.

Kad hakeriai pasiektų savo tikslus, jiems reikalingas betarpiškas priėjimas arba prieiga per kompiuterių tinklus. Betarpiškas priėjimas prie kompiuterių sistemos įmanomas tada, kai tam tikras pastatas yra blogai saugomas. Kai kurių darbuotojų, paliekančių savo kompiuterius be priežiūros, nerūpestingumas labai palengvina įsilaužėlių darbą. Gerai pasiruošusiam hakeriui nereikia daug laiko, kad įsibrautų į kompiuterių sistemą: 15-20 minučių (labai gerai po darbo) gali užtekti, kad prasiskverbtų į kompiuterių sistemą, apsaugotą daugiapakope apsauga. Pirmojo įsibrovimo metu gautų duomenų pakanka, kad išanalizuotų, per kiek laiko galima įsiskverbti į kompiuterių sistemą bet kuriuo metu[42].

Profesionalūs nusikaltėliai visada stengėsi maksimaliai sumažinti riziką. Nusikaltimų vykdymas kompiuterių tinklo pagalba leido jiems tapti praktiškai nesugaunamiems. Neretai kartu su jais dirba ir firmos darbuotojai arba neseniai iš firmos atleisti darbuotojai. Profesionalūs nusikaltėliai siekia tokių buvusių darbuotojų pagalbos, ypač tais atvejais, kai firmos kompiuterių tinklas gerai saugomas.

2. „Tipiniai nusikaltėliai“

Tai dažniausiai būna suaugę žmonės. Jie koncentruojasi ties dviem pagrindinėmis

[41] Petrauskas R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 18.
[42] Petrauskas R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 20.

veikomis: šnipinėjimu ir sukčiavimu bei piktnaudžiavimu.

Šnipinėjimas

Ši elektroninių nusikaltėlių kategorija – tai asmenys, kurie pavagia slaptą informaciją iš strategiškai svarbių ir kitų objektų. Į šią kategoriją įeina ir nusikaltėliai, pavagiantys informaciją iš teisėsaugos kompiuterių; taip pat industrinio špionažo agentai, dirbantys konkurentų firmoms ar užsienio vyriausybėms, pasirengusioms mokėti už informaciją.

Sukčiavimas ir piktnaudžiavimas

Apgavysčių ir piktnaudžiavimo naudojant kompiuterius atvejų sparčiai daugėja. Kriminalinės grupuotės – tiek vietinės, tiek tarptautinės – įsitraukia į elektroninius nusikaltimus kaip į tiesioginį nelegalių pajamų šaltinį. Nusikaltėliai supranta, kad vykdydami kompiuterinį sukčiavimą jie gali uždirbti daugiau pinigų ir tai daryti daug saugiau nei darant kitus įprastus nusikaltimus. Bankai visada traukė kompiuterinius nusikaltėlius. 1988 metais septynių įsilaužėlių grupė atliko operaciją, nukreiptą į vieną iš stambiausių Vakarų bankų. 70 mln. dolerių, kurie priklausė trims kompanijoms, jie neteisėtai pervedė iš pradžių į vieną Niujorko bankų, o po to į du Europos bankus. Pinigų pervedimai buvo sankcionuoti telefonu, todėl bankas atlikdavo kontrolinius skambučius, kad patvirtintų užklausimą. Tačiau nusikaltėliai padarė esminę klaidą – visus skambučius jie nukreipė į namus vienam iš bendrininkų. Kai pinigai buvo pervesti, trys kompanijos susisiekė su banku, kad išsiaiškintų, kas įvyko. Prasidėjo tyrimas ir telefono numeris, kuriuo buvo atliekami kontroliniai skambučiai, užvedė ant nusikaltėlių pėdsakų.

3. Vandalai

Ši kategorija dažniausiai nedaro nusikaltimų tam, kad parodytų savo intelektualinius sugebėjimus (kaip hakeriai) ar finansiniais, politiniais sumetimais (kaip elektroniniai nusikaltėliai). Vandalizmo motyvas dažnai būna kerštas už realų ar išgalvotą įžeidimą. Dažniausiai šios kategorijos žmonės būna pikti, paprastai pyksta ant konkrečios organizacijos, bet kartais būna tiesiog apskritai nusivylę gyvenimu. Vandalus apytikriai galima padalinti į dvi grupes, kurias būtų galima pavadinti naudotojais ir svetimšaliais. Naudotojai yra tie, kurie piktnaudžiauja teisėta prieiga prie kompiuterių sistemos. Svetimšaliai teisėtos prieigos prie sistemos neturi[43].

Pagal tolesnį elektroninių nusikaltimų skirstymą, egzistuoja hackeriai ir krackeriai. Remiantis naujuoju hakerių žodynu, krackeris apibrėžiamas taip: tas, kas pralaužia kompiuterių sistemos apsaugą. Hackeris apibrėžiamas kaip asmuo, kuris mėgaujasi programinėmis sistemomis, kad sustiprintų savo sugebėjimus, dirba iš entuziazmo. Ir hackeriai, ir krackeriai įsilaužia į kompiuterių sistemas, bet jų įsilaužimo motyvai skiriasi. Hackeriai įsilaužia tam, kad patikrintų savo intelektualinius sugebėjimus, tuo tarpu krackeriai piktaviliškesni ir daro žalą kompiuterių sistemoms. Dažniausi motyvai – naudos siekimas arba kerštas.

Reikėtų paminėti ir elektroninių nusikaltėlių klasifikaciją, paplitusią Rusijoje. Čia

[43] Petrauskas R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 21.

elektroninių nusikaltimų subjektai skirstomi į tris grupes[44]:

1. Pirmajai elektroninių nusikaltėlių grupei priklauso kompiuterių technikos profesionalai, programavimo žinovai. Jiems taip pat būdingas tam tikras fanatizmas bei išradingumas. Kai kurių autorių manymu, šie subjektai kompiuterių technikos priemones vertina kaip tam tikrą iššūkį jų profesionalioms žinioms. Būtent tai ir yra pagrindinis stimulas įvykdyti veikas, kurių didžioji dalis yra nusikalstamos. Reikia paminėti dar vieną šios grupės požymį – šie nusikaltėliai neturi jokių konkrečių tikslų pažeisti įstatymo. Praktiškai visus veiksmus jie atlieka norėdami pademonstruoti savo intelektualinius ir profesinius gebėjimus. Šios grupės atstovai yra gana žingeidūs, aukšto intelekto, taip pat turi tam tikro „sportinio azarto“. Jie bet kokiomis priemonėmis nori įrodyti savo pranašumą prieš kompiuterius. Paprastai tai ir paskatina juos padaryti nusikaltimą.

Kartais bėgant laikui šios kategorijos žmonės ne tik įgyja patirties, bet keičiasi ir jų interesai. Iš savo veiklos jie pradeda ieškoti materialinės naudos. Tokiu būdu mėgėjas-programuotojas virsta profesionaliu nusikaltėliu.

Taigi galima išskirti tokius nagrinėtos grupės požymius:

- nėra tam tikro išankstinio pasiruošimo, kad būtų įvykdytas konkretus nusikaltimas;
- nusikaltimo įvykdymo būdas turi būti originalus;
- nusikaltimui įvykdyti naudojamos buitinės kompiuterių technikos priemonės;
- nusikaltimo pėdsakai neslepiami.

2. Šiai grupei artima ir kita nusikaltėlių grupė, serganti naujomis psichikos ligomis, t.y. informacinėmis ligomis ir kompiuterinėmis fobijomis.

Nurodyti susirgimai kyla žmogui sistemingai pažeidžiant informacinį režimą: patiriant arba informacinį badą, arba informacinę perkrovą. Šių klausimų tyrimu užsiima gana nauja medicinos šaka – informacinė medicina. Žiūrint iš šios šakos pozicijų, žmogus suprantamas kaip universali, save reguliuojanti informacinė sistema su nustatytu biologinės informacijos balansu. Balansą pažeidus dėl vidinių ar išorinių destabilizuojančių veiksnių susergama įvairiomis informacinėmis ligomis, tarp kurių labiausiai paplitusios informacinės neurozės. Kai informacijos mažai, ateina informacinis badas, kai daug – žmogus kenčia nuo informacinės perkrovos (pasireiškia įvairūs stresai ir emociniai protrūkiai). Visa tai gali peraugti į informacinę ligą. Esant dabartiniam darbo kompiuterizavimui, daugelis darbuotojų patenka į stresines situacijas, kas kai kada baigiasi kompiuterine fobija. Tai ne kas kita, kaip profesinė liga. Jos simptomai

[44] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 247.

stokie: greitas nuovargis, staigūs kraujo spaudimo šuoliai, fiziškai ir audiovizualiai kontaktuojant su kompiuteriu, galvos svaigimas ir skausmas, galūnių drebėjimas ir t.t. Faktiškai atsiranda baimė prarasti savikontrolę.

Taigi elektroninius nusikaltimus gali vykdyti žmonės, sergantys minėtomis psichikos ligomis. Tiriant tokį elektroninį nusikaltimą, būtina skirti teismo psichiatrinę ekspertizę, kad būtų nustatyta kaltinamojo psichinė būklė nusikaltimo padarymo metu (ar tai nebuvo afekto būsena arba nepakaltinamumas).

Dažniausiai šios grupės nusikaltėliai iš dalies arba visiškai praradę kontrolę, fiziškai naikina kompiuterius (be nusikalstamų ketinimų).

Trečiąją grupę sudaro profesionalūs elektroniniai nusikaltėliai. Į šią grupę įeina žmonės su aiškiai išreikštais nusikalstamais ketinimais. Skirtingai nuo pirmųjų dviejų grupių, jų veikos nebūna vienkartinės. Dažniausiai jie slepia savo nusikaltimus. Paprastai šie žmonės būna gerai organizuotų grupių, aprūpintų specialia technika (neretai operatyvine), nariai. Tai kvalifikuoti specialistai, turintys techninį, aukštąjį juridinį ar ekonominį išsilavinimą. Būtent ši grupė visuomenei kelia didžiausią grėsmę. Pavyzdžiui, 79 % pinigų grobimų stambiu mastu įvykdo šie asmenys.

Galimos ir kitokios elektroninių nusikaltėlių pagal elektroninių nusikaltimų įvykdymo būdus klasifikacijos, pvz.:

1) krekeriai[45] (nuo angliško žodžio „cracker“) – asmenys, vykdantys įsilaužimus (įskaitant duomenų modifikavimą, blokavimą ar sunaikinimą) į įstatymo saugomas informacines sistemas;
2) frekeriai (nuo angliško žodžio „phreacker“) – asmenys, elektroninius nusikaltimus vykdantys panaudodami elektroninius ryšius, kai specialių priemonių pagalba slapta perimama konfidenciali informacija;
3) karderiai (nuo angliško žodžio „card“) – asmenys, vykdantys elektroninius nusikaltimus, susijusius su mokėjimo kortelių apyvarta.

2.3. Elektroninių nusikaltimų atlikimo būdai

Nusikaltimo padarymo būdas – fakultatyvinis bendrosios nusikaltimo sudėties požymis. Jei jis numatytas konkrečioje nusikaltimo sudėtyje, tampa būtinu požymiu. Būdas apibūdina objektyviąją nusikaltimo pusę. Jis parodo, kaip buvo padarytas nusikaltimas.

Kriminalistikoje nusikaltimo padarymo būdas suprantamas kaip subjekto elgesys iki nusikaltimo padarymo, nusikaltimo padarymo metu ir po nusikaltimo, paliekantis tam tikrus pėdsakus. Kitaip sakant, tai subjekto veiksmų, padarytų ruošiantis, vykdant bei slepiant nusikaltimą, kompleksas.

[45] Nors, kita vertus, krekeriais dažnai vadinami asmenys, nulaužinėjantys kompiuterių programų ar audiovizualinio turinio failų techninę apsaugą.

Žinios apie šiuos veiksmų būdus (rūšis), tam tikrų pėdsakų nustatymas labai palengvina elektroninių nusikaltimų tyrimą. Nusikaltimo padarymo būdas charakterizuoja nusikaltėlį, o tai leidžia geriau atlikti tyrimą.

Teisinėje literatūroje egzistuoja atskiros nuomonės dėl klausimų, susijusių su elektroninių nusikaltimų įvykdymo būdų išskyrimu, klasifikacija ir pavadinimais. Elektroninių nusikaltimų būdai yra labai įvairūs. Išsamų sąrašą sudaryti sunku, nes pačių veikų vystantis technikai vis daugėja. Tačiau pagal tam tikrus požymius juos galima skirstyti į grupes. Pagrindinis kvalifikuojantis požymis yra nusikaltėlio naudojami veiksmai, nukreipti gauti neteisėtą prieigą prie kompiuterinės įrangos įvairiais tikslais.

Apibendrinant literatūroje pateikiamus elektroninių nusikaltimų įvykdymo būdus, galima juos suskirstyti į 4 metodų grupes[46]:

I. perėmimo metodai;
II. neteisėtos prieigos metodai;
III. manipuliacijų metodai;
IV. kompleksiniai metodai[47].

I. Perėmimo metodai. Šiai grupei priskiriami elektroninių nusikaltimų įvykdymo būdai, kuriais nusikaltėlis gauna duomenis ir kompiuterinę informaciją, panaudodamas audiovizualinio ir elektromagnetinio perėmimo metodus, kuriuos plačiai naudoja teisėsaugos operatyvinės tarnybos.

1. **Tiesioginis perėmimas.** Naudojant šį būdą, prie kompiuterio komunikacinių linijų/elektroninių ryšių tinklų tiesiogiai prijungiama reikiama aparatūra. Norint atlikti tokius veiksmus, būtina atitinkama techninė bazė. Dažniausiai, pasirinkus šį būdą, betarpiškai prisijungiama prie kompiuterio, kompiuterių sistemos ar tinklo, pvz.: prie spausdintuvo linijos, ryšio kanalo kabelio, naudojamo duomenims persiųsti; arba prie kompiuterio tiesiogiai prisijungiamą per atitinkamą prievadą.
2. **Elektromagnetinis perėmimas.** Ne visi perėmimo įrenginiai reikalauja tiesioginio prisijungimo. Duomenis ir informaciją galima perimti ne tik ryšių kanalais, bet ir patalpose, kuriose yra komunikacijos priemonės, o taip pat tam tikru atstumu nuo jų. Toks metodas tapo galimas dėl elektrinių ir elektroninių prietaisų darbo metu atsirandančios emisijos efekto (kuriuo pasižymėdavo senosios kartos monitoriai). Emisijos efektas pasireiškia tuo, kad į aplinką išspinduliuojamos radijo bangos. Tačiau reikia pažymėti, jog skystųjų kristalų monitoriams nebūdingas aukščiau paminėtas emisijos efektas, todėl šis būdas praktikoje naudojamas vis rečiau.
3. **Pasiklausymo įrenginių panaudojimas.** Tai radioelektroninių įrenginių (pvz.: „blakių“) panaudojimas papildomai informacijai gauti. Apsauga nuo tokio informacijos nutekėjimo yra labai sudėtinga. Šį būdą galima įgyvendinti

[46] Reikia pažymėti, kad šioje ir kitose būdų grupėse kompiuterinės technikos priemonės gali būti ir kaip objektas, ir kaip nusikaltimo įvykdymo įrankis. Todėl būdų klasifikacija čia pateikiama remiantis plačiąja elektroninio nusikaltimo sąvoka.
[47] Petrauskas R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 25.

dvejopai:

1) įrenginius naudojant patalpoje;
2) įrenginius naudojant už patalpos ribų.

Pirmuoju atveju pasiklausymo įrenginys įtaisomas į informacijos apdorojimo įrenginių aparatūrą, į įvairius techninius įtaisus, komunikacines linijas, o taip pat į inžinierines-technines konstrukcijas, buities prietaisus. Gaunama garsinė informacija transliuojama radijo bangomis arba dedama į pastarojo įrenginio atmintį, jeigu jis tokią turi. Taip surenkama informacija apie darbo ypatybes su kompiuteriu ir kompiuterių tinklu, apie apsaugos lygmenį, dirbantį personalą, taip pat techninių priemonių garsinius signalus (šaukiamojo abonento numerio nustatymas ir t.t.).

Antruoju atveju akustiniai ir vibratoriniai informacijos fiksavimo davikliai montuojami inžinierinėse konstrukcijose, esančiose už saugomos patalpos ribų. Davikliai gali būti montuojami sienose, languose, duryse, ventiliacijos angose ir t.t. Tam nebūtina patekti į patalpą – užtenka priartėti prie jos iš išorės. Daviklis pastatomas vietoje arba per atstumą (informacija fiksuojama pro atidarytus langus ar duris).

4. **Informacijos fiksavimas ir atranka.** Tai taip pat pagalbinis būdas, kurį pasitelkus gaunama papildoma informacija apie dominantį objektą. Informacija renkama vizualiai stebint objektą. Tiesa, nagrinėjamas ne informacijos turinys, o informacijos cirkuliavimo schemos, forma ir t.t. Naudojama technika gana įvairi – tai ir buitinis binoklis, ir skaitmeninės vaizdo kameros, kurios gali būti įvairiai paslėptos ir t.t.
5. **Šiukšlių rinkimas.** Pasirinkus šį būdą, neteisėtai naudojamos informacijos proceso techninės liekanos (šiukšlės). Pažeidėjas turi vienintelį tikslą – surasti svarbią informaciją, pvz., įėjimo į sistemą kodus ir pan. Pažeidėjas ar jo padėjėjas pasirinktame objekte ieško šiukšlių (dokumentų, raštelių, popieriaus ar kitokių skiaučių, ant kurių būtų užrašyta svarbi informacija). Skiriami dvejopų šiukšlių paieškos variantai:

   a) paprastų;
   b) elektroninių.

   Ieškant paprastų šiukšlių, rizika yra minimali. Paprastai nusikaltėliai tai padaryti tiesiog paprašo techninio personalo ar valytojų, arba ieško patys. Ieškoma visur: ant darbo stalų, prie kompiuterio, ant grindų, stalčiuose, šiukšliadėžėse ir t.t. Praktikoje tai labai paplitęs būdas gauti svarbios informacijos ir paprastai didesnioji dalis žmonių visai nesilaiko slaptažodžių ar kitokių kodų naudojimo taisyklių.

   Ieškant elektroninių šiukšlių jau reikalinga kompiuterių įrangos žinovo pagalba. Šiuo atveju ieškoma tokio pat pobūdžio informacijos, tačiau ne fizinėje aplinkoje, o kompiuteryje (t.y. programų lygmenyje). Ne visa informacija iš kompiuterio operatyviosios atminties ištrinama, kurį laiką dar galima ją atkurti. Taip pat dalis naudotojų, kad nepamirštų, svarbią informaciją tiesiog

įrašo į pastoviąją atmintį.

II. Nesankcionuotos prieigos metodai. Tai veiksmai, kuriais siekiama gauti nesankcionuotą prieigą prie kompiuterio.

1. **„Paskui kvailį“.** Šis būdas yra labai paprastas ir naudojamas norint patekti į zonas su ribota prieiga. Pagrindas – žmogaus pastabumas. Pažeidėjas sudaro įspūdį, kad yra teisėtas tos zonos vartotojas (darbuotojas) ir laukia, kol į jį dominančią zoną eis teisėtas naudotojas. Tuomet tereikia paskubėti ir įeiti kartu. Čia, kaip renkant šiukšles, yra dvi sferos:
   a) fizinės patalpos;
   b) elektroninė erdvė (tiesiogiai prijungia terminalą prie teisėto vartotojo linijos arba pasinaudoja paliktu neišjungtu teisėto vartotojo kompiuteriu, kai pastarasis trumpam išeina).
2. **Įsilaužimas į kompiuterį ar sistemą.** Pažeidėjas, naudodamas specialią įrangą (pvz., paprastą telefoną) ir savo įgūdžius, bando pasijungti prie kito kompiuterių tinklo vartotojo. Pats pasijungimas prie kito vartotojo, kai pastarasis yra tinkle, nėra sudėtingas, tačiau vien prisijungimas dar nereiškia prieigos prie aukos resursų. Šiuos sunkumus bandoma įveikti naudojant įvairas programas ir pasitelkiant kitas hakerių gudrybes.
3. **Lėta atranka.** Nusikaltėlis neteisėtą prieigą prie kompiuterių sistemos atlieka aptikdamas silpnas jos apsaugos vietas. Toks būdas dažniausiai naudojamas tada, nusižiūrėta auka skiria mažai dėmesio savo kompiuterio sistemos apsaugai. Surastos silpnos vietos panaudojamos, tačiau šis būdas turi keblumą. Jeigu apsaugos sistemos architektūra pakeičiama, pažeidėjui tenka dirbti iš naujo.
4. **Klaidos paieška.** Skirtingai nei pasirinkus lėtos atrankos būdą, čia ieškoma ne silpnosios vietos, bet klaidos. Tokių klaidų atsiranda dėl logikos ar kokių nors kitų netikslumų kuriant apsaugos sistemą. Sistemos apsaugą užtikrina kompleksas veiksnių, vienas jų yra programinė įranga, t.y. konkrečios programos. O klaidos programose yra normalus reiškinys, nes jas kuria žmonės, be to, ne vienas, o didelė grupė programuotojų. Programa dažniausiai būna nemaža, be to, veikia tarp kitų programų. Taigi patikrinti, ar tokios programos funkcijos nepriekaištingai veikia visomis galimomis sąlygomis yra tiesiog neįmanoma, nes tam prireiktų ne vienerių metų. Taip pat gali pasitaikyti ir techninės įrangos klaidų.
5. **Liukas.** Šis būdas panaudojamas suradus klaidą programoje. Aptikus klaidą, toje vietoje programa šiek tiek pakeičiama, t.y. papildoma keliomis ar keliolika naujų komandų, kurias panaudodamas, pažeidėjas ateityje gali bet kada patekti į sistemą, apeidamas standartinius kelius. Tiesa, tokie liukai yra visose apsaugos sistemose, nes to reikia tikrinant tokią programą. Liukus gali žinoti programų autoriai.
6. **„Apsišaukėlis“ (Maskaradas).** Nusikaltėlis į kompiuterių sistemą patenka

apsimetęs teisėtu vartotoju. Nuo tokio pasikėsinimo neapsaugotos sistemos, kurios neturi asmens identifikavimo galimybių (pvz., pirštų atspaudų sulyginimas, balso atpažinimo procedūra ir t.t.). Pats paprasčiausias patekimo į tokias sistemas būdas – gauti teisėtų vartotojų kodus ir kitus identifikuojančius šifrus. Tai galima padaryti papirkus, įsigijus vartotojų sąrašą su visa būtina informacija, taip pat ir kitais būdais, tačiau tik reikalingas asmuo, turintis priėjimą prie minėto dokumento.

7. **Mistifikacija.** Pažeidėjas imituoja, pvz., serverio darbą (galima imituoti tik apsaugos sistemos darbo pradžią, t.y. užklausti vartotojo identifikavimo kodų). Aišku, pastarasis tuos kodus įveda ir taip pažeidėjas gali gauti juos. Šis būdas yra gana sudėtingas, jį įgyvendinti gali tik labai aukštos kvalifikacijos programuotojas ir tos apsaugos sistemos žinovas.
8. **Avarinė programa.** Bet kuriame didesniame kompiuterių centre yra speciali programa, kuri taikoma tik tam tikrais numatytais atvejais, pvz., sutrikus sistemos darbui. Ši programa leidžia greitai apeiti apsaugą. Gavęs tokią prieigą, nusikaltėlis gali viską.
9. **„Sandėlis be sienų“.** Tai natūralus sistemos trūkumas ar laikinas gedimas, dėl kurio pažeidėjas gali pasiekti ne tik jam skirtą programinį plotą, bet ir pasižiūrėti kaimynų failus. Tai tiesiog pasinaudojimas susidariusiomis aplinkybėmis.

III. Manipuliacijų metodai. Šiai elektroninių nusikaltimų įvykdymo būdų grupei priskiriami nusikaltėlių veiksmai, susiję su duomenų ar kompiuterio komandų manipuliavimo metodu panaudojimu. Šiais metodais dažnai pakeičiami buhalteriniai duomenys.

1. **Duomenų pakeitimas.** Paprastas ir gana dažnas nusikaltimų įvykdymo būdas. Tai tikrų duomenų pakeitimas arba naujų įvedimas dažniausiai atliekamas vykstant duomenų įvedimo ar išvedimo procesui. Toks būdas dažniausiai taikomas esant programoms, kurios atlieka kokių nors vertybių apskaitą, jų įvertinimą, paskirstymą ar registravimą ir pan. Pvz., pakoreguojamas apskaitomų vertybių sąrašas ar skaičius ir t.t.
2. **Kodo pakeitimas.** Iš esmės tai yra aukščiau minėtas būdas. Tai tik atskiro kodo ar funkcijos iškreipimas, nepakeičiant pačios programos funkcionavimo ir be detalios programos duomenų analizės neįmanoma pastebėti (pvz., neteisingai koduojamas tam tikrų sumų pervedimas).
3. **Trojos arklys.** Pasirinkus šį būdą, į svetimą programinę įrangą slapta įvedamos specialiai sukurtos programos, kurios patekdamos į informacines-skaičiavimo sistemas (paprastai imituodamos žinomas programas), pradeda atlikti naujas, teisėto savininko neplanuotas funkcijas. Tai vizuali maskuotė, nes ši programėlė įrašoma šalia kitos programos ar jos viduje, ir tik po to pati programa atlieka vienokio ar kitokio pobūdžio pakeitimus. Svarbu yra tai, kad programos veikimas dėl to nesikeičia. Tai labai panašu į liuką, tačiau čia toks liukas atidaromas ne įvedant reikiamas komandas, o toliau

pažeidėjui tiesiogiai nedalyvaujant, t.y. įvestoji programa pati atlieka kokias nors nelegalias funkcijas. Tokias operacijas Trojos arklys atlieka kiekvieną pakartotiną programos ciklą, kuris užkliudo patį Trojos arklį. Aptikti tokią programėlę labai sunku, nes tai tik keletas kodų, kurie niekuo neišsiskiria tarp kitų programos kodų. Kvalifikuoti specialistai šios programos paieškai dažniausiai išeikvoja daug laiko, kai kada iki 1 metų.

Šiuo būdu nusikaltėliai paprastai nuo kiekvienos operacijos tam tikrą sumą perveda į iš anksto atidarytą sąskaitą. Taip pat galimas pinigų kiekio padidinimas perskaičiuojant pinigus iš vienos valiutos į kitą, dirbtinai nedaug padidinant valiutos kursą.

4. **Kompiuterių virusai.** Tai ne kas kita, kaip Trojos arklio loginė moduliacija. Dažniausiai standartinis viruso algoritmas yra toks: „padaryk tą ir tą, paskui pereik prie kito ir atlik tą patį“. Tačiau dirbti pagal numatytą algoritmą virusas gali tik tuomet, kai yra atliekamos kokios nors komandos, t.y. procesorius atlieka tam tikrus skaičiavimus. Virusas tiesiog greta naudotojo darbo su kompiuteriu atlieka tam tikras komandas. Tokio tipo programos dažnai pridaro daug žalos.

   Reikia paminėti, kad nusikaltimo įvykdymas panaudojant virusą gali būti savarankiškas arba būti kitų kompleksinių būdų dalis. Antruoju atveju virusas bus kaip nusikaltimo maskuotė, turint tikslą jį nuslėpti.

5. **„Saliamis“.** Šis būdas atsirado tada, kai kompiuteriai buvo pradėti naudoti buhalterinėms operacijoms atlikti. Tai Trojos arklio taktika, kuri remiasi tiesiog aritmetinių sumų apvalinimu. Žiūrint iš nusikaltėlių pozicijos, tai vienas paprasčiausių nusikaltimo įvykdymo būdų. Šiuo būdu grobiamos piniginės lėšos, panaudojant buhalterines operacijas su slankiojo kablelio skaičiais. Tokiais atvejais pinigų sumos apvalinamos iki sveiko skaičiaus. Nusikaltėlių privalumas yra tas, kad kiekvienu atveju prarandamos labai mažos sumos – daromos tokios mažos paklaidos, kad yra tiesiog nepastebimos, o jeigu ir pastebimos, niekas nesiima aiškintis, kodėl taip yra. Pvz., nuo 101 259,49 atskaitoma 1 cnt. Šio būdo sėkmė priklauso nuo tokių operacijų skaičiaus ir ar jos lieka nepastebėtos.

6. **Loginė bomba.** Kai kada, vertinant iš taktinių pozicijų, grobimą geriau vykdyti tam tikromis numatomomis aplinkybėmis. Naudodami šį būdą, nusikaltėliai slapta į aukos programą įveda komandas, kurios turi suveikti tam tikromis aplinkybėmis. Tada įsijungia Trojos arklio algoritmas. Tiesa, analogiškas programėles naudoja sistemų programuotojai, siekdami patikrinti programą norimomis sąlygomis.

7. **Laiko bomba.** Visiškai toks pats būdas, kaip ir loginė bomba, tik šiuo atveju sąlyga yra data (tam tikras laikas). Pavyzdžiui, JAV labai išplito nusikaltimai, per kuriuos nusikaltėliai naudoja laiko bombas, norėdami pagrobti pinigines lėšas. Mechanizmas yra toks: nusikaltėliui esant šalyje A ir panaudojant anksčiau į banko automatizuotą tarptautinių atsiskaitymų sistemą įvestą laiko bombą

šalyje B, tam tikru nustatytu momentu pagrobiami pinigai. Visas operacijas kontroliuoja ta pati įvesta programa. Nusikaltėliams tereikia pasiimti pinigus iš sąskaitos.

8. **Asinchroninė ataka.** Šis metodas labai sudėtingas ir reikalauja labai gerų operacinės sistemos žinių. Operacinė sistema (OS) – tai kompleksas programinių priemonių, užtikrinančių informacinių procesų valdymą, funkcionuojant kompiuterių sistemai. Pagrindinė OS užduotis – užtikrinti maksimalų kompiuterių sistemos našumą, realizuojant įvairias kibernetines funkcijas: planavimo, valdymo. Priklausomai nuo kompiuterio modelio ir specifikacijos, naudojamos vienokios ar kitokios OS. OS sąsaja tokia sudėtinga, kad jų negali sukurti vienas asmuo, net labai kvalifikuotas. OS kolektyvai kuria net po kelerius metus. Todėl labai sunku patikrinti jų užbaigtumą įvairiomis situacijomis. Kitaip sakant, OS funkcionavimo ypatumai visomis sąlygomis lieka neaiškūs. Tuo ir naudojasi nusikaltėliai, organizuodami asinchronines atakas. Nusikaltėlis priverčia OS dirbti sunkiomis sąlygomis, dėl to informacijos apdorojimo valdymas iš dalies ar visiškai pažeidžiamas. Nusikaltėlis gali išnaudoti šią situaciją, kad atliktų pakeitimus operacinėje sistemoje ir nukreiptų ją įgyvendinti jo piktavališkus tikslus, be to, šie pakeitimai nebus pastebimi.
9. **Modeliavimas.** Programinės įrangos pagalba modeliuojama, kaip veiks įrenginys ar sistema. Pvz., daroma tikros programos, į kurią norima įsilaužti, kopija (panaši programa) ir žiūrima, kaip ji veiks, kai į ją bus bandoma įsilaužti. Viską išanalizavus, galima sudaryti įsilaužimo į tikrąją sistemą planą ir bandyti jį įgyvendinti.

   Esant reversiniam modeliavimui, padaromas konkrečios sistemos modelis (ar tiesiog jos kopija), įvedami realūs išvesties duomenys ir gaunami realūs teisingi rezultatai. Po to parenkami maksimaliai realybei artimi norimi rezultatai ir modelis „prasukamas“ atbuline seka iki išeitinio taško. Nusikaltėliui paaiškėja, kokias manipuliacijas su įvedamais duomenimis reikia atlikti, kad būtų gautas norimas rezultatas. Tokiu būdu gautus išvesties duomenis belieka įvesti į tikrąją sistemą.
10. **„Aitvaras“.** Dviejuose bankuose atidaromos dvi fiktyvių asmenų sąskaitos. Vėliau atliekami piniginiai pervedimai iš vienos sąskaitos į kitą, vis didinant pervedamą sumą. Kompiuterinė technika čia panaudojama iškreipti gaunamos tų bankų korespondencijos turiniui apie tai, kad kito banko sąskaitoje yra pakankamai pinigų, kad būtų garantuotas didesnis pervedimas ir t.t. Praktikoje dažniau atidaroma labai daug tokių sąskaitų ir naudojamasi daugelio bankų paslaugomis.
11. **Sukčiavimas (angl. *phishing*).** Tai duomenų vagystė. Nieko blogo neįtariantys interneto vartotojai įviliojami į kibernetinių nusikaltėlių, siekiančių piktavališkai pasinaudoti, užmestus informacijos rinkimo tinklus. Tai pastaruoju metu vis labiau populiarėjantis metodas. Pvz., vartotojas įveda slaptą informaciją, manydamas, kad tai daro oficialioje banko svetainėje, tačiau iš tikrųjų tai daro

nusikaltėlių sukurtoje svetainėje. Angliškame termine „phishing“ priebalsių junginys „ph“ vietoje „f“ pavartotas dėl šio nusikaltimo asociacijų su aštuntajame dešimtmetyje JAV populiaria nusikaltimų rūšimi – neteisėtu prisijungimu prie telefono tinklų ir mokesčio už telefoninius pokalbius nemokėjimu, kuris angliškai vadinasi „phone phreaking“. Paminėtina, kad 2009 metais buvo 50 000 aktyvių veikiančių tokio sukčių tinklalapių[48].

IV. Kompleksiniai metodai. Tai nėra kitokie tokių veikų atlikimo būdai. Elektroniniai nusikaltimai yra vykdomi pasitelkus du, kelis ar keletą aukščiau aprašytų būdų. Teisinga į šiuos nusikaltimus (tiksliau į jų atlikimo būdus) būtų žiūrėti kaip į kompleksą veiksmų, būdų, kurių kiekvienas elementas turi savų ypatybių.

Aukščiau pateiktas nusikaltimų įvykdymo būdų sąrašas nėra išsamus, jis nuolat keičiasi kartu su besikeičiančia technine ir programine įranga.

Paminėtina, kad ir kai kurios elektroninių nusikaltimų rūšys pasižymi savitais tokių nusikaltimų įvykdymo metodais. Pvz., nagrinėjant tapatybės vagystę elektroninėje erdvėje pastebima, kad dažniausiai pasitaiko šie nusikaltimai pasitelkiant modernias technologijas[49]; [50]:

- Įsibrovimas (angl. *hacking*). Dažniausiai sukčius į sistemą patenka apeidamas sistemos slaptažodžius, saugumo priemones. Ypač stengiamasi pasinaudoti saugumo spragomis, neapsaugotais belaidžiais, intraneto tinklais, taip pat ieškoma sistemų, kuriose dauguma apsaugos funkcijų yra išjungtos.
- Šnipinėjimo programa (angl. *spyware*). Tai programinė įranga, kuri be asmens žinios renka ir siunčia jo asmeninius duomenis nurodytu adresu. Dažniausiai pažeidinėjamas privatumas. Renkami ir fiksuojami asmens naršymo įpročiai, dažnai lankomų svetainių adresai. Rinkodaros kompanijos kasmet išleidžia milijonus dolerių, bandydamos nustatyti naudotojų išlaidų įpročius. Naršymo įpročiai paprastai nusiunčiami reklamos kompanijai, kuri ateityje pateikia tuos įpročius atitinkančią reklamą.
- Slaptažodžio žvejyba (angl. *phishing, Password phishing*). Pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar netikrais tinklalapiais bandoma išgauti prisijungimo prie informacinių sistemų slaptažodžius, kitus asmeninius duomenis. Dažniausiai tokio sukčiavimo aukos būna banko klientai. Siekiama sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Gauta informacija gali būti panaudota pasipelnymo tikslais vykdant nusikalstamas veikas, neteisėtus prisijungimus prie informacinių sistemų, vagystes iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes svetimomis mokėjimo kortelėmis. Taip pat egzistuoja trumpųjų žinučių sukčiavimai (angl.

[48] Kshetri N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, 2010, p. 27.

[49] Identity Theft Protection (2007) [interaktyvus, žiūrėta 2011-06-27]. <http://www.identitytheftsecurity.com/protect.shtml#phone>.

[50] Štitilis D., Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*, 2009, 50, p. 242.

Smishing), internetinės balso telefonijos sukčiavimai (angl. *vishing*), apgaulingi laiškai (angl. *scam*). Tai nėra baigtinis sukčiavimų sąrašas, kiti būdai ir metodai labai panašūs į ką tik aptartuosius.

- Trojos arklys (angl. *trojans*). Programa, sprendžianti kokį nors naudingą uždavinį, tačiau iš tikrųjų atliekanti kitą darbą. Naikina, sugadina kompiuteryje esančius duomenis, programas. Dažniausiai Trojos arkliai skirstomi į kirminams artimas programas, jos platina savo kopijas kompiuterių tinkluose. Kita rūšis – nuotolinio valdymo programos. Tai įprastos programos, kurios naudojamos nuotoliniam sistemų administravimui. Pavojingiausios programos pasisavina informaciją, ją persiunčia tretiesiems asmenims, dažnai net naudoja paprastą el. paštą ar svetaines.
- Apgaulinga IP taktika (angl. *pharming*). Siekiama nukreipti vienos svetainės srautą į kitą. Tai gali būti atliekama pakeitus pagrindinio kompiuterio nustatymus arba pasinaudojus sričių vardų serverių (DNS) eksploatavimo pažeidimais. Pažeisti sričių vardų serveriai vadinami užnuodytais (angl. *dns cache poisoning*).
- Pakartojimo ataka (angl. *replay attack*). Mėginama prisijungti prie kompiuterio tinklo, siekiant pakartotinai išsiųsti vartotojo informaciją. Jeigu informacija koduojama, galima pakartoti tą patį duomenų siuntimą tikintis, kad serveris patikės, jog tai tas pats vartotojas[51].

3. TEISINIAI ELEKTRONINIŲ NUSIKALTIMŲ ASPEKTAI

3.1. Elektroninių nusikaltimų reglamentavimas tarptautiniu ir ES mastu

Tarptautiniu mastu elektroninių nusikaltimų sritį reguliuoja (teisines priemones koordinuoja) šios organizacijos: Europos ekonominio bendradarbiavimo ir vystymo organizacija (OECD), Europos taryba, Jungtinių tautų organizacija, Pasaulio prekybos organizacija, Europos Komisija ir kt.

3.1.1. Konvencija dėl elektroninių nusikaltimų

Svarbiausias tarptautinės teisės aktas elektroninių nusikaltimų srityje – 2001 m. Konvencija dėl elektroninių nusikaltimų CETS Nr. 185 (priedas Nr. 1). Šis teisės

[51] Štitilis D., Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai.* 2009, 50: 239-247.

aktas mokslinėje literatūroje laikomas vienu iš sistemingiausių tarptautinių teisės aktų, reguliuojančių „žalingas“ ir kriminalines veikas panaudojant kompiuterį[52].

Atsižvelgiant į tai, jog elektroninėje erdvėje vykdomos veikos yra pavojingos visuomenei, nusikaltėlio buvimo bei nusikaltimo padarymo vieta dažnai nesutampa, atskirų valstybių įstatymai yra apriboti jų teritorija, elektroninė erdvė leidžia atlikti naujo tipo pavojingas veikas, bei pripažįstant, jog pavojingų veikų, vykdomų elektroninėje erdvėje, teisinis reglamentavimas yra nepakankamas, siekiant apsaugoti visuomenę nuo tokių nusikaltimų, *inter alia* priimant tam tikrus norminius aktus bei skatinant tarptautinį bendradarbiavimą, 2001 metais buvo pasirašyta Konvencija dėl elektroninių nusikaltimų[53]. Konvencijos projektą parengė Europos Tarybos ekspertai kartu su JAV, Kanada, Japonija ir kitomis valstybėmis, kurios nėra šios organizacijos narės. Tai pirmasis tarptautinis norminio pobūdžio dokumentas, skirtas spręsti nusikalstamų veikų kompiuterių tinkluose problemoms. 2001 m. lapkričio 8 d. Konvencijai dėl elektroninių nusikaltimų pritarė užsienio reikalų ministrai, o Europos Tarybos šalys narės šią konvenciją pasirašė 2001 m. lapkričio 23 d. Konvencijos įsigaliojimo sąlyga – 5 ratifikacijos (iš jų – bent 3 Europos Tarybos valstybių narių). Ši sąlyga buvo įvykdyta ir Konvencija įsigaliojo 2004 m. liepos 1 d. Lietuva Konvenciją pasirašė 2003 m. birželio 23 d., o ratifikavo 2004 m. kovo 18 d.

2011 m. balandžio mėn. Konvenciją buvo pasirašiusios 30 valstybės, ratifikavo 17. Kadangi iš viso yra 195 valstybės, konvencija labai minimaliai įtakoja globalią kovą su elektroniniais nusikaltimais[54]. Todėl konvencija gali būti svarbus, bet ne vienintelis teisinis dokumentas kovojant su elektroniniais nusikaltimais.

Konvencijos struktūra ir turinys aptartini detaliau. Konvenciją sudaro trys pagrindiniai skyriai: I. Sąvokos; II. Priemonės, kurių reikia imtis nacionaliniu lygiu bei III. Tarptautinis bendradarbiavimas. Pirmojo skyriaus 1 skirsnyje (Konvencijos 2-11 str.) Konvencijos Šalys įpareigojamos kriminalizuoti Konvencijoje numatytas veikas, taip pat nustatyti juridinių asmenų atsakomybę. Antrajame skirsnyje Konvencija nustato reikalavimus Konvencijos Šalimis tampančių valstybių procesinėms teisės normoms, įpareigoja imtis priemonių, būtinų operatyviai išsaugoti laikomus kompiuterių, srauto duomenis, juos atskleisti ar pateikti, surinkti srauto duomenis realiuoju laiku, įrašyti tokius duomenis ir pan. Pastarųjų proceso veiksmų atlikimas siejasi su pagrindinėmis žmogaus teisėmis ir laisvėmis, jų apsauga. Todėl pati Konvencija numato, kad minėtų veiksmų atlikimas turi būti suderinamas su pagrindiniais tarptautiniais dokumentais žmogaus teisių ir laisvių apsaugos srityje. Trečiajame skyriuje Konvencija įtvirtina nuostatas, skirtas ekstradicijos bei savitarpio pagalbos reglamentavimui. Visos Konvencijos 2-11 str. apibrėžtos veikos yra pripažįstamos nusikaltimais, už kuriuos asmenys gali būti išduodami vienos Susitariančiosios Šalies kitai Susitariančiajai Šaliai. Konvencija taip pat įpareigoja Susitariančiąsias Šalis teikti skubią ir visapusišką savitarpio pagalbą tiriant ar nagrinėjant baudžiamąsias bylas dėl elektroninių nusikaltimų. Tuo tikslu

[52] Williams M. *Virtually criminal: Crime, deviance and regulation online*. New York: Routledge, 2006, p. 33.
[53] Štitilis D. Teisinės atsakomybės pagrindų už neteisėtas veikas elektroninėje erdvėje nustatymo prolemos. Disertacija. Vilnius: 2002, p. 77.
[54] Brenner S. W. *Cybercrime. Criminal Threats from Cyberspace*. Library of Congress Cataloging, 2010, p. 209.

Konvencijos 35 str. įpareigoja Susitariančiąsias Šalis paskirti 24 valandas per parą ir 7 dienas per savaitę veikiančią instituciją, kuri galėtų teikti technines konsultacijas ir atlikti Konvencijoje nurodytus veiksmus.

3.1.1.1. Konvencijos dėl elektroninių nusikaltimų nuostatos dėl materialinės teisės

Konvencijos pirmojo skyriaus pirmajame skirsnyje, kuris susijęs su materialine teise, siūloma nustatyti teisinės atsakomybės pagrindus už šias pavojingų veikų rūšis:

- ➤ konfidencialumo, duomenų vientisumo, kompiuterių duomenų ir sistemų pažeidimus (neteisėta prieiga, neteisėtas perėmimas, įsikišimas į duomenų apdorojimo procesą, įsikišimas į kompiuterių sistemų darbo procesą, piktnaudžiavimas kompiuteriniais įrenginiais);
- ➤ su kompiuteriais susijusius pažeidimus (sukčiavimas, susijęs su kompiuteriais; klastojimas, susijęs su kompiuteriais);
- ➤ pažeidimus, susijusius su turiniu (pažeidimai, susiję su vaikų pornografija);
- ➤ pažeidimus, susijusius su autorių teisėmis ar gretutinėmis teisėmis.

Konvencijos nuostatos, susijusios su materialine teise (t.y. teisinės atsakomybės pagrindų už pavojingas veikas elektroninėje erdvėje nustatymu)[55]:

1) *konfidencialumo, duomenų vientisumo, kompiuterių duomenų ir sistemų pažeidimai*

Neteisėta prieiga. Konvencijos 2 straipsnyje numatyta, jog „turi būti priimtos įstatymų normos, pagal kurias būtų nustatyti baudžiamosios atsakomybės pagrindai už tyčinę prieigą prie kompiuterių sistemos, neturint tam teisės“. Šia nuostata siekiama, kad būtų nustatyta baudžiamoji atsakomybė už veikas, keliančias pavojų kompiuterių sistemų ir duomenų saugumui (t.y. konfidencialumui, integruotumui ir prieinamumui), t.y. angliškai vadinamas „Hacking“, „Cracking“, „Computer trespass“. Tame pačiame Konvencijos straipsnyje nurodoma, kad nustatant baudžiamosios atsakomybės pagrindus, gali būti reikalaujama, jog nusikaltimas būtų padaromas pažeidžiant saugumo priemones, siekiant gauti kompiuterinę informaciją arba turint nesąžiningą tikslą, arba kai veika yra susijusi su kompiuterių sistema, kuri sujungta su kita kompiuterių sistema. Anksčiau paminėta formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę nustatant baudžiamosios atsakomybės pagrindus už neteisėtą prieigą. Galima konstatuoti, jog Konvencijoje laikomasi nuostatos, kad tyčinė prieiga prie kompiuterių sistemos neturint tam teisės turi būti įvardijama kaip neteisėta veika.

Neteisėtas perėmimas. Konvencijos 3 straipsnyje nurodyta, jog „*turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį*

[55] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006, p. 234.

informacijos perėmimą, neturint tam teisės, kai tai padaroma pasinaudojus techninėmis priemonėmis bei informacija, perimama neviešai siunčiant kompiuterinę informaciją į, iš ar viduje kompiuterių sistemos (įskaitant ir elektromagnetinį kompiuterio sistemos spinduliavimą)". Šia nuostata siekiama apsaugoti duomenų komunikacijų privatumą, kuris apsaugotas Europos žmogaus teisių konvencijos 8 straipsniu. Paminėta veika gali būti vykdoma neteisėtai perimant kompiuterinę informaciją, siunčiant ją elektroniniu paštu, persiunčiant failus (sauginius) ir kt. Anksčiau paminėtos nuostatos tekstas praktiškai buvo perkeltas iš Rekomendacijos (89)9. Reikia pažymėti, jog remiantis Konvencijos komentaru, sąvoka „neviešas" turėtų būti vartojama kalbant apie informacijos perdavimo neviešumą, o ne pačios perduodamos informacijos neviešumą. Tame pačiame Konvencijos straipsnyje nurodyta, jog nustatant baudžiamosios atsakomybės pagrindus už paminėtą veiką, gali būti reikalaujama nesąžiningo tikslo ar kad veika būtų susijusi su kompiuterių sistema, kuri prijungta prie kitos kompiuterių sistemos. Konvencijos formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę nustatant baudžiamosios atsakomybės pagrindus už neteisėtą kompiuterinės informacijos perėmimą. Reikia paminėti, jog formuojant pažeidimo aprašymą buvo atsisakyta techninių apsaugos priemonių pažeidimo požymio, nes tokiu atveju būtų saugoma tik koduota kompiuterinė informacija.

Įsikišimas į duomenų apdorojimo procesą. Konvencijos 4 straipsnyje nustatyta, jog „*turi būti priimtos teisės normos, nustatančios baudžiamąją atsakomybę už tyčinį kompiuterinės informacijos sunaikinimą, ištrynimą, pakeitimą, sugadinimą, neturint tam teisės"*. Šios nuostatos tikslas yra apsaugoti tinkamą kompiuterinės informacijos apdorojimą, tinkamą išsaugotos kompiuterinės informacijos ar kompiuterių programų naudojimą. Konvencijoje taip pat nurodoma, jog nustatant baudžiamosios atsakomybės pagrindus už paminėtą veiką, gali būti reikalaujama didelės žalos. Taigi ši Konvencijos formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę.

Įsikišimas į kompiuterių sistemos darbo procesą. Konvencijos 5 straipsnyje nustatyta, jog „*turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį pavojingą kompiuterių sistemos darbo trukdymą, kuris pasireiškia kompiuterinės informacijos įvedimu, perdavimu, sunaikinimu, ištrynimu, sugadinimu, pakeitimu*". Ši nuostata panaši į Rekomendacijos (89)9 nuostatą „Sabotažas, susijęs su kompiuteriais" ir turi tikslą kriminalizuoti trukdymą teisėtai naudoti kompiuterių sistemą, įskaitant telekomunikacijų įrenginius, naudojant ar darant įtaką kompiuterinei informacijai. Šiame Konvencijos straipsnyje nesiūloma įvesti jokių papildomų požymių nustatant baudžiamosios atsakomybės pagrindus už anksčiau paminėtą veiką. Pažymėtina, jog Konvencijos formuluotė valstybėms narėms nepalieka veikimo laisvės nustatant baudžiamosios atsakomybės pagrindus už neteisėtą įsikišimą į duomenų apdorojimo procesą.

*Piktnaudžiavimas įrenginiais(*angl. *Misuse devices).* Konvencijos 6 straipsnyje nustatyta, jog „*turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį:*

a) *įrenginio (priemonės), įskaitant kompiuterio programą, sukurto ar*

pritaikyto bet kokiam iš pažeidimų, nurodytų Konvencijos 2-5 straipsniuose, padaryti, taip pat kompiuterinio slaptažodžio, prieigos kodo ar panašių duomenų, kuriais pasinaudojus galima prieiti prie kompiuterių sistemos, gaminimą, pardavimą, parūpinimą, importą, platinimą ar kitu būdu padarymą prieinamus;

b) *įrenginio (priemonės), įskaitant kompiuterio programą, sukurto ar pritaikyto bet kokiam iš pažeidimų, nurodytų Konvencijos 2-5 straipsniuose, padaryti, laikymą"*. Tačiau Konvencijoje nurodyta, jog galima nustatyti, kad baudžiamoji atsakomybė kyla tik tuo atveju, jei laikoma keletas tokių įrenginių (priemonių), tuo paliekant valstybėms narėms tam tikrą pasirinkimo laisvę.

Ši nuostata skirta atskiru nusikaltimu įvardyti tyčinį specifinių neteisėtų veikų, susijusių su įrenginiais (priemonėmis) ar prieigos informacija, padarymą, siekiant įvykdyti kitus Konvencijoje paminėtus nusikaltimus pažeidžiant kompiuterių sistemų ar duomenų konfidencialumą, integruotumą ar prieinamumą. Reikia paminėti, jog Konvencijoje paliekama teisė iš viso nenumatyti baudžiamosios atsakomybės pagrindų už kompiuterinio slaptažodžio, prieigos kodo ar panašių duomenų, kuriais pasinaudojus galima prieiti prie kompiuterių sistemos, pardavimą, platinimą ar kitu būdu padarymą prieinamus. Paminėtina, jog siekiant atriboti pavojingas veikas, įvestas svarbus požymis – tikslas įvykdyti pažeidimus, susijusius su kompiuterių panaudojimu. Tokiomis nuostatomis aiškiai įvardijama, jog priemonės, skirtos teisėtam kompiuterių sistemų testavimui, nepatenka į teisinės atsakomybės pagrindų veikimo sferą.

2) *Su kompiuteriais susiję pažeidimai*

<u>*Klastojimas, susijęs su kompiuteriais.*</u> Konvencijos 7 straipsnyje nustatyta, jog „*turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį (taip pat neturint tam teisės) kompiuterių duomenų įvedimą, pakeitimą, ištrynimą, dėl to gaunami neautentiški duomenys (informacija), siekiant, jog jie būtų laikomi autentiškais*". Šios nuostatos tikslas yra nustatyti paralelią atsakomybę, kaip ir atsakomybę už materialių dokumentų klastojimą, t.y. pašalinti baudžiamųjų įstatymų spragas, susijusias su atsakomybės pagrindų nustatymu už tradicinį klastojimą, kai atitinkami įstatymai netaikomi elektroniniams duomenims. Kadangi vis daugiau sandorių sudaroma elektronine forma, vis daugiau žmonių veiklos perkeliama į elektroninę erdvę, tokia paminėta nuostata yra ganėtinai svarbi. Reikia taip pat paminėti, jog šiame straipsnyje valstybėms narėms palikta pasirinkimo laisvė, nustatant baudžiamosios atsakomybės pagrindus už minėtą veiką, reikalauti tikslo apgauti ar kito nesąžiningo tikslo.

<u>*Sukčiavimas, susijęs su kompiuteriais.*</u> Konvencijos 8 straipsnyje nustatyta, jog „*turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį (taip pat neturint tam teisės):*

a) kompiuterinės informacijos įvedimą, ištrynimą;

b) bet kokį įsikišimą į kompiuterių sistemos funkcionavimą,

dėl to padaroma žala, turint apgavikišką ar nesąžiningą tikslą gauti materialinę naudą sau ar kitam". Ši nuostata susijusi su naujos technologinės revoliucijos, dėl kurios atsirado unikalios galimybės vykdyti ekonominius nusikaltimus elektroninėje erdvėje, atėjimu. Kadangi kompiuterių sistemose apdorojama informacija (pvz., susijusi su pinigais) pasidarė labai vertinga, kai kuriais atvejais netgi vertingesnė už nekilnojamąjį turtą, šios nuostatos įgyvendinimas tapo būtinas. Reikia paminėti, jog šiame straipsnyje nepaliekama jokios veikimo laisvės nustatant baudžiamosios atsakomybės pagrindus už nurodytą veiką.

3) *Pažeidimai, susiję su turiniu*

<u>Pažeidimai, susiję su vaikų pornografijos medžiaga.</u> Konvencijos 9 straipsnyje nustatyta, jog „*turi būti priimtos teisės normos, nusikalstamomis veikomis įvardijančios tyčines (taip pat neturint tam teisės) veikas:*

a) medžiagos su vaikų pornografija gaminimą, siekiant ją platinti per kompiuterių sistemą;

b) medžiagos, susijusios su vaikų pornografija, padarymą prieinama (taip pat siūlymą) per kompiuterių sistemą;

c) medžiagos, susijusios su vaikų pornografija, platinimą ar siuntimą per kompiuterių sistemą;

d) medžiagos, susijusios su vaikų pornografija, siuntimą per kompiuterių sistemą sau ar kitam;

e) medžiagos, susijusios su vaikų pornografija, turėjimą kompiuterių sistemoje ar įrenginyje, galinčiame saugoti kompiuterinę informaciją".

Šiomis nuostatomis siekiama sustiprinti vaikų teisines apsaugos priemones, įskaitant jų apsaugą nuo seksualinio išnaudojimo, modernizuojant baudžiamosios teisės normas, siekiant kovoti su veikomis, kai panaudojant kompiuterių sistemas bei kompiuterių tinklus įvykdomi seksualiniai pažeidimai prieš vaikus. Konvencijos komentare pažymima, jog nors daugelis valstybių yra kriminalizavusios tradicines veikas, susijusias su vaikų pornografijos panaudojimu ir platinimu, tačiau nauja tokios nelegalios veiklos forma (pvz., vykdant per internetą) taip pat turėtų būti numatyta baudžiamuosiuose įstatymuose. Šiame straipsnyje nustatyta pasirinkimo laisvė nenustatyti baudžiamosios atsakomybės už išvardytas veikas, nurodytas d) ir e).

4) *Pažeidimai, susiję su autorių teisėmis ar gretutinėmis teisėmis*

Konvencijos 10 straipsnyje nustatyta, jog „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už autorių teisių ir gretutinių teisių pažeidimą (pagal įstatymus, priimtus remiantis tarptautiniais dokumentais: (Berno konvencija dėl literatūros ir meno kūrinių apsaugos ir kiti)), padarytą naudojant kompiuterių sistemą, esant komerciškam tikslui". Tačiau tame pačiame straipsnyje nustatoma, jog už tokias veikas baudžiamoji atsakomybė gali būti ir nenumatyta, jei yra numatyta kitų pakankamų priemonių ir laikomasi visų tarptautinių įsipareigojimų autorių

teisių ir gretutinių teisių srityje. Svarbios yra PINO (Pasaulio intelektualios nuosavybės organizacijos) autorių teisių bei PINO atlikimų ir fonogramų sutartys, nes jos itin pakeičia tarptautinę intelektualios nuosavybės apsaugą, ypač susijusią su apsaugotos medžiagos padarymu prieinama per internetą „pagal pareikalavimą“. Pavyzdžiui, 1996 m. PINO autorių teisių sutarties 6 straipsnyje platinimo teisė apibrėžiama taip: literatūros ir meno kūrinių autoriai turi išimtinę teisę suteikti leidimą padaryti jų kūrinių originalus ar jų kopijas viešai prieinamus, juos parduodant ar kitaip perduodant nuosavybėn[56].

3.1.1.2. Konvencijos dėl elektroninių nusikaltimų nuostatos dėl proceso teisės

Vienas iš pagrindinių Konvencijos tikslų – ne tik unifikuoti nacionalinius baudžiamuosius įstatymus dėl elektroninių nusikaltimų[57], bet ir tobulinti nacionalinę baudžiamojo proceso teisę. Tokie elektroninių nusikaltimų požymiai kaip globalumas, elektroninė veikos forma, sukuria gana rimtas kliūtis minimų nusikaltimų tyrimui. Viena iš pagrindinių problemų kovojant su elektroniniais nusikaltimais, yra nusikaltimo subjekto identifikavimas, taip pat nusikalstamos veikos masto ar poveikio įvertinimas[58]. Taip pat iššūkį kelia elektroninės informacijos, kuri gali tapti nusikalstamos veikos įrodymu, pažeidžiamumas, galimybė ją pakeisti ar sunaikinti. Užsienio valstybių praktika rodo, kad dažnai neužtenka galiojančių procesinių normų, kurios istoriškai pritaikytos tradicinių nusikaltimų tyrimui (pvz., kratos išplėtimo kompiuterių tinkluose problema).

Konvencijoje išskirtas atskiras skirsnis, skirtas vienodinti valstybių nacionalinių įstatymų proceso normoms. Šiuo 2 skirsniu siekiama tradicines procesines priemones, tokias kaip kratą ir poėmį, pritaikyti elektroninei aplinkai. Taip pat, siekiant tradicines įrodymų rinkimo priemones, pvz., kratą, poėmį, padaryti efektyvias besikeičiančioje elektroninėje aplinkoje, nustatomos tokios naujos priemonės, kaip operatyvus laikomųjų kompiuterių duomenų išsaugojimas ir pan. Išskirtinos šios toliau nagrinėtinos pagrindinės proceso teisės skirsnio nuostatos dėl procesinių priemonių: operatyvus laikomųjų kompiuterių duomenų išsaugojimas, laikomųjų kompiuterių duomenų paieška ir poėmis bei kompiuterių duomenų surinkimas realiuoju laiku.

Konvencijos apžvalgoje teigiama, kad Lietuva, siekdama įgyvendinti Konvencijos nuostatas, pakeitė Lietuvos Respublikos baudžiamojo proceso kodeksą[59]. Prisijungus prie Konvencijos, Lietuvos Respublikos baudžiamojo proceso kodeksas buvo papildytas

[56] Štitilis D. *Teisinės atsakomybės pagrindų už neteisėtas veikas elektroninėje erdvėje nustatymo prolemos*. Disertacija. Vilnius: 2002, p. 82.

[57] Terminas „elektroniniai nusikaltimai“ šiame straipsnyje bus vartojamas atsižvelgiant į Elektroninių nusikaltimų konvencijoje siūlomą veikų sąrašą, ir tuo pačiu bus platesnis nei „informatikos nusikaltimų“ terminas.

[58] Explanatory Report to the Convention on Cybercrime (adopted 8 November 2001,the Convention has been opened for signature in Budapest, on 23 November 2001), 133 p. [interaktyvus, žiūrėta 2011-06-21]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

[59] Survey on the Cybercrime Convention (CETS 185) and its additional protocol (CETS 189). European Committee on Crime Problems. [interaktyvus, žiūrėta 2011-06-28]. p. 4. <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_en.asp>.

bei pakeistas (pvz., kodekso 154 straipsnio papildymas antrąja dalimi[60]). Tačiau ar įstatymo leidėjas identifikavo visas su elektroniniais nusikaltimais susijusias procesines problemas, kurias bandoma spręsti Konvencijos proceso teisės skirsnio pagalba?

Operatyvus laikomųjų kompiuterių duomenų išsaugojimas

Konvencijoje dėl elektroninių nusikaltimų teigiama, kad „*kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgalinant jos kompetentingas institucijas nurodyti arba panašiai pasirūpinti operatyviu konkrečių kompiuterių duomenų, įskaitant srauto duomenis, laikomus kompiuterių sistemoje, išsaugojimu, ypač, kai yra pagrindo manyti, jog tie kompiuterių duomenys gali būti nesunkiai prarasti arba pakeisti*“[61]. Konvencijos 17 straipsnyje taip pat reglamentuojamas minimų išsaugotų duomenų atskleidimo galimybės užtikrinimas, o 18 straipsnyje – nurodymas dėl duomenų pateikimo.

Poreikis išsaugoti kompiuterių duomenis gali kilti tais atvejais, kai tyrimo nustatyta, jog tam tikri kompiuterių duomenys kitų duomenų srauto sudėtyje yra laikomi atitinkamo paslaugų teikėjo serveryje, kur teikėjas verslo tikslais ši srautą kaupia už tam tikrą laikotarpį. Tam, kad reikiama informacija iš duomenų srauto būtų išskirta bei išimama, reikalinga laikina duomenų apsauga. Tai įmanoma įgyvendinti tik tuo atveju, jei tyrimo organai turės atitinkamas teises įpareigoti paslaugų teikėją išsaugoti saugomus kompiuterių duomenis[62].

Ši priemonė taikytina tuo atveju, kai kompiuterių duomenys jau išsaugoti. Tačiau tyrimui svarbūs kompiuterių duomenys, nors ir išsaugoti, per trumpą laiką gali būti ištrinami. Pavyzdžiui, praktikoje galima situacija, kai paslaugos teikėjo užfiksuoti kompiuterių duomenys kompiuterių sistemoje saugomi ne ilgiau nei kelios valandos ar kelios paros. Laikomų duomenų sunaikinimą gali įtakoti teisės aktų reikalavimai. Tuo atveju, jei kompiuterių duomenys laikytini asmens duomenimis, asmens duomenų apsaugą reglamentuojantys teisės aktai reikalauja tokius duomenis sunaikinti (arba padaryti anonimiškus) iš karto po to, kai šie duomenys tampa nereikalingi ūkinei veiklai užtikrinti.

Paminėtina, jog Konvencijos rengėjų nuomone, tokia teisė įpareigoti subjektą išsaugoti laikomuosius kompiuterių duomenis nacionalinėje teisėje turi būti įtvirtinta ir siekiant sudaryti galimybę pagelbėti kitai valstybei tarptautiniu lygiu, išsaugant aktualius kompiuterių duomenis savo teritorijoje. Taip būtų užtikrinta, jog svarbūs kompiuterių duomenys nebūtų prarasti iki to laiko, kol bus nustatyta tvarka gautas teisinės pagalbos prašymas suteikti informaciją. Atsižvelgiant į tai, kad nusikaltimo tyrimo procese skirtingų valstybių teisėsaugos institucijos privalo bendradarbiauti viena su kita tiek oficialiai, tiek neoficialiai, gali kilti tam tikrų problemų. Jei vienos iš valstybių teisės normos nenustato konkrečių įgalinimų elektroninės informacijos rinkimui, tokia valstybė iš esmės gali būti nepajėgi adekvačiai reaguoti į prašymą suteikti pagalbą.

[60] 2004 m. sausio 29 d. Lietuvos Respublikos baudžiamojo proceso kodekso 154 straipsnio pakeitimo ir papildymo įstatymas Nr. IX-1993. *Valstybės žinios*, 2002, Nr. 37-1341.

[61] Convention on Cybercrime. [interaktyvus, žiūrėta 2011-06-21]. 16 str. 1 d. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm >.

[62] Volevodz A. G. *Protivodeistvije kompiuternim prestuplenijam*. Moskva: Jurlitinform, 2002, p. 207.

Laikomųjų kompiuterių duomenų paieška ir poėmis

Konvencijoje dėl elektroninių nusikaltimų teigiama, jog „*kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas apieškoti ar panašiai ištirti:*

a) kompiuterių sistemą arba jos dalį ir joje laikomus kompiuterių duomenis;

b) kompiuterių duomenų atmeniąją terpę, kurioje tos Šalies teritorijoje gali būti laikomi kompiuterių duomenys“[63].

Kaip nurodyta Konvencijos 19 str. 2 d., *„Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinti, kad jos institucijoms pagal šio straipsnio 1 dalies a punktą apieškant ar panašiai tiriant konkrečią kompiuterių sistemą arba jos dalį ir turint priežasčių manyti, kad ieškomi duomenys laikomi tos Šalies teritorijoje esančioje kitoje kompiuterių sistemoje arba jos dalyje ir kad tokie duomenys yra teisėtai prieinami naudojant pirmąją sistemą, tokios institucijos galėtų operatyviai išplėsti paiešką ar panašų tyrimą į kitą sistemą“.*

Vienas iš pagrindinių aukščiau minėtų Konvencijos normų tikslų – kad informacijos elektroninėje formoje paėmimas iš apieškomos vietos nebūtų diskriminuojamas kitų materialių daiktų ar dokumentų atžvilgiu. Kitaip tariant, krata turi būti vienodai efektyvi tiek materialių, tiek nematerialių objektų atžvilgiu.

Labai aktuali nuostatų dėl kratos „išplėtimo“[64] įgyvendinimo problema. Konvencija nenurodo mechanizmo, kaip kratos „išplėtimas“ turi būti vykdomas. Tai paliekama nacionaliniam reguliavimui.

Šiuo metu nesiginčijama, jog tyrėjas turi turėti teises, tikslu betarpiškai išplėsti paiešką į kitas sujungtas kompiuterių sistemas[65]. Tačiau kaip tai turi būti įgyvendinama? Konvencijos rengėjų nuomone, nacionalinėje teisėje svarstytini keli kratos į kitą kompiuterių sistemą išplėtimo variantai:

1) išduota sankcija yra papildoma ją išdavusios institucijos, t.y. „praplečiama“ apimant ir kompiuterių sistemą, kurioje talpinama informacija, prieinama iš tiriamosios kompiuterių sistemos;
2) suteikiami įgaliojimai sankciją papildyti sankciją gavusiai institucijai (pareigūnui).

Nors pirmuoju atveju nereikėtų kreiptis dėl naujos sankcijos, šio varianto neigiama pusė būtų ta, jog tyrėjui, prieš „išplečiant“ kratos veiksmus į kitą kompiuterių sistemą, reikėtų kreiptis dėl sankcijos papildymo[66]. Turint omenyje kitoje kompiuterių sistemoje saugomos informacijos pažeidžiamumą ir tai, jog sankcijos papildymas negali būti atliekamas betarpiškai (t.y. tyrėjas turėtų atlikti veiksmus, kurie, laiko sąnaudų

63 Convention on Cybercrime. [interaktyvus, žiūrėta 2011-06-21]. 19 str. 1 d. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm >.

64 Convention on Cybercrime [interaktyvus, žiūrėta 2011-06-21], 19 str. 1 d. b). < http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm >.

65 Volevodz A. G. *Protivodeistvije kompiuternim prestuplenijam*. Moskva: Jurlitinform, 2002, p. 206.

66 Tokio procesinio veiksmo galimybė Lietuvos Respublikos baudžiamajame proceso kodekse iš viso nėra numatyta.

prasme, prilygintini naujos sankcijos gavimui) būnant kratos vietoje, šis būdas yra diskutuotinas.

Antruoju atveju tyrėjas nesikreiptų dėl sankcijos papildymo, o būtų traktuojama, jog išduota sankcija įgalina tyrėją savarankiškai „išplėsti“ paiešką į su tiriamąja kompiuterių sistema sujungtą kompiuterių sistemą, esančią Lietuvos Respublikos teritorijoje, jei būtų manoma, kad toje kompiuterių sistemoje talpinama tyrimui svarbi informacija. Šiuo atveju būtų betarpiškai „išplečiama“ krata ir iki minimumo sumažinama galimybė pakeisti ar ištrinti informaciją iš atitinkamos kompiuterių sistemos, kol bus gauta nauja sankcija ar esamos sankcijos papildymas[67].

Paminėtina, jog Konvencijos paaiškinamajame rašte įvardijama, kad kratos „išplėtimo“ galimybė nebūtinai turi būti reglamentuojama naujais teisės aktais pagal nacionalinę teisę. Jei egzistuojantys teisės aktai suteikia galimybę „išplėsti“ kratą, nėra būtinybės priimti naujų teisės normų, reglamentuojančių kratos „išplėtimą“.

Kompiuterių duomenų surinkimas realiuoju laiku

Konvencijoje numatyta, jog „*kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas:*

a) tos šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti;

b) priversti paslaugos teikėją pagal jo technines galimybes:

- *tos šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti arba*
- *bendradarbiauti su kompetentinga institucija ir padėti jai surinkti arba įrašyti*

realiuoju laiku srauto duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterių sistema“ (Konvencijos 20 straipsnis) arba „*realiuoju laiku turinio duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterių sistema*“ (Konvencijos 21 straipsnis).

Kai kalbama apie kompiuterių duomenų surinkimą realiuoju laiku, turima omenyje įrodymų rinkimą iš esamu metu vykdomų komunikacijų, kurios generuoja tam tikrus duomenis[68]. Reikėtų atskirti, jog šiuo atveju galimi dviejų tipų duomenys: srauto duomenys[69] bei turinio duomenys[70]. Manoma, jog procesiniai reikalavimai srauto ir

[67] Štitilis D., Krikščiūnas R., Petrauskas R. Kai kurie Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai. *Jurisprudencija*, 2005, 67(59), p. 25.

[68] Explanatory Report to the Convention on Cybercrime [interaktyvus, žiūrėta 2011-06-21], 208 p. <http://conventions.coe.int/treaty/en/reports/html/185.htm>.

[69] Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 3 str. 52 p., srauto duomenimis laikytini duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai. 2002-09-19 Konstitucinio teismo nutarime telekomunikacijų įvykis apibūdinamas kaip „informacijos perdavimo, siuntimo, priėmimo telekomunikacijų tinklais faktas“. Pvz., srauto duomenimis laikytina informacija apie sujungimo laiką, trukmę, naudotus protokolus ir pan.

[70] Nei Konvencijoje, nei Lietuvos Respublikos teisės aktuose nėra apibrėžta, kas laikytina turinio duomenimis, tačiau šie duomenys susiję su susižinojimo (komunikacijų) turiniu (išskyrus srauto duomenis). Pagal 2002/58/EB direktyvos 2 (d) str., „pranešimas“ – tai informacija, kuria apsikeičiama arba kuri perduodama tarp baigtinio skaičiaus šalių, naudojantis viešai prieinamomis elektroninių ryšių paslaugomis. Kitaip tariant, turinio duomenimis laikytinas pokalbio telefonu ar elektroninio pašto žinutės turinys.

turinio duomenų surinkimui turėtų skirtis[71], kadangi turinio duomenys atskleidžia komunikacijų turinį ir jų neteisėtas atkleidimas daro didesnę žalą, lyginant su srauto duomenų neteisėtu atkleidimu[72]. Todėl turinio duomenų kontrolės sankcionavimas turėtų būti griežtesnis[73].

Vis dėlto, net ir Valstybėse Narėse įgyvendinus šias Konvencijos nuostatas dėl proceso teisės, lieka neišspręstos kai kurios aktualios problemos. Viena iš jų – problema dėl įpareigojimų operatoriams užtikrinti technines IP telefonijos kontrolės galimybes[74].

3.1.1.3. Kitos Konvencijos dėl elektroninių nusikaltimų nuostatos

Konvencija taip pat įtvirtina nuostatas, skirtas ekstradicijos bei savitarpio pagalbos reglamentavimui. Visos Konvencijos 2-11 str. apibrėžtos veikos yra pripažįstamos nusikaltimais, už kuriuos asmenys gali būti išduodami vienos Susitariančiosios Šalies kitai Susitariančiajai Šaliai.

Konvencija taip pat įpareigoja Susitariančiąsias Šalis teikti skubią ir visapusišką savitarpio pagalbą tiriant ar nagrinėjant baudžiamąsias bylas dėl elektroninių nusikaltimų. Tuo tikslu Konvencijos 35 str. įpareigoja Susitariančiąsias Šalis paskirti 24 valandas per parą ir 7 dienas per savaitę veikiančią instituciją, kuri galėtų teikti technines konsultacijas ir atlikti Konvencijoje nurodytus veiksmus[75].

3.1.2. Konvencijos dėl elektroninių nusikaltimų papildomas protokolas

Konvencijos dėl elektroninių nusikaltimų Papildomas Protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterių sistemomis, kriminalizavimo[76] priimtas 2003 m. sausio 28 d. Strasbūre. 2011 m. balandžio mėnesį protokolą buvo ratifikavusios 18 valstybių. Lietuva šį protokolą ratifikavo 2006 m. birželio 8 d. įstatymu Nr. X-674[77].

Papildomo Protokolo tikslas – papildyti 2001 m. Konvencijos dėl elektroninių

[71] Broadhurst R. Content crimes: criminality and sencorship in Asia. *The Challenge of Cybercrime Conference* on 15-17 September, 2004. Palais de l`Europe, Strasbourg, France [interaktyvus, žiūrėta 2011-06-27]. 10 p. <http://ceps.anu.edu.au/publications/pdfs/broadhurst_pubs/broadhurst-content_cybercrimes.pdf>.

[72] Štitilis D. Privataus gyvenimo elektroniniuose ryšiuose ribojimas nusikaltimų tyrimo tikslais. *Jurisprudencija*, 2006, 9(87), p. 71.

[73] Maxwell W. *Electronic Communications: The New EU Framework*. New York: Oceana Publications, Inc., Dobbs Ferry, 2002; 1.5-10.

[74] Štitilis D. IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui. *Socialinių mokslų studijos*, 2009, 1(1), p. 218.

[75] Aiškinamasis raštas dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo [interaktyvus, žiūrėta 2011-06-27]. <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=223058>.

[76] Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems Strasbourg, 28.I.2003 [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>.

[77] Lietuvos Respublikos įstatymas dėl Konvencijos dėl elektroninių nusikaltimų papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, ratifikavimo. *Valstybės žinios.* 2006, Nr. 75-2848.

nusikaltimų nuostatas įpareigojimais valstybėms, ratifikavusioms Protokolą, kriminalizuoti rasistinio ir ksenofobinio pobūdžio veikas, padarytas naudojantis kompiuterių sistemomis, įpareigoti valstybes bendradarbiauti tarpusavyje tiriant tokius nusikaltimus.

Protokole pateikiama rasistinės ir ksenofobinės medžiagos sąvoka – tai bet kuri rašytinė medžiaga, bet kuris vaizdas arba bet kuris kitoks idėjų ar teorijų pateikimas, propaguojantis, skatinantis arba kurstantis neapykantą, diskriminavimą ar smurtą, nukreiptą prieš asmenį arba asmenų grupę dėl rasės, odos spalvos, kilmės arba tautinės ar etninės kilmės, taip pat religijos, jeigu tai naudojama kaip pretekstas kuriam nors iš šių veiksnių.

Dėl rasistinės ir ksenofobinės medžiagos skleidimo naudojantis kompiuterių sistemomis, protokole numatyta, jog kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamąją atsakomybę už tokią sąmoningą ir neteisėtą veiką: rasistinės ir ksenofobinės medžiagos platinimą ar kitokį skleidimą visuomenei naudojantis kompiuterių sistema[78].

Dėl rasistiniais ir ksenofobiniais ketinimais grindžiamo grasinimo protokole numatyta, jog Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamąją atsakomybę už tokią sąmoningą ir neteisėtą veiką: grasinimą, naudojantis kompiuterių sistema, padaryti sunkų nusikaltimą, kaip apibūdinama pagal jos vidaus teisę, i) asmenims dėl to, kad jie priklauso grupei, kuri yra kitokia dėl rasės, odos spalvos, kilmės arba tautinės ar etninės kilmės, taip pat religijos, jeigu tai naudojama kaip pretekstas kuriam nors iš šių veiksnių, arba ii) asmenų grupei, kuri yra kitokia dėl kurio nors iš šių požymių[79].

Dėl rasistiniais ir ksenofobiniais ketinimais grindžiamo įžeidimo protokole numatyta, jog Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamąją atsakomybę už tokią sąmoningą ir neteisėtą veiką: viešą įžeidimą, naudojantis kompiuterių sistema, i) asmenų dėl to, kad jie priklauso grupei, kuri yra kitokia dėl rasės, odos spalvos, kilmės arba tautinės ar etninės kilmės, taip pat religijos, jeigu tai naudojama kaip pretekstas kuriam nors iš šių veiksnių; arba ii) asmenų grupės, kuri yra kitokia dėl kurio nors iš šių požymių[80].

Protokole taip pat siūloma nustatyti baudžiamąją atsakomybę už genocide arba nusikaltimų žmoniškumui neigimą, šiurkštų menkinimą, pritarimą jiems arba pateisinimą.

Kitas Papildomo Protokolo (8 str. 2 d.) įpareigojimas – išplėsti Konvencijos 14-21 ir 23-25 straipsniuose apibūdintų priemonių taikymą Papildomo Protokolo atžvilgiu. Minėti

[78] Konvencijos dėl elektroninių nusikaltimų Papildomas Protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo, 3 str. *Valstybės žinios*. 2006-07-05, Nr. 75-2850. [interaktyvus, žiūrėta 2011-06-27]. <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=279838>.

[79] Konvencijos dėl elektroninių nusikaltimų Papildomas Protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo, 4 str. *Valstybės žinios*. 2006-07-05, Nr. 75-2850. [interaktyvus, žiūrėta 2011-06-27]. <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=279838>.

[80] Konvencijos dėl elektroninių nusikaltimų Papildomas Protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo, 5 str. *Valstybės žinios*. 2006-07-05, Nr. 75-2850. [interaktyvus, žiūrėta 2011-06-27]. <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=279838>.

Konvencijos straipsniai nustato reikalavimus valstybių procesinėms teisės normoms, įpareigoja imtis priemonių, būtinų operatyviai išsaugoti laikomus kompiuterių, srauto duomenis, juos atskleisti ar pateikti, surinkti srauto duomenis realiuoju laiku, įrašyti tokius duomenis ir pan.

3.1.3. Tarptautinių organizacijų ir ES dokumentai dėl elektroninių nusikaltimų

Dėmesys elektroninių nusikaltimų problemai tarptautiniu mastu buvo parodytas jau 1983 metais. 1983-1985 metais Ekonominio bendradarbiavimo ir plėtros organizacijos paskirti ekspertai atliko tyrimą dėl baudžiamųjų įstatymų, susijusių su nusikaltimais, susietais su kompiuteriais, derinimo[81]. Atlikus tyrimą, valstybėms narėms buvo pateiktas minimalus pavojingų veikų, susijusių su kompiuteriais, sąrašas. Prie tokių veikų buvo priskirta:

- tyčinis kompiuterių duomenų ir (arba) programų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas, siekiant nelegaliai pasisavinti lėšas ar kitas vertybes;
- tyčinis kompiuterių duomenų ir (arba) programų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas klastojimo tikslais;
- tyčinis kompiuterių duomenų ir (arba) kompiuterių programų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas ar kitoks kišimasis į kompiuterių sistemos darbą, siekiant trukdyti kompiuterių ir (arba) telekomunikacijų sistemos funkcionavimą;
- išskirtinės savininko teisės į saugomą kompiuterių programą pažeidimas, siekiant naudoti ją komerciniais tikslais arba paleisti į rinką;
- patekimas į kompiuterį arba kompiuterio ir (arba) telekomunikacijos sistemos perėmimas be asmens, atsakingo už šią sistemą, leidimo, pažeidžiant apsaugos priemones arba dėl kitų nesąžiningų ar žalingų paskatų.

Valstybėms buvo siūloma užtikrinti, kad jų baudžiamieji įstatymai būtų pataisyti pagal išvardytą veikų sąrašą. Dauguma Informacijos, kompiuterių ir ryšių politikos komiteto narių taip pat buvo už tai, jog baudžiamosiomis normomis turėtų būti uždraustos ir kitos veikų rūšys, pvz., neteisėtas kompiuterių sistemų naudojimas ir kt.

Detaliau aptartina Europos Tarybos veikla, koordinuojant teisines priemones, nukreiptas užkirsti kelią elektroninių nusikaltimų plitimui. Verta paminėti Europos Tarybos rekomendacijas. Nuo 1985 iki 1989 metų Europos tarybos su kompiuteriais susijusių nusikaltimų ekspertų komitetas analizavo teisines kompiuterinių nusikaltimų problemas. Europos Tarybos Ministrų komitetas 1989 m. priėmė Rekomendaciją Nr.

[81] Petrauskas R., Štitilis D. Lietuvos Respublikos baudžiamasis kodeksas nusikaltimų elektroninėje erdvėje konvencijos kontekste. *Jurisprudencija*, 2002, 24(16), p. 80.

R(89)9 [12], kuria ET šalių-narių vyriausybes kviečia atsižvelgti į ekspertų komiteto parengtą ataskaitą kuriant įstatymus, susijusius su kompiuteriniais nusikaltimais. Šią ataskaitą sudaro penkios dalys. Pirmoji dalis aprašo kompiuterinio nusikaltimo fenomeną. Antrojoje dalyje išdėstyti vadinamieji principai nacionaliniams įstatymų leidėjams (minimalus ir neprivalomas nusikalstamų kompiuterinių veikų sąrašai). Kitos dalys susijusios su procesinių normų taikymu: kompiuterinių įrodymų leistinumas, įrodymų rinkimas ir kt. Paskutinėje dalyje kalbama apie kompiuterinių nusikaltimų prevenciją, latentiškumo mažinimą, ir kt.

Kaip minėta, pranešime pateikiami du veikų, susijusių su tokiais nusikaltimais, sąrašai. Europos Sąjungos šalims leidžiama savarankiškai spręsti, kaip ir kiek pasinaudoti šiuo pasiūlymu. Minimaliame sąraše išvardytos 8 pavojingesnės veikos, susijusios su kompiuterių technologijomis. Papildomas sąrašas apima keturias mažiau pavojingas veikas, kurios įtraukiamos į įstatymų leidybą, bet nėra privalomos. Šie sąrašai reikalingi suvienodinant ES šalių teisines sistemas kompiuterinių nusikaltimų atžvilgiu.

Pasiūlytas minimalus sąrašas:

- sukčiavimas, susijęs su kompiuteriu (kompiuterių duomenų ar programų įvedimas, ištrynimas, pakeitimas ar paslėpimas, ar kitoks įsikišimas į duomenų apdorojimo procesą, dėl ko padaroma žala kitam asmeniui, turint tikslą gauti materialinę naudą sau ar kitam asmeniui);
- klastojimas naudojant kompiuterį (kompiuterių duomenų ar programų įvedimas, ištrynimas, pakeitimas ar paslėpimas, ar kitoks įsikišimas į duomenų apdorojimo procesą, dėl to įvykdomas tradicinis klastojimas);
- kompiuterių duomenų ar programų sunaikinimas ar sugadinimas (kompiuterių duomenų ar programų ištrynimas, sunaikinimas, sugadinimas, neturint tam teisės);
- sabotažas panaudojant kompiuterį (kompiuterių duomenų ar programų įvedimas, ištrynimas, pakeitimas ar paslėpimas, ar kitoks įsikišimas į duomenų apdorojimo procesą, siekiant sutrikdyti kompiuterio ar telekomunikacijų sistemos darbą);
- neteisėta prieiga prie kompiuterių sistemos (prieiga prie kompiuterių sistemos ar tinklo, neturint tam teisės bei pažeidžiant saugumo priemones);
- neteisėtas informacijos perėmimas kompiuterių sistemoje (neteisėtas susirašinėjimo perėmimas į, iš ar viduje kompiuterių sistemos ar tinklo, atliktas techninėmis priemonėmis);
- neteisėtas apsaugotų kompiuterių programų dauginimas ir platinimas;
- neteisėtas kompiuterių lustų (mikroschemų) topografijų dauginimas ir platinimas.

Pasiūlytas neprivalomas sąrašas: kompiuterių duomenų ar programų pakeitimas, kompiuterinis špionažas, neteisėtas kompiuterio naudojimas (laiko vagystė), neteisėtas apsaugotų kompiuterių programų naudojimas.

Yra priimtos ir dvi Europos tarybos kompiuterinių nusikaltimų komiteto rekomendacijos, susijusios su baudžiamojo proceso teisės taikymu tiriant elektroninius nusikaltimus: Nr. R(85)S ir Nr. R(95)13[82]. Pastarojoje valstybių narių vyriausybėms rekomenduojama, peržiūrint nacionalinius teisės aktus, atsižvelgti į prie rekomendacijos pridedamus principus:

- *krata ir poėmis*. Nacionaliniai įstatymai kratai ir poėmiui elektroninėje erdvėje turi sudaryti vienodas sąlygas.Taip pat įstatymai turi sudaryti sąlygas „išplėsti" kratą ar poėmį į kitas kompiuterių sistemas, sujungtas per kompiuterių tinklą;
- *telekomunikacijų kontrolė.* Procesiniai įstatymai turi būti peržiūrėti, tikslu sudaryti galimybę teisėsaugos institucijoms, tiriant sunkius nusikaltimus, kontroliuoti telekomunikacijų srauto duomenis ar telekomunikacijų turinį;
- *pareiga bendradarbiauti su teisėsaugos institucijomis.* Teisės aktai telekomunikacijų operatoriams turi nustatyti specialias pareigas teikti informaciją, reikialingą pradėtam tyrimui;
- *elektroniniai įrodymai.* Teisės aktų nuostatos dėl tradininių įrodymų turi būti vienodai taikomos ir įrodymams elektronine forma;
- *šifravimo naudojimas.* Turi būti apsvarstytas šifravimo naudojimas, turint omenyje, teisėsaugos institucijų galimybę prieiti prie informacijos turinio;
- *tyrimas, statistika ir mokymai.* Turi būti apsvarstyta galimybė steigti specialius padalinius, tiriančius pavojingas veikas elektroninėje erdvėje ir turinčius pakankamai patirties;
- *tarptautinis bendradarbiavimas.* Valstybių sienos neturi trukdyti atlikti numatytų tyrimo veiksmų, pvz., kratos ar poėmio, siekiant paimti reikimą informaciją elektroninėje formoje.

Dalis aukščiau minėtų principų jau yra įgyvendinta, tačiau po rekomendacijos priėmimo praėjus daugiau nei dešimtmečiui, kelios esminės problemos nebuvo išspręstos: efektyvaus tarptautinio bendradarbiavimo, elektroninių įrodymų ir pan.

Per pastarąjį dešimtmetį elektroninių nusikaltimų srityje savo veiklą suaktyvino Europos Sąjungos institucijos, ypač Europos Komisija. Per šį laikotarpį priimta keletas, daugiausia neprivalomų, dokumentų. Šie dokumentai aptartini detaliau.

Vienas iš pirmųjų ES komunikatų dėl elektroninių nusikaltimų – 2001 m. sausio 26 d. komunikatas „Saugesnės informacinės visuomenės kūrimas, gerinant informacinių infrastruktūrų saugą ir kovą su nusikaltimais, susijusiais su kompiuteriais"

[82] Council of Europe. Committee of Ministers. Recommendation No. R (95)13 of the Committee of Ministers to member States concerning Problems of Criminal Procedural law Connected with Information Technology [ineraktyvus, žiūrėta 2011-06-27]. <https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2>.

KOM(2000)890 galutinis[83]. Komunikate nurodyta, jog nusikaltimai, susiję su kompiuteriais, vykdomi visoje elektroninėje erdvėje ir negali būti sustabdyti ties sutartinėmis valstybių sienomis. Tačiau nacionaliniu lygiu dažnai trūksta atsvaros naujiems tinklų saugumo iššūkiams bei naujai kompiuterinių nusikaltimų grėsmei. Daugelyje valstybių, į kompiuterinius nusikaltimus reaguojama nacionaline teise (ypatingai baudžiamąja teise), tačiau trūksta alternatyvių prevencijos priemonių.

Skiriasi ne tik nacionalinių valstybių baudžiamosios materialinės teisės normos, tačiau ir tyrimo struktūrų procesinės teisės. O tai sunkina kovą su kompiuteriniais nusikaltimais.

Komunikate nurodoma, kokiu aspektu suprantamas terminas „su kompiuteriais susiję nusikaltimai“ (angl. *computer-related crime*). Ši kategorija suprantama plačiąja prasme, kaip bet koks nusikaltimas, kai vienu ar kitu būdu nusikaltimui įvykdyti naudojamos informacinės technologijos. Tačiau pažymima, kad egzistuoja skirtingos nuomonės, kas sudaro „su kompiuteriais susijusius nusikaltimus“. Komunikate nurodoma, kad terminai „kompiuterinis nusikaltimas“, „su kompiuteriais susijęs nusikaltimas“, „aukštų technologijų nusikaltimas“ ir „elektroninis nusikaltimas“ dažnai vartojami kaip sinonimai. Vis dėlto, anot komunikato, skirtumas yra tarp specialių kompiuterinių nusikaltimų (angl. *Computer specific crime*) ir tradicinių nusikaltimų, kurie įvykdomi panaudojant kompiuterines technologijas.

Komunikate taip pat nurodoma, kad teisės aktai, susiję su specialiais kompiuteriniais nusikaltimais, ES gali būti skirti kelioms tokių pažeidimų grupėms:

1) *Privatumo pažeidimai*. Daugelis valstybių nusikaltimu laiko neteisėtą asmens duomenų rinkimą, saugojimą, modifikavimą, atskleidimą ar platinimą[84].
2) *Su turiniu susiję pažeidimai*. Tokiems pažeidimams priskiriami pažeidimai, kai internetu platinama medžiaga su vaikų pornografija ar rasistinio pobūdžio informacija.
3) *Ekonominiai pažeidimai, neteisėta prieiga ir sabotažas*. Šių nusikaltimų objektas dažniausiai nematerialus, t.y. pinigai elektronine forma ar kompiuterių programos.
4) *Pažeidimai, susiję su intekeltine nuosavybe*.

Taigi, komunikate taip pat pabandyta pateikti su kompiuteriais susijusių nusikaltimų rūšių klasifikaciją.

Pažymėtina, kad komunikatae nurodoma, jog atitinkamose valstybėse, kovojant su kompiuteriniais nusikaltimais, reikia imtis šių priemonių:

I. Materialinės teisės aspektai.

[83] Communication from the Commision 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 Infrastructuresand Combating Computer-related Crime. Brusssels, 2001.01.26. COM (2000)890 final.[interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF>.

[84] Reikia paminėti, kad šiuo metu asmens duomenų teisinės apsaugos pažeidimai dažniausiai traktuojami kaip administraciniai pažeidimai ar kaip baudžiamieji nusižengimai (jei atitinkamoje valstybėje nėra administracinių pažeidimų). Tuo tarpu, tik privatumo pažeidimai, pažeidžiant komunikacinį privatumą, laikomi kaip nusikaltimai.

Šioje srityje pažymima, kad nacionalinės baudžiamosios teisės harmonizavimas aukštų technologijų nusikaltimų srityje padėtų minimaliai užtikrinti apsaugą potencialioms elektroninių nusikaltimų aukoms. Būtent šiame komunikate pirmą kartą

paminėta Konvencija dėl elektroninių nusikaltimų, kuri galėtų prisidėti prie nacionalinės baudžiamosios teisės elektroninių nusikaltimų srityje harmonizavimo.

II. Proceso teisės aspektai.

Proceso teisės vienodinimas galėtų pagerinti potencialių elektroninių nusikaltimų aukų apsaugą, užtikrinant tyrimo institucijų procesines teises tiriant elektroninius nusikaltimus. Komunikate išskiriamos šios proceso teisės vienodinimo sritys:

- komunikacijų perėmimas;
- srauto duomenų saugojimas;
- anonimiška prieiga ir naudojimas;
- praktinis bendradarbiavimas tarptautiniu lygiu;
- procesinės teisės ir jurisdikcija;
- įrodomoji kompiuterinių duomenų vertė.

Komunikate taip pat akcentuojamos ir ne teisinės priemonės, kovojant su elektroniniais nusikaltimais. Pvz., bendradarbiavimo gerinimas su vartotojų organizacijomis, elektroninės informacijos saugos priemonių kūrimo skatinimas ir kt.

2005 metais Europos taryba priėmė pamatinį sprendimą „Dėl atakų prieš informacines sistemas“ **Nr. 2005/222/JHA**[85]. Sprendimas priimtas turint tikslą gerinti bendradarbiavimą tarp teisminių ir kitų kompetentingų institucijų, įskaitant policijos struktūras, vienodinant ES valstybių narių baudžiamuosius įstatymus atakų prieš informacines sistemas srityje. Priimant šį sprendimą, ypač buvo pabrėžta teroristinių atakų prieš informacines sistemas bei kritinę infrastruktūrą grėsmė. Taip pat buvo konstatuota, kad skubių veiksmų baudžiamosios teisės srityje reikia imtis dėl transnacionalinio ir besienio elektroninių nusikaltimų braižo.

Visų pirma, siekiama unifikuoti tam tikras sąvokas atakų prieš informacines sistemas srityje. Sprendime pateikiamos „informacinės sistemos“, „kompiuterių duomenų“, „juridinio asmens“, taip pat „be teisės“ sąvokos. Sprendimu iš principo ketinta unifikuoti ES valstybių narių baudžiamąją teisę trijų veikų atžvilgiu:

1) neteisėtos prieigos prie informacinės sistemos;
2) neteisėto įsikišimo į informacinės sistemos funkcionavimą;
3) neteisėto įsikišimo į elektroninių duomenų apdorojimą.

Visais atvejais paminėtos veikos turi būti įvykdytos tyčia.

[85] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT>.

Sprendimu taip pat numatyta, kad baudžiamoji atsakomybė turėtų būti taikoma ir už rengimąsi ar pasikėsinimą įvykdyti aprašytas tris veikas. Taip pat reglamentuojama, kad sankcijos už numatytas nusikalstamas veikas turėtų būti efektyvios, proporcingos bei atgrasančios nuo kitų nusikaltimų.

Sprendimas taip pat reglamentuoja juridinių asmenų atsakomybę už paminėtas pavojingas veikas elektroninėje erdvėje (laikinas veiklos apribojimas ir kt.) bei jurisdikcijos klausimus. Nustatant jurisdikciją, siūloma naudoti teritorinį, pilietybės bei universalųjį jurisdikcijos principus.

Šis pamatinis sprendimas ES valstybėse narėse turėjo būti įgyvendintas iki 2007 m. kovo 16 d. Nors valstybės narės iš esmės įgyvendino Pamatinio sprendimo nuostatas, dėl vis didesnio nusikalstamos veikos (kibernetinių atakų) masto ir dažnumo Sprendimas, pasirodė, turi tam tikrų trūkumų. Sprendimu suderinamos tik ribotą skaičių nusikalstamų veikų reglamentuojančios nuostatos, tačiau nėra visapusiškai sprendžiama didelio masto atakų visuomenei keliamos potencialios grėsmės problema. Sprendime neatsižvelgiama į nusikaltimų sunkumą ir už juos taikomas sankcijas.

2007 m. gegužės 22 d. buvo priimtas EK komunikatas „Link bendros politikos kovojant prieš elektroninius nusikaltimus“ **KOM(2007)267 galutinis**[86]. Komunikato įvade nagrinėjama, kas yra elektroninis nusikaltimas (angl. *cyber crime*). Nurodoma, jog apibrėžti šiai neteisėtai ir nusikalstamai veikai vartojama nemažai terminų, kurie yra sinonimiški. Išskiriama, kad praktikoje terminas „elektroninis nusikaltimas“ vartojamas apibūdinti trims kriminalinių veikų kategorijoms:

1) Tradiciniai nusikaltimai, tokie kaip klastojimas ar sukčiavimas, elektroninių nusikaltimų atveju vykdomi panaudojant elektroninių ryšių tinklus ir informacines sistemas.
2) Neteisėto turinio nusikaltimai panaudojant elektroninę mediją, pvz., platinama medžiaga su vaikų pornografija.
3) Elektroniniams tinklams būdingi nusikaltimai, pvz., atakos prieš informacines sistemas, DDoS atatkos ar neteisėta prieiga (angl. *Hacking*).

Apie pastarojo meto situaciją komunikate užsimenama, kad elektroninių nusikaltimų skaičius auga, o nusikalstamos veikos tampa vis sudėtingesnės ir tarptautinio pobūdžio. Taip pat pastabima, kad elektroninių nusikaltimų srityje didėja organizuoto nusikalstamumo dalis ir beveik negerėja skirtingų valstybių teisėsaugos institucijų bendradarbiavimas.

Dėl to komunikate nurodomas pagrindinis tikslas – besikeičiančios aplinkos šviesoje kyla skubi būtinybė imtis priemonių – tiek nacionaliniu, tiek ir ES lygiu – prieš visas elektroninių nusikaltimų formas, kurios kelia vis didesnę grėsmę kritinei infrastruktūrai, visuomenei, verslui ir piliečiams. Apibendrinant, šį tikslą galima dalinti į tris pagrindinius potikslius:

[86] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions Towards a general policy on the fight against cyber crime. Brussels, 2007.05.22, COM (2007) 267 final. [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

1) gerinti koordinaciją ir bendradarbiavimą tarp elektroninių nusikaltimų padalinių, kitų kompetentingų institucijų ir ekspertų Europos Sąjungoje;
2) koordinuojant su ES valstybėmis narėmis, tarptautinėmis organizacijomis ir kitais dalyviais, vystyti ES politiką kovoje su elektroniniais nusikaltimais;
3) didinti žinojimą, susijusį su elektroninių nusikaltimų daroma žala ir pavojingumu.

Komunikate išskiriamos šios kovos su elektroniniais nusikaltimais priemonės:

1. Teisėsaugos bendradarbiavimo gerinimas ir mokymai.
2. Dialogo su verslu skatinimas.
3. Teisės aktų leidyba. Šioje srityje pažymima, kad nacionalinės baudžiamosios teisės harmonizavimas vis dar nėra tinkamas. Kaip pavyzdys minima tapatybės vagystė elektroninėje erdvėje. Ši veika (kai neteisėtai naudojami asmeniniai duomenys su tikslu įvykdyti nusikaltimą) kaip tokia nekriminalizuota daugelio ES nacionalinių valstybių baudžiamuosiuose įstatymuose. Pagal šių valstybių įstatymus kaltas asmuo būtų baudžiamas už sukčiavimą ar kitą nusikaltimą, tačiau ne už tapatybės vagystę kaip tokią. Kriminalizuoti tapatybės vagystę elektroninėje erdvėje kaip savarankišką nusikaltimą siūloma dėl to, jog tapatybės vagystę įrodyti daug lengviau nei sukčiavimą. Todėl kriminalizavus tapatybės vagystę, pagerėtų teisėsaugos institucijų bendradarbiavimas.
4. Statistinių duomenų vystymas.

Naujausias EK komunikatas priimtas susirūpinus kritinės infrastruktūros apsauga. 2009 m. kovo 30 d. buvo priimtas Komisijos komunikatas Europos parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ **KOM(2009)149 galutinis**[87] (priedas Nr. 2).

Komunikate teigiama, jog kasdienis gyvenimas vis labiau susijęs su informacinėmis ir komunikacinėmis technologijomis (IKT). Europos ekonomikai ir visuomenei gyvybiškai svarbios kai kurios iš tų IKT sistemų, paslaugų, tinklų ir infrastruktūros objektų (trumpai tariant, IKT infrastruktūros objektų), nes jos naudojamos teikti būtiniausioms prekėms ir paslaugoms arba yra kitų ypatingos svarbos infrastruktūros objektų laikančioji konstrukcija. Paprastai jos laikomos ypatingos svarbos informacinės infrastruktūros objektais[88], nes jeigu jos būtų sugadintos arba sunaikintos, tai turėtų sunkių pasekmių gyvybiškai svarbioms visuomenės funkcijoms. Naujausi pavyzdžiai: 2007 m. didelio masto kibernetiniai Estijos antpuoliai, 2008 m. įvykę incidentai, kai buvo nutraukti tarpžemyniniai kabeliai.

[87] Komisijos komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“. Briuselis, 2009.03.30, KOM (2009) 149 galutinis. [interaktyvus, žiūrėta2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:PDF>.

[88] Ypatingos svarbos informacinės infrastruktūros objektų apibrėžtis pasiūlyta Žaliojoje knygoje Apie Europos programą dėl ypatingos svarbos infrastruktūros objektų apsaugos. Briuselis, 2005-11-17 KOM (2005) 576 (galutinis). [interaktyvus, žiūrėta 2011-06-27]. < http://eur-lex.europa.eu/LexUriServ/site/lt/com/2005/com2005_0576lt01.pdf>.

2008 m. Pasaulio ekonomikos forume apskaičiuota, kad ypatingos svarbos informacinės infrastruktūros avarijos, kuri pasaulio ūkiui kainuotų apytiksliai 250 mlrd. JAV dolerių[89], tikimybė per artimiausią dešimtmetį yra 10–20 %.

Šiame komunikate daugiausiai dėmesio skirta prevencijai, parengčiai bei informavimui ir sudarytas neatidėliotinų veiksmų planas, kaip didinti ypatingos svarbos informacinės infrastruktūros objektų saugumą ir atsparumą. Tokie tikslai dera su Tarybos ir Europos Parlamento prašymu pradėta diskusija, kurioje siekiama išnagrinėti sudėtingus tinklų ir informacijos saugumo politikos uždavinius bei prioritetus ir nutarti, kokių priemonių dėl tų uždavinių ir prioritetų reikia ES. Be to, pasiūlytais veiksmais papildomi veiksmai, kuriais siekiama užkirsti kelią prieš ypatingos svarbos informacinės infrastruktūros objektus nukreiptai nusikalstamai ir teroristinei veiklai, su ja kovoti ir už ją persekioti baudžiamąja tvarka, ir užtikrinama sąveika su dabartinėmis bei būsimomis tinklų ir informacijos saugumo ES mokslinių tyrimų pastangomis ir su tarptautinėmis šios srities iniciatyvomis.

Apie ypatingos svarbos informacinės infrastruktūros objektams kylančias grėsmes komunikatas nurodo, jog „dėl piktavalių antpuolių, gaivalinių nelaimių arba techninių gedimų kylanti grėsmė dažnai nėra aiškiai suprantama ir (arba) pakankamai išnagrinėjama“. Todėl suinteresuotosios šalys nepakankamai informuotos, kad sukurtų veiksmingas apsaugos ir atoveikio priemones. Kibernetiniai antpuoliai tapo kaip niekada sudėtingi. Paprasti eksperimentai perauga į sudėtingus veiksmus, vykdomus siekiant pelno arba politinių tikslų. Neseniai įvykdyti didelio masto kibernetiniai Estijos, Lietuvos ir Gruzijos antpuoliai – tai plačiausiai nušviesti bendrosios tendencijos pavyzdžiai. Kokia sunki problema, galima įsitikinti iš to, kad yra daug virusų, kirminų (savaime plintančių kenkimo programų) ir kitos kenkimo programinės įrangos, kad didėja kenkimo programiniu kodu apkrėstų kompiuterių tinklai (angl. *botnet*) ir nuolat daugėja nepageidaujamų e. pašto laiškų[90].

Atsižvelgiant į didelį priklausomumą nuo ypatingos svarbos informacinės infrastruktūros objektų, jų tarpvalstybinius sujungimus ir tarpusavio priklausomumą nuo kitos infrastruktūros objektų, taip pat į jų pažeidžiamumą ir jiems kylančias grėsmes, apsisaugoti nuo gedimų ir gintis nuo antpuolių reikėtų pirmiausia sistemingai sprendžiant ypatingos svarbos informacinės infrastruktūros objektų saugumo ir atsparumo klausimus.

Komunikate įvardijami tokie Europos uždaviniai:

1) Nevienodi ir nesuderinti nacionaliniai metodai.

Nors sudėtingi uždaviniai ir problemos, su kuriomis susiduriama, turi bendrybių, valstybėse narėse skiriasi ypatingos svarbos informacinės infrastruktūros objektų saugumo ir atsparumo užtikrinimo priemonės ir tvarka, profesinė kompetencija ir

[89] Global Risks 2008*,* 2008 m. pasaulinių grėsmių ataskaita. [interaktyvus, žiūrėta 2011-06-27]. <http://www.scribd.com/doc/6310131/Global-Risk-Report-2008>.

[90] Komisijos komunikatas Europos parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei regionų komitetui. Dėl kovos su nepageidaujamu e. paštu, šnipinėjimo programomis ir žalinga programine įranga COM (2006) 688 galutinis 2006-11-15, Briuselis [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:LT:PDF>.

parengties lygis.

Šioms aplinkybėms įveikti reikia Europos pastangų, kad papildomos vertės nacionalinei politikai ir programoms būtų suteikta, puoselėjant sąmoningumo ugdymą ir bendrą sudėtingų uždavinių supratimą, skatinant bendrų politikos uždavinių ir prioritetų priėmimą, stiprinant valstybių narių bendradarbiavimą ir integruojant nacionalines politikos kryptis labiau Europos ir pasaulinėje sferoje.

2) Ypatingos svarbos informacinės infrastruktūros objektams reikia Europos valdymo modelio.

Nacionaliniu lygmeniu, kaip bazinis modelis, sudaryta viešojo ir privataus sektorių partnerystė šiai valdymo problemai spręsti. Nors ir sutariama, kad viešojo ir privataus sektorių partnerystė būtų naudinga ir Europos lygmeniu, tokia Europos masto partnerystė dar nesukurta. Privatųjį sektorių dalyvauti nustatant viešosios politikos tikslus bei veiklos prioritetus ir priemones būtų galima paskatinti Europos masto daugelio suinteresuotųjų šalių dalyvavimu grindžiama valdymo sistema, kurioje gali būti numatytas aktyvesnis ENISA vaidmuo. Tokia sistema leistų panaikinti atotrūkį tarp nacionalinės politikos formavimo ir praktinės veiklos tikrovės.

3) Ribotos Europos ankstyvojo atpažinimo ir reagavimo į incidentus išgalės.

Europoje išgalės anksti atpažinti pavojus ir reaguoti į incidentus turi būti pagrįstos sklandžiai dirbančiomis nacionalinėmis (valstybinėmis) kompiuterinių incidentų tyrimo grupėmis (angl. *National/Governmental Computer Emergency Response Teams*, CERT), t. y. turi turėti bendras pagrindines išgales. Šios įstaigos valstybėse turi skatinti suinteresuotųjų šalių susidomėjimą ir gebėjimą vykdyti viešosios politikos veiklą (įskaitant veiklą, susijusią su piliečius ir mažąsias ir vidutines įmones apimančiomis informacijos mainų ir įspėjimo sistemomis) ir užsiimti efektyviu tarpvalstybiniu bendradarbiavimu bei informacijos mainais, galbūt maksimaliai naudodamosi esamomis organizacijomis, pavyzdžiui, Europos vyriausybinių CERT grupe (angl. *European Governmental CERTs Group*, EGC)[91].

4) Tarptautinis bendradarbiavimas.

Internetas – pasaulinis, labai plačiai paskirstytas tinklų tinklas, kurio valdymo centrai veiklą dažnai vykdo neatsižvelgdami į nacionalines sienas. Norint užtikrinti interneto atsparumą bei stabilumą, būtinas specialus tikslinis metodas, pagrįstas dviem viena kitą papildančiomis priemonėmis. Pirma, būtina susitarti, kokie interneto atsparumo ir stabilumo Europos prioritetai, atsižvelgiant į viešąją politiką ir praktinį diegimą. Antra, remiantis mūsų strateginiu dialogu ir bendradarbiavimu su trečiosiomis šalimis ir tarptautinėmis organizacijomis, būtina drauge su pasauline bendruomene ir laikantis pagrindinių Europos vertybių nustatyti interneto atsparumo ir stabilumo principus. Ši veikla būtų pagrįsta Pasaulio aukščiausiojo lygio susitikimo informacinės visuomenės klausimais[92] pripažinimu, kad interneto stabilumas yra svarbiausia.

[91] European Government CERTs (EGC) group. [interaktyvus, žiūrėta 2011-06-27]. <http://www.egc-group.org/>.

[92] Tuniso informacinės visuomenės darbotvarkė. 2005-11-18 [interaktyvus, žiūrėta 2011-06-27]. <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>.

Komunikate numatytas ir atitinkamas veiksmų planas, kurio reikėtų imtis įgyvendinant aukščiau paminėtus uždavinius.

Jau 2008 metų liepos 14 d. Europos Komisija paskelbė Pamatinio sprendimo įgyvendinimo ataskaitą[93], kurios išvadose nurodyta, kad daugelis valstybių narių padarė didelę pažangą ir pakankamai gerai įgyvendina sprendimą, tačiau kai kurios valstybės narės įgyvendinimo dar neužbaigė. Ataskaitoje taip pat nurodyta, kad „po to, kai priimtas Sprendimas, visoje Europoje įvykdytos atakos parodė, kad kyla naujų pavojų: vienu metu įvykdytos itin didelio masto atakos prieš informacines sistemas ir padidėjo vadinamųjų „zombių“ tinklų naudojimas nusikalstamiems tikslams.“ Priimant sprendimą, šioms atakoms nebuvo skirta daug dėmesio.

Dėl to 2010 metais Europos Komisija parengė **pasiūlymą** dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir **dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo**[94]. Pasiūlyme akcentuojama, jog pagrindinė elektroninių nusikaltimų priežastis – pažeidžiamumas, kurį lemia įvairūs veiksniai. Minėti reiškiniai nepašalinami ir dėl nepakankamo atsako taikant teisėsaugos mechanizmus, sunkumų taip pat daugėja, nes tam tikros nusikalstamos veikos yra tarpvalstybinio pobūdžio.

Dažnai apie tokio pobūdžio nusikaltimus nėra pranešama, iš dalies todėl, kad kai kurie nusikaltimai lieka nepastebėti, o kartais nukentėjusieji (ūkinės veiklos vykdytojai ir įmonės) apie nusikaltimus nepraneša baimindamiesi blogos reputacijos ir pakenkti įmonės ateities perspektyvoms, galimoms viešai pranešus apie įmonės pažeidžiamumą. Be to, dėl valstybių baudžiamosios teisės sistemos ir procedūrų skirtumų tokių nusikaltimų tyrimo ir traukimo baudžiamojon atsakomybėn tvarka gali skirtis, todėl kovoti su tokiais nusikaltimais gali tekti skirtingomis priemonėmis. Dėl informacinių technologijų raidos tokių problemų dar padaugėjo, nes vis lengviau kuriamos ir platinamos priemonės (kenkimo programinė įranga ir botnetai), kaltininkai gali išlikti anonimiški, o atsakomybė spręsti klausimus priklauso skirtingoms jurisdikcijoms. Dėl sunkumų baudžiamojo persekiojimo srityje organizuoti nusikaltėliai gali daug uždirbti mažai rizikuodami. Šiame pasiūlyme atsižvelgiama į naujus elektroninių nusikaltimų metodus, visų pirma botnetų panaudojimą. Sąvoka „botnetas“ reiškia kompiuterių, kuriuose įdiegta kenkimo programinė įranga (kompiuterio virusai), tinklą. Toks užkrėstų kompiuterių („zombių“) tinklas gali būti naudojamas konkretiems veiksmams atlikti, pavyzdžiui, atakoms prieš informacines sistemas (t. y. kibernetinėms atakoms) rengti. Šie „zombiai“ gali būti kontroliuojami iš kito kompiuterio, dažnai užkrėstų kompiuterių naudotojams visiškai nieko nežinant. Šis kontroliuojantis kompiuteris dar vadinamas komandų ir kontrolės centru. Šį centrą kontroliuojantys asmenys yra pažeidėjai, nes jie naudojasi užkrėstais

[93] Report from the Comission to the Council Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems. Brussels, 2008.07.14 COM (2008) 448 final. [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:EN:PDF>.

[94] Europos Parlamento ir Tarybos direktyva dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo pasiūlymas. Briuselis, 2010.9.30 KOM (2010) 517 galutinis. [interaktyvus, žiūrėta 2011-06-27]. <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_lt.pdf>.

kompiuteriais atakoms prieš informacines sistemas rengti. Nusikaltėlius susekti labai sunku, nes botnetui priklausantys kompiuteriai, naudojami atakoms rengti, gali būti visai kitoje vietoje nei pažeidėjas. Botneto pagalba rengiamos atakos dažnai būna didelio masto. Didelio masto atakos yra tokios atakos, kurios rengiamos pasitelkiant priemones, dėl kurių nukenčia daug informacinių sistemų (kompiuterių), arba tokios atakos, dėl kurių patiriama didelė žala, pvz., dėl sutrikusių sistemos paslaugų, finansinių išlaidų, prarastų asmens duomenų ir t. t. Šiame kontekste didelis botnetas yra laikomas tinklu, galinčiu padaryti didelę žalą. Sunku nustatyti botnetų dydį, tačiau apskaičiuota, kad prisijungimų prie didžiausių nustatytų botnetų skaičius buvo nuo 40 000 iki 100 000 (t. y. užkrėstų kompiuterių) per 24 valandas[95].

Direktyvoje, kuria ketinama panaikinti Pamatinį sprendimą 2005/222/TVR, išliks šio sprendimo nuostatos ir bus įtraukti šie nauji elementai (Materialinės baudžiamosios teisės srityje šia direktyva):

1) Reglamentuojamos sankcijos už nusikalstamai veikai daryti naudojamų įrenginių ir (arba) priemonių gamybą, pardavimą, įsigijimą siekiant naudotis, importą, platinimą arba galimybių jais naudotis sudarymą kitu būdu.
2) Įtraukiamos nuostatos dėl sunkinančių aplinkybių:
   - ➤ didelio masto atakų rengimo, botnetų ar panašių priemonių naudojimo problema būtų sprendžiama įtraukiant nuostatas dėl sunkinančių aplinkybių, t. y. botneto kūrimas arba panašių priemonių naudojimas darant Pamatiniame sprendime išvardytus nusikaltimus būtų laikomas sunkinančia aplinkybe;
   - ➤ kai tokios atakos rengiamos slepiant tikrąją nusikaltėlio tapatybę ir daroma žala;
   - ➤ teisėtam tapatybės turėtojui. Tokios taisyklės turėtų derėti su baudžiamųjų nusikaltimų ir bausmių teisėtumo ir proporcingumo principais ir galiojančiais asmens duomenų apsaugą reglamentuojančiais teisės aktais.
3) Įtraukiamos nuostatos, pagal kurias neteisėtas duomenų perėmimas laikomas nusikalstama veika.
4) Nustatomos priemonės bendradarbiavimui baudžiamosios teisenos srityje gerinti, stiprinant ištisą parą be poilsio dienų veikiančių informacinių punktų struktūrą: siūloma laikytis įsipareigojimo tenkinti informacinių punktų prašymą suteikti pagalbą per tam tikrą nustatytą laikotarpį (Direktyvos 14 straipsnis). Konvencijoje dėl elektroninių nusikaltimų tokios privalomos nuostatos nėra. Šios priemonės tikslas – užtikrinti, kad informaciniai punktai per nurodytą terminą atsakytų, ar jie galėtų patenkinti prašymą suteikti pagalbą ir kiek laiko

[95] Europos Parlamento ir Tarybos direktyva dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo pasiūlymas. Briuselis, 2010.9.30 KOM (2010) 517 galutinis. [interaktyvus, žiūrėta 2011-06-27]. 3 psl.
<http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_lt.pdf>.

reikėtų, kad pagalba būtų suteikta. Nenurodyta, kokio pobūdžio pagalba būtų teikiama.

5) Reaguojama į būtinybę parengti statistinius duomenis apie elektroninius nusikaltimus, įpareigojant valstybes nares užtikrinti, kad būtų parengta tinkama statistinių duomenų apie Pamatiniame sprendime nurodytus elektroninius nusikaltimus registravimo, rengimo ir teikimo sistema.

Paminėtina, kad kol kas tai tik projektas ir minimas dokumentas nėra oficialiai priimtas.

3.2. Kai kurių užsienio valstybių baudžiamųjų įstatymų nuostatos dėl elektroninių nusikaltimų

Literatūroje nurodoma, kad elektroniniai nusikaltėliai renkasi valstybes su silpnesniu teisiniu reguliavimu[96]. Todėl svarbu, kaip atitinkamose valstybėse yra uždrausti elektroniniai nusikaltimai nacionaliniuose baudžiamuosiuose įstatymuose. Žemiau atitinkamose valstybėse teisinis reguliavimas aptariamas siaurinamąja prasme, t.y. koncentruojamasi tik į atitinkamų valstybių baudžiamuosius įstatymus.

3.2.1. Rusijos Federacija

Paminėtina, kad Rusijos Federacija nėra prisijungusi prie Konvencijos dėl elektroninių nusikaltimų[97], todėl Rusijos baudžiamieji įstatymai nėra tiesiogiai įtakojami šio tarptautinio teisės akto.

Iki 1997 m. sausio 1 d., kai įsigaliojo naujasis baudžiamasis kodeksas, Rusijoje nebuvo galimybės efektyviai kovoti su kai kuriomis pavojingomis veikomis elektroninėje erdvėje. Daugelis veikų nebuvo nusikalstamos, nepaisant jų pavojingumo. Dabar galiojančiame Rusijos baudžiamajame kodekse, be kitų straipsnių, numatyti trys pagrindiniai straipsniai, nustatantys teisinę atsakomybę už nusikaltimus elektroninėje erdvėje. Šie straipsniai sudaro atskirą 28 skyrių „Nusikaltimai kompiuterinės informacijos srityje“:

- Neteisėta prieiga prie kompiuterinės informacijos (272 str.).

Šiame straipsnyje nustatyta atsakomybė už tyčinę neteisėtą prieigą prie įstatymo saugomos kompiuterinės informacijos (informacijos, esančios kompiuterinės informacijos laikmenoje, kompiuterių sistemoje ar tinkle), jei tai sukėlė kompiuterinės informacijos sunaikinimą, blokavimą, modifikavimą ar kopijavimą, taip pat sutrikdė kompiuterių sistemos darbą[98]. Anot *M. M. Karelinos*, objektyviąją nusikaltimo dalį sudaro neteisėta prieiga prie įstatymo saugomos kompiuterinės informacijos, kuri gali

[96] Kshetri N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, 2010, p. 188.

[97] Convention of Cybercrime CETS No.: 185, Status as of : 10/05/2011. [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=10/05/2011&CL=ENG>.

[98] The Criminal code of the Russian Federation, str. 272. [interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.

pasireikšti:

- specialių techninių ar programinių priemonių, leidžiančių įveikti įdiegtas apsaugos sistemas, naudojimu;
- neteisėtu galiojančių slaptažodžių ir kodų panaudojimu (patekimui į kompiuterį) ar kitų veiksmų atlikimu, siekiant patekti į kompiuterių sistemą ar kompiuterių tinklą kaip teisėtam vartotojui;
- informacijos laikmenų grobimu, esant sąlygai, jog buvo imamasi jų apsaugos priemonių, jei tokia veika sąlygojo informacijos sunaikinimą ar blokavimą[99].

Asmens, neturinčio teisės gauti informacijos bei su ja dirbti (įskaitant ir kompiuterių sistemą) prieiga prie kompiuterinės informacijos laikoma neteisėta[100]. Be to, tokiai informacijai turi būti taikomos apsaugos priemonės, nustatant asmenis, galinčius prie jos prieiti[101]. Specialioje literatūroje nurodoma, jog neteisėtą prieigą prie kompiuterinės informacijos reikėtų suprasti kaip neteisėtą susipažinimą su duomenimis, esančiais kompiuteryje[102]. Tačiau kai kurie autoriai kritikuoja tokį neteisėtos prieigos traktavimą, pareikšdami savo abejones dėl vartojamo termino *susipažinimas*. Anot *V. S. Komissarovo*, termino *susipažinimas* vartojimas atima galimybę nusikalstama veika laikyti tokius veiksmus, kai asmuo, jau žinodamas informacijos turinį iš kitų šaltinių, tiktai kopijuoja ar naikina sauginius[103]. Šio nusikaltimo subjektyvioji pusė – tik tiesioginė tyčia.

- Kenkimo programų, skirtų elektroninėms skaičiavimo mašinoms, sukūrimas, naudojimas ar platinimas (273 str.).

Straipsnyje nustatyta baudžiamoji atsakomybė už kompiuterių programų sukūrimą ar jų modifikavimą (taip pat naudojimą ar platinimą), kurios skirtos neteisėtai modifikuoti, naikinti, blokuoti ar kopijuoti kompiuterinei informacijai, trukdyti kompiuterių sistemos darbui[104]. Baudžiamoji atsakomybė pagal šį straipsnį kyla ir nesant jokių padarinių, užtenka vien kompiuterių programos sukūrimo ar modifikavimo fakto. Kenkimo programomis laikomos programos, sukurtos sutrikdyti normaliam kompiuterių programų darbo funkcionavimui. *M. M. Karelina* teigia, kad normaliu kompiuterių programos darbo funkcionavimu reikėtų laikyti operacijų, kurioms vykdyti skirta programa, atlikimą[105]. Labiausiai paplitusiomis kenkimo programomis laikomos: kompiuterių virusai bei loginės bombos. Kompiuterių programos naudojimu laikomas jos išleidimas į apyvartą, atkūrimas, platinimas. Naudojimas taip pat gali būti atliekamas kompiuterių programą įrašant į ESM, į informacijos laikmeną, platinant šią programą kompiuterių

[99] Karelina M. M. Prestuplenije v sfere kompiuternoi informaciji.*Centr issledovanija problem kompjuternoj prestupnosti.* [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/CodeRu.htm>.
[100] Krylov V. V. Informacionnye kompiuternyje prestuplenija. M., 1997, p. 40.
[101] Karelina M. M. Prestuplenije v sfere kompiuternoi informaciji. *Centr issledovanija problem kompjuternoj prestupnosti.* [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/CodeRu.htm>.
[102] Krylov V. V. Informacionnye kompiuternyje prestuplenija. M., 1997, p. 40.
[103] Komissarov V. S. Prestuplenija v sfere kompiuternoi informaciji: ponetije i otvetstvennost. *Juridičeskij mir*, 1998, fevral, p. 14.
[104] The Criminal code of the Russian Federation, str. 273. [interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.
[105] Karelina M. M. Prestuplenije v sfere kompiuternoi informaciji. *Centr issledovanija problem kompjuternoj prestupnosti.* [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/CodeRu.htm>.

tinklais ar kitokiu būdu perduodant tretiesiems asmenims[106]. Šis nusikaltimas gali būti įvykdomas tik esant tyčiai.

➤ Elektroninės skaičiavimo mašinos, elektroninės skaičiavimo sistemos ar tinklo eksploatacijos taisyklių pažeidimas (274 str.).

Šiame straipsnyje nustatyta baudžiamoji atsakomybė už elektroninės skaičiavimo mašinos, elektroninės skaičiavimo sistemos ar tinklo eksploatacijos taisyklių pažeidimą, dėl to buvo sunaikinta, blokuota ar modifikuota įstatymo saugoma informacija, taip pat jei tokia veika buvo padaryta žymi žala[107].

Paminėtina, jog daugelis aukščiau išvardytuose straipsniuose vartojamų sąvokų ir terminų (pvz., „kompiuterinė informacija“, „kompiuterių programa“, „kompiuteris“, „kompiuterių tinklas“ ir kt.) yra nustatytos atskiruose Rusijos įstatymuose, pvz., Informacijos, informatizacijos ir informacijos apsaugos įstatyme bei kt. Tokiu būdu yra išsprendžiama kai kurių sąvokų traktavimo nevienodumo, o kartu veikos kvalifikavimo problema.

272 straipsnis saugo savininko teisę į kompiuterinės informacijos neliečiamumą kompiuterių sistemoje. Remiantis straipsnio dispozicija, galima teigti, jog neteisėta prieiga prie kompiuterių sistemos siejama su tam tikrais padariniais (turi kilti bent vienas iš jų):

- kompiuterinės informacijos sunaikinimas (t.y. informacijos iš materialios laikmenos pašalinimas ir jos atkūrimo negalimumas);
- kompiuterinės informacijos blokavimas (t.y. veiksmų, lemiančių prieigos prie kompiuterių sistemos ar jos informacinių resursų ribojimą, atlikimas[108]);
- kompiuterinės informacijos modifikavimas (t.y. pakeitimų įvedimas į programas, duomenų bazes, tekstinę informaciją, esančią materialioje laikmenoje);
- kompiuterinės informacijos kopijavimas (informacijos į kitą materialią laikmeną perkėlimas, kartu išsaugant nepakeistą pirminę informaciją);
- kompiuterio, kompiuterių sistemos ar tinklo darbo sutrikdymas (gali pasireikšti tiek atskirų programų, duomenų bazių darbo sutrikdymu, tiek aparatinės įrangos ar periferinių įrenginių darbo sutrikdymu arba normalaus tinklo funkcionavimo sutrikdymu) [109].

Preliminariai galima teigti, jog kai šių pasekmių (žalos) nėra (jokie veiksmai neatliekami, t.y. pažeidėjas tik peržiūri informaciją, jos nekopijuoja, nemodifikuoja ar

[106] Otečestvennoje zakonodatelstvo v borbe s kompiuternimu prestuplenijami. [interaktyvus, žiūrėta 2011-06-27]. <http://www.russianlaw.net/law/doc/a01.htm>.
[107] The Criminal code of the Russian Federation. [interaktyvus, žiūrėta 2011-06-27]. str. 274. <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.
[108] Komissarov V. S. Prestuplenija v sfere kompiuternoi informaciji: ponetije i otvetstvennost. *Juridičeskij mir*, 1998, fevral, p. 14.
[109] Karelina M. M. Prestuplenije v sfere kompiuternoi informaciji. *Centr issledovanija problem kompjuternoj prestupnosti.* [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/CodeRu.htm>.

pan.) – baudžiamoji atsakomybė nekyla, nors asmuo neteisėtai ir įsibrauna į kompiuterių sistemą. Taigi atrodo, jog Rusija bent jau kol kas pasirinko neteisėtos prieigos kriminalizavimo kelią, kai nusikalstama veika įvardijama tik tokia veika, dėl kurios kyla nustatytos pasekmės (žala). Kitokios nuomonės yra *D. V. Čepčugovas*. Anot šio rusų autoriaus, 272 str. apima visus neteisėtos prieigos atvejus[110]. Tam, kad kiltų baudžiamoji atsakomybė, per neteisėtą prieigą turi kilti įstatyme nustatytos pasekmės, t.y. informacija turi būti sunaikinta, blokuota, modifikuota ar nukopijuota. Asmeniui, kuris įvykdė neteisėtą prieigą, gali kilti klausimas: „Aš gi nieko nekopijavau, nieko nepavogiau, tik peržiūrėjau informaciją, kuo tuomet aš kaltas?“ *D. Čepčugovo* nuomone, tokie veiksmai laikytini kompiuterinės informacijos kopijavimu. Kai kompiuterių sistemoje esantys duomenys pasirodo pažeidėjo kompiuterio ekrane, įvyksta informacijos perkėlimas. Kadangi elektroniniai impulsai per ryšių linijas atsiranda pažeidėjo kompiuteryje ir apdorojami šio kompiuterio procesoriaus bei išvedami į ekraną, galima sutikti su šio autoriaus nuomone, jog tokie veiksmai gali būti laikomi informacijos kopijavimu ir patenka į Rusijos baudžiamojo kodekso 272 str. veikimo sritį[111]. Taigi neteisėtos prieigos metu kopijuojant informaciją, nebūtinas įsikišimas į šios informacijos apdorojimo procesą, nes tokiu atveju kiltų kita šiame straipsnyje nurodyta pasekmė – informacijos modifikavimas. Tačiau kai kurie kiti Rusijos autoriai nesutinka su nuomone, jog visi neteisėtos prieigos atvejai Rusijos baudžiamajame kodekse yra kriminalizuoti. Šių autorių nuomone, turint omenyje, kad 272 str. bei 274 str. dispozicijos reikalauja tam tikrų pasekmių (žalos teisiniams gėriams), kai kurios per internetą atliekamos pavojingos veikos lieka nekriminalizuotos[112]. Vis dėlto autorius palaiko *D. Čepčugovo* poziciją.

Manoma, jog Rusijos baudžiamojo kodekso 272 str. taip pat nereglamentuoja situacijos, kai neteisėta prieiga įvykdoma dėl neatsargumo, dėl to atsakomybė nekyla dėl didelės dalies veikų. Tokios nuomonės laikosi *A. I. Spivakovas*[113] ir kiti. Taip pat yra nuomonių, kad 272 str. ir 274 str. aprašytos veikos yra labai panašios, todėl svarstytinas klausimas dėl šių veikų sujungimo (išskyrimo į vieną straipsnį)[114, 115]. *A. I. Spivakovas* teigia, kad skirtumas tarp šių straipsnių yra tik prieigos prie ESM, sistemos ar tinklo teisėtumas ar neteisėtumas. 274 str. yra blanketinė norma, kuri nukreipia į kompiuterių sistemų eksploatavimo taisykles, tačiau 272 straipsnyje viena iš pasekmių nurodytas kompiuterių sistemos darbo pažeidimas, tai iš techninės pusės reiškia kompiuterių sistemos eksploatacijos režimo pažeidimą. Su šia pozicija sutikti negalima. Kompiuterių sistemos darbo sutrikdymas ir kompiuterių sistemos naudojimo taisyklių pažeidimas yra skirtingi dalykai, nes pirmuoju atveju dažniausiai sutrikdomas sistemos darbas (pvz., neveikianti paleidimo programa ar kt.), o antruoju atveju sistemos darbas

[110] Čepčugov D. MVD Onlain. *InterNet magazine*, 2001, 14. [interaktyvus, žiūrėta 2011-05-10]. <http://www.gagin.ru/internet/14/3.html>.
[111] Čepčugov D. MVD Onlain. *InterNet magazine*, 2001, 14. [interaktyvus, žiūrėta 2011-05-10]. <http://www.gagin.ru/internet/14/3.html>.
[112] Naumov V. Otečestvennoje zakonodatelstvo v borbe s kompiuternimu prestuplenijami [interaktyvus, žiūrėta 2011-06-27]. <http://www.russianlaw.net/law/doc/a01.htm>.
[113] Spivakov A. I. Rosijskoje zakonodatelstvo v borbe s kompiuternimi prestuplenijami. *Centr issledovanija problem kompjuternoj prestupnosti.* 2001 [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Spivak.htm >.
[114] Naumov V. Otečestvennoje zakonodatelstvo v borbe s kompiuternimu prestuplenijami [interaktyvus, žiūrėta 2011-06-27]. <http://www.russianlaw.net/law/doc/a01.htm>.
[115] Spivakov A. I. Rosijskoje zakonodatelstvo v borbe s kompiuternimi prestuplenijami *Centr issledovanija problem kompjuternoj prestupnosti.* 2001 [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Spivak.htm>.

gali ir nesutrikti. Be to, minėti straipsniai skiriasi pagal numatytą subjektą. Jei 272 straipsnio subjektas yra bendrasis, tai 274 straipsnio subjektas yra specialusis, todėl, šių straipsnių sujungimas būtų netikslingas. Diskusijos gali kilti dėl 272 bei 274 straipsnių nuostatos dėl įstatymo saugomos informacijos. Kaip jau minėta anksčiau, šio straipsnio dispozicijos reikalauja, jog būtų paveikta ne bet kokia informacija, o tik įstatymo saugoma informacija. Jei šią sąvoką aiškinsime plečiamai, įstatymo saugoma gali būti bet kokia informacija. Tačiau galimas ir toks variantas, jog įstatymo saugomai informacijai bus priskirta tik informacija, laikoma, pvz., tarnybine ar komercine paslaptimi, o visa kita informacija nepateks į „įstatymu saugomos informacijos“ apibrėžimą. Kai kuriuose komentaruose būtent ir nurodoma, jog įstatymo saugoma informacija reikia laikyti tokią informaciją, kuriai specialiais įstatymais nustatyta teisinė apsauga (valstybinė, tarnybinė ir komercinė paslaptys, asmens duomenys ir kt.)[116],[117]. Tokiu atveju tampa nesuprantamas Rusijos įstatymų leidėjų siekis apsaugoti tik dalį informacijos, nes privačių asmenų turima informacija, jei joje nėra komercinių paslapčių ir pan., tampa neapsaugota minėta norma. Tačiau paminėtinas Rusijos federalinio įstatymo Dėl informacijos, informatizacijos ir informacijos apsaugos 6 str., kuriame nustatyta, jog „*informaciniai resursai, esantys fizinių ir juridinių asmenų nuosavybe, laikomi jų turtu ir reglamentuojami civilinių įstatymų*“[118]. Taigi, pritaikant šį straipsnį, juridinių bei fizinių asmenų turimą kompiuterinę informaciją galima laikyti saugomą įstatymo ir ji patenka į 272 bei 274 straipsnių veikimo sritį.

Literatūroje kritikuojamas ir Rusijos baudžiamojo kodekso 273 straipsnis. *V. S. Komissarovas* nurodo, jog straipsnio dispozicija suformuota ne visai sėkmingai. Aprašant nusikalstamą veiką, vartojama daugiskaita, t.y. „kenkimo programos“. Todėl gali susidaryti įspūdis, kad įstatymo leidėjas baudžiamajai atsakomybei kilti reikalauja kelių kenkimo programų sukūrimo ar pan.[119] Tačiau, šio autoriaus nuomone, baudžiamosios atsakomybės už nurodytą nusikaltimą esmę sudaro ne tiek kiekybinis faktorius, kiek potencialiai konkrečios kenkimo programos savybės, t.y. jos sugebėjimas paveikti informaciją ar ESM darbą[120].

Taip pat, ekspertų nuomone, Rusijos baudžiamojo kodekso 272 ir 273 str. neišskiria pakankamai kvalifikuojančių sudėčių. Pvz., kompaktinių diskų su kompiuterių virusais platinimas turguje daug mažiau pavojingas nei botneto įkūrimas (kai tinklui gali priklausyti tūkstančiai užkrėstų kompiuterių). Kol kas abiem atvejais nusikaltėliui grėstų vienoda baudžiamoji atsakomybė[121].

Pastaruoju metu tarp Rusijos mokslininkų ir praktikų kyla diskusijos ir dėl grobimo

[116] Naumov V. Otečestvennoje zakonodatelstvo v borbe s kompiuternimu prestuplenijami [interaktyvus, žiūrėta 2011-06-27]. <http://www.russianlaw.net/law/doc/a01.htm>.

[117] Karelina M. M. Prestuplenije v sfere kompiuternoi informaciji. *Centr issledovanija problem kompjuternoj prestupnosti.* [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/CodeRu.htm>.

[118] Federal Law on Information, Informatization and the Protection of Information No. 24-FZ [interaktyvus, žiūrėta 2011-06-27]. str. 6. <http://www.fas.org/irp/world/russia/docs/law_info.htm>.

[119] Komissarov V. S. Prestuplenija v sfere kompiuternoi informaciji: ponetije i otvetstvennost. *Juridičeskij mir*, 1998, fevral, p. 16.

[120] Komissarov V. S. Prestuplenija v sfere kompiuternoi informaciji: ponetije i otvetstvennost. *Juridičeskij mir*, 1998, fevral, p. 16.

[121] Dlia borby s kiberprestupnostju nužny popravki v UK. *Centr issledovanija problem kompjuternoj prestupnosti.*[interaktyvus}. 2011-05-17 [žiūrėta 2011-06-27]. <http://www.crime-research.ru/news/17.05.2011/7235/>.

panaudojant elektroninę erdvę kvalifikavimo. Rusijos baudžiamajame kodekse nėra atskiros normos, nustatančios baudžiamąją atsakomybę už svetimo turto grobimą pasinaudojant elektronine erdve. Tuo Rusijos baudžiamieji įstatymai skiriasi nuo tokių valstybių, kaip Vokietija, JAV, įstatymų, kur jau seniai buvo pripažinta tokio pobūdžio normų būtinybė[122]. D. Gončarovas mano, jog literatūroje vartojamas terminas „kompiuterinis sukčiavimas“, atsižvelgiant į Rusijos baudžiamąjį kodeksą, yra fikcija, nes nė viena iš kodekse esančių normų visiškai nerodo tos visuomeninių santykių specifikos, atsirandančios neteisėtais tikslais naudojant kompiuterius. Šio autoriaus nuomone, jei asmuo, įveikęs kompiuterinės informacijos apsaugos sistemas, parinkęs slaptažodžius ir raktus, pateko į banko kompiuterių tinklą ir įvedė pakeitimus, o po to dėl tokių pakeitimų į savo sąskaitą pervedė piniginių lėšų, tokiu atveju jo veiksmus reikia kvalifikuoti pagal Rusijos baudžiamojo kodekso 272 str. ir straipsnio, nustatančio atsakomybę už grobimą, sutaptį[123]. Kiti autoriai tvirtina, jog tokiu atveju grobimas turi būti kvalifikuojamas kaip sukčiavimas[124] pagal Rusijos baudžiamojo kodekso 159 str., kuriame nurodyta, kad sukčiavimas – svetimo turto grobimas apgaule arba piktnaudžiaujant pasitikėjimu[125]. Taip pat ir *B. Zavidovas* nekelia klausimo, ar tokioje veikoje egzistuoja apgaulė. Anot šio autoriaus, kaip apgaulė traktuotini šie veiksmai: neteisėtas poveikis informacijos apdorojimo procesui, neteisėtas informacijos naudojimas ir kt.[126] Tačiau *D. Zikovas* nesutinka su tokia nuomone, teigdamas, jog tokiu atveju apgaunamas ne nukentėjusysis, o kompiuteris ar kompiuterių sistema, todėl tikslesnis terminas – manipuliacijos, o ne apgaulė[127]. *A. V. Černichas* pabrėžia, jog vykdant sukčiavimą panaudojant kompiuterį, manipuliuojama programomis, duomenimis ar aparatine elektroninės skaičiavimo sistemos dalimi[128]. Todėl *D. Zikovas* apgaulę vykdant sukčiavimą panaudojant kompiuterį supranta kaip tyčinius veiksmus, iškreipiant ar paslepiant duomenis, turint tikslą suklaidinti asmenį, arba manipuliacijas programomis, duomenimis ar aparatine elektroninės skaičiavimo mašinos dalimi, dėl to gaunamas turtas ar teisės į turtą. Tačiau autorius sutinka su nuomone, jog sukčiavimas panaudojant kompiuterį kvalifikuotinas pagal Rusijos baudžiamojo kodekso 159 str. („Sukčiavimas“)[129]. Nors apgaunant nukentėjusįjį, tiesiogiai su juo nekontaktuojama, tokie veiksmai laikytini apgaule ir pasireiškia paminėtu duomenų pakeitimu bei pan. Kadangi sukčiavimo sudėtis nereikalauja tiesioginio apgavimo, šiuo straipsniu kriminalizuojami ir sukčiavimo veiksmai, panaudojant kompiuterį (elektroninę erdvę). Tą patvirtina ir *I. V. Iljino* pozicija. Šis autorius nurodo, jog apgaule, aprašoma Rusijos baudžiamojo kodekso 159 straipsnyje, laikytinas tyčinis tiesos iškreipimas ar

[122] Gončarov D. Kvalifikacija chiščenij, soveršajemich s pomoščju kompjuterov. [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Goncharov.htm>.

[123] Gončarov D. Kvalifikacija chiščenij, soveršajemich s pomoščju kompjuterov. [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Goncharov.htm>.

[124] Kočoj S., Saveljev D. Otvetsvennost za neprovomernij dostup k kompiuternoj informaciji. *Rosijskaja justicija*, 1999, 1, p. 44-45.

[125] The Criminal code of the Russian Federation. [interaktyvus, žiūrėta 2011-06-27]. st. 159. <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.

[126] Zavidov B. O ponetiji mošenničestva i jego modifikacijach v ugolovnom prave. *Pravo i ekonomika*, 1998, 11, p. 50-51.

[127] Zykov D. Ponjatie obmana, soveršajemogo pri kompjuternom mošenničestve. *Centr issledovanija problem kompjuternoj prestupnosti*. [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Zikov1.htm>.

[128] Černov A. V. Nekotorije voprosi ugolovno-pravovoj kvalifikaciji kompiuternich mošenničetv. *Sovetskoje gosudarstvo i pravo*, 1989, 6, p. 71.

[129] Zykov D. Ponjatie obmana, soveršajemogo pri kompjuternom mošenničestve. *Centr issledovanija problem kompjuternoj prestupnosti*. [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Zikov1.htm>.

paslėpimas, turint tikslą suklaidinti asmenį, valdantį turtą ar teises į turtą, ir gauti turtą ar teises į turtą[130].

Už pornografinio turinio medžiagos platinimą baudžiamojon atsakomybėn traukiama remiantis Rusijos baudžiamojo kodekso 242 straipsniu. Šio straipsnio dispozicijoje nurodyta, jog yra baudžiama neteisėta pornografinio turinio dalykų gamyba, siekiant platinti ar reklamuoti, pornografinio turinio dalykų platinimas ar reklamavimas, taip pat neteisėta prekyba pornografinio turinio dalykais[131]. Pastebėtina, jog dispozicijoje neišskiriama veika, kai platinama medžiaga su vaikų pornografija. Tačiau, baudžiamųjų įstatymų nuostatos, susijusios su pornografinio turinio dalykais, atskirose valstybėse skiriasi, nes tai priklauso nuo valstybėje egzistuojančio visuomenės požiūrio į pornografinio turinio dalykus, vyraujančių tradicijų bei nuostatų. Literatūroje abejojama, ar 242 str. taikytinas veikoms internete, nes straipsnio dispozicija nėra aiški.

Už autorių teisių ir gretutinių teisių pažeidimus baudžiamojon atsakomybėn traukiama pagal Rusijos baudžiamojo kodekso 146 straipsnį. Šio straipsnio dispozicijoje nurodoma, jog baudžiamas neteisėtas autorių teisių ar gretutinių teisių objektų naudojimas, taip pat autorystės pasisavinimas, jei dėl to padaryta didelė žala[132]. Šios nuostatos skiriasi nuo kai kurių valstybių baudžiamųjų įstatymų nuostatų bei tarptautinių rekomendacijų, nes nenurodo komercinio tikslo. Straipsnio dispozicija nekriminalizuojama veika, kai autorių teisių objektai turint komercinį tikslą neteisėtai patalpinami elektroninėje erdvėje, nes terminas „naudojimas“ neturėtų apimti šios veikos.

3.2.2. Lenkija

Lenkija 2001 metais pasirašė Konvenciją dėl elektroninių nusikaltimų, bet iki šiol jos neratifikavo. Todėl Lenkijos baudžiamojo kodekso tiesiogiai neįtakoja šis tarptautinis teisės aktas.

Iš esmės visi su kompiuteriais susiję pažeidimai, kurie buvo paminėti 1989 m. ET rekomendacijos „minimaliame sąraše“, Lenkijoje buvo kriminalizuoti jau 1997 metų baudžiamajame kodekse. Teigiama, kad Lenkijoje naujasis baudžiamasis kodeksas beveik visais atvejais nustato atsakomybę už nusikalstamas veikas, įvykdomas per internetą. Pavyzdžiui, 1998 m. rugpjūčio 1 d. baudžiamasis kodeksas kriminalizuoja vadinamąjį neteisėtą patekimą į kompiuterių sistemą, pažeidžiant saugumo priemones. Tačiau šiuo atveju būtinas požymis yra apsaugotos informacijos pasisavinimas[133]. Taigi Lenkijoje neteisėtos prieigos sudėtis yra materiali, o ne formali ir neteisėta prieiga, nesukelianti pasekmių (informacijos pasisavinimo) nėra kriminalizuota.

1997 m. Lenkijos baudžiamojo kodekso 33 skyriuje „Pažeidimai prieš saugomą

[130] Iljin I. V. *Viktimologičeskaja profilaktika ekonomičeskogo mošenničestva*: Disertacija kand. jurid. nauk. N.Novgorod, 2000, p. 24-25.

[131] The Criminal code of the Russian Federation [interaktyvus, žiūrėta 2011-06-27]. st. 242. <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.

[132] The Criminal code of the Russian Federation [interaktyvus, žiūrėta 2011-06-27]. st. 146. <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.

[133] Kosinski J. Some Aspects of Computer Crime in Poland. *The Second International Scientific Practical Conference Information Society 2000 and League of Investors*, Vilnius, October 23-24, 2000, p. 124.

informaciją“ nustatyta baudžiamoji atsakomybė už pažeidimus:

- keliančius pavojų kompiuterinės informacijos bei kompiuterių sistemų konfidencialumui, integruotumui ir prieinamumui (267 str.);
- įsikišimą į kompiuterinės informacijos apdorojimą (268 str.);
- sabotažą, susijusį su kompiuteriais (269 str.)[134].

Taip pat specialios nuostatos dėl sukčiavimo, susijusio su kompiuteriais, ir neteisėto kompiuterių programų atgaminimo buvo įtrauktos 1997 metais į nusikaltimų prieš nuosavybę kategoriją. Teisinis dokumento apibrėžimas buvo modifikuotas, siekiant nustatyti baudžiamąją atsakomybę už klastojimą panaudojant kompiuterius.

1997 m. Lenkijos baudžiamasis kodeksas nustato baudžiamąją atsakomybę ir už kitus su kompiuteriais susijusius pažeidimus, tokius kaip:

- sukčiavimas telekomunikacijomis (285 str.);
- neteisėtos kompiuterių programos turėjimas (293 str.);
- špionažas, susijęs su kompiuteriais (130 str.);
- neteisėtai gautos informacijos platinimas (267 str.);
- medžiagos su vaikų pornografija platinimas (202 str.) [135].

1997 m. Lenkijos baudžiamasis kodeksas suteikia teisinę apsaugą įvairioms nuosavybės formoms (įskaitant intelektualios nuosavybės teises). Remiantis Lenkijos baudžiamuoju kodeksu, baudžiamoji atsakomybė gali kilti ir už šias veikas: medžiagos, susijusios su pornografija, platinimas, žalingo turinio informacijos platinimas, informacijos apie kreditinių kortelių kodus platinimas. Visos šios veikos dažniausiai vykdomos internete.

Lenkijos baudžiamojo kodekso veikimo sritis taip pat siekia ir tokias veikas, kai platinama informacija, gauta neteisėtu būdu. Remiantis kodekso 267 str. 3 d., tas, kuris atskleidžia kitam asmeniui informaciją, gautą pažeidžiant kompiuterių saugumo priemones ar perimant siunčiamą informaciją, yra baudžiamas laisvės atėmimu iki 2 metų. Ši dalis apima ne tiktai neteisėtai gautų slaptažodžių atskleidimą trečiajam asmeniui, tačiau ir tokios informacijos platinimą per elektronines skelbimų lentas ar sistemlaužių tinklalapiuose.

Lenkijos baudžiamojo kodekso 202 str. 3 d. draudžia medžiagos su vaikų pornografija (įeina medžiaga, susijusi su vaikais iki 15 metų) platinimą, taip pat informacijos, susijusios su smurto pasireiškimu, platinimą[136]. Ši norma taip pat taikoma ir internetu platinamai medžiagai. Paminėtina, jog Lenkijoje pirmasis teismo procesas, susijęs su

[134] Criminal Code of the Republic of Poland. [interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/documents/section/criminal-codes/country/10 >.
[135] Criminal Code of the Republic of Poland. [interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/documents/section/criminal-codes/country/10>.
[136] Criminal Code of the Republic of Poland. [interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/documents/section/criminal-codes/country/10>.

internetu siunčiama medžiaga su vaikų pornografija, įvyko 1997 m. Nusikaltėlis buvo nuteistas 9 mėnesiams laisvės atėmimo, atidedant bausmės vykdymą 3 metams. Jis buvo suimtas ir nuteistas dėl to, jog talpindamas į USENET grupes medžiagą, susijusią su vaikų pornografija, paliko elektroninius pėdsakus, t.y. elektroninio pašto adresą.

3.2.3. Ukraina

Ukraina Konvenciją dėl elektroninių nusikaltimų pasirašė 2001 metais, o ratifikavo 2006 metais (tais pačiais metais konvencija Ukrainoje ir įsigaliojo). Taigi Konvencija tapo Ukrainos nacionalinės teisės dalimi ir Ukrainos baudžiamasis kodeksas iki šios dienos turėtų atitikti pagrindines Konvencijos nuostatas dėl materialinės teisės.

Paminėtina, jog jau 2001 m. Ukrainoje buvo priimta nauja baudžiamojo kodekso redakcija, kurioje numatytas atskiras XVI skyrius „Nusikaltimai panaudojant elektronines skaičiavimo mašinas (kompiuterius), sistemas ir kompiuterių tinklus bei telekomunikacijų tinklus“. Iš pradžių šiame skyriuje buvo numatyti trys straipsniai: 361, 362 ir 363:

- 361 straipsnyje nusikaltimu įvardytas neteisėtas įsikišimas į elektroninės skaičiavimo mašinos, sistemos ar kompiuterių tinklo darbą, jei tokiais veiksmais buvo iškraipyta ar sunaikinta kompiuterinė informacija ar tokios informacijos laikmenos, taip pat kompiuterių viruso (naudojant programines ir technines priemones), skirto neteisėtai patekti į kompiuterių sistemą ar kompiuterių tinklą ir galinčio iškraipyti ar sunaikinti kompiuterinę informaciją ar tokios informacijos laikmeną, platinimas;
- 362 straipsnyje nusikaltimu įvardytas kompiuterinės informacijos pagrobimas, pasisavinimas, prievartavimas arba užvaldymas sukčiavimo būdu ar pasinaudojant tarnybine padėtimi;
- 363 straipsnyje nusikaltimu įvardytas automatizuotų elektroninių skaičiavimo sistemų ar kompiuterių tinklų eksploatavimo taisyklių pažeidimas asmens, atsakingo už jų eksploataciją, jei dėl to buvo pagrobta, iškraipyta ar sunaikinta kompiuterinė informacija, jos apsaugos priemonės, arba neteisėtas kompiuterinės informacijos kopijavimas ar esminis kompiuterių sistemos darbo pažeidimas.

Paminėtina, jog pagal minėto Ukrainos baudžiamojo kodekso skirsnio straipsnių kvalifikuojančias dalis, jei veiksmais padaroma didelė žala, taikoma griežtesnė atsakomybė[137].

Tačiau vėliau skirsnis buvo papildytas šiais straipsniais:

- 361-1 str. Žalingos programinės ir aparatinės įrangos kūrimas turint tikslą

[137] Orlov P., et al. K opredeleniju vida i razmera nakazanija za prestuplenija v sfere ispolzovanija elektronnoi-vičislitelnoj techniki (kompjuterov), sistem i kompjiuternykh setej v svjazi s prinjatijam novogo ugolovnogo kodeksa Ukrainy. *Centr issledovanija problem kompiuternoj prestupnosti*. [interaktyvus, žiūrėta 2011-06-27] <http://www.crime-research.org/library/End.htm>.

naudoti, skleisti ar platinti, taip pat skleidimas ir platinimas;

- 361-2 str. Ribotos informacijos, kuri saugoma kompiuteriuose, automatinėse sistemose, kompiuterių tinkluose ar informacijos laikmenose, neteisėtas skleidimas ir platinimas;
- 363-1 str. Kompiuterių, automatinių sistemų, kompiuterių tinklų ar telekomunikacijų tinklų darbo sutrikdymas, panaudojant masines elektronines žinutes.

Kaip matome, pastarieji Ukrainos baudžiamojo kodekso pakeitimai atlikti reaguojant į pastarųjų metų grėsmes dėl elektroninių nusikaltimų. Ypač paminėtinas 363-1 str., kuris skirtas užkirsti kelią DDoS atakoms.

Grįžtant prie pirmųjų trijų Ukrainos baudžiamojo kodekso straipsnių, 361 straipsnio dispozicijoje nurodyta, jog baudžiamąją atsakomybę užtraukia neteisėtas įsikišimas į elektroninės skaičiavimo mašinos, jų sistemos ar kompiuterių tinklo darbą, dėl to buvo paveikta (sugadinta ar sunaikinta) kompiuterinė informacija, taip pat kompiuterių viruso, skirto patekti į kompiuterių sistemą ar tinklą ir paveikti kompiuterinei informacijai, platinimas[138]. *M. I. Melnik* teigia, kad šiuo straipsniu kriminalizuojamos dvi veikų rūšys:

- neteisėtas įsikišimas į elektroninės skaičiavimo mašinos, jų sistemų ar kompiuterių tinklo darbą, dėl to kyla nurodytos pasekmės;
- kompiuterių viruso platinimas, kai jokių žalingų pasekmių nereikalaujama[139].

Nors šios nuostatos įvestos neseniai, kai kurie mokslininkai jau pareiškė nuomonę dėl galimų probleminių klausimų. *M. Dutovas* kritikuoja Ukrainos baudžiamąjį kodeksą, nes šiame įstatyme nenustatyta, kas yra laikoma kompiuterine informacija. Šis autorius pateikia Rusijos pavyzdį, kur baudžiamojo kodekso 272 str. „Neteisėta prieiga prie kompiuterinės informacijos“ nurodoma, jog toks terminas turi būti suprantamas kaip informacija laikmenoje, esančioje elektroninėje skaičiavimo mašinoje, ESM sistemoje ar tinkle. Nors Ukrainos norminiuose aktuose ir yra detalizuojamos panašios sąvokos, pvz., „informacija automatizuotoje sistemoje“, šio autoriaus nuomone, reikia tiksliai nustatyti, kas yra kompiuterinė informacija.

Taip pat kritikuojamos Ukrainos baudžiamojo kodekso nuostatos dėl kompiuterių virusų. *M. Dutovo* nuomone, kompiuterių virusas gali būti nepiktybiškas, todėl nustatyti baudžiamąją atsakomybę už kompiuterių viruso platinimą netikslinga, be to, egzistuoja daug kitų programų, dėl kurių panaudojimo kyla žalingos pasekmės (tai Trojos arkliai, kirminai ir kt., kurie gali būti panaudojami grobiant pinigus iš banko sąskaitų, šnipinėjant ar chuliganiškais tikslais ir t.t.)[140]. Su tokia pozicija galima sutikti iš dalies. Ukrainos baudžiamajame kodekse vis dėlto yra normos, pagal kurias galima kvalifikuoti veiksmus, kai panaudojamos kitos kenkimo programos. Pvz., Ukrainos baudžiamojo

[138] Kriminalnij kodeks Ukrainy. *Oficialnij vestnik Ukrainy*, 2001, p. 105-106, st. 361.
[139] Melnik M. I. *Naučno-praktičeskij komentarij ugolovnogo kodeksa Ukraini*. Kiev: Kannon, A.C.K, 2001, p. 902.
[140] Ten pat,, p. 902.

kodekso 362 str. nustatyta atsakomybė už informacijos pagrobimą sukčiaujant ar piktnaudžiaujant tarnybine padėtimi, todėl paminėtų kenkimo programų panaudojimas iš dalies gali užtraukti baudžiamąją atsakomybę pagal šį straipsnį. Tačiau 361 straipsnyje nėra numatyta baudžiamoji atsakomybė už tokias veikas, kai informacija sunaikinama panaudojant Trojos arklį ir kitais būdais. Tačiau nagrinėjamu atveju galima pasiremti Rusijos pavyzdžiu, kur normos suformuluotos vartojant šį apibrėžimą: „kenkimo programos, skirtos elektroninėms skaičiavimo mašinoms, galinčioms neteisėtai sukelti kompiuterinės informacijos sunaikinimą, blokavimą, modifikaciją ar kopijavimą, arba sutrikdyti kompiuterių sistemos ar tinklo darbą“, kuris, tinkamesnis apibrėžti kenkimo programoms, nenurodant konkrečios programos rūšies. Be to, Rusijos baudžiamajame kodekse nustatyta atsakomybė ne tik už kenkimo programų platinimą, bet ir kūrimą.

Ukrainos baudžiamojo kodekso 362 straipsnio dispozicijoje nurodyta, jog baudžiamoji atsakomybė kyla už kompiuterinės informacijos pagrobimą, pasisavinimą ar prievartavimą arba tokios informacijos užvaldymą sukčiavimo būdu ar piktnaudžiaujant tarnybine padėtimi. Taigi šios nusikaltimo sudėties objektyviąją pusę sudaro veiksmai, kai asmuo neteisėtai, prieš kompiuterinės informacijos savininko ar teisėto valdytojo valią, užvaldo tokią informaciją, o šios informacijos savininkas ar teisėtas valdytojas ją praranda[141].

Ukrainos baudžiamojo kodekso 363 straipsnio dispozicijoje nurodyta, jog baudžiamoji atsakomybė kyla už elektroninių skaičiavimo mašinų, jų sistemų ar kompiuterių tinklo eksploatavimo taisyklių pažeidimą asmens, atsakingo už jų eksploataciją, jei dėl to buvo pagrobta ar sunaikinta kompiuterinė informacija, jos apsaugos priemonės ar kompiuterinė informacija buvo neteisėtai nukopijuota arba buvo itin sutrikdytas elektroninės skaičiavimo mašinos, jų sistemos ar kompiuterių tinklo darbas[142]. Remiantis šio straipsnio sudėtimi, subjektas yra specialus, t.y. asmuo, kuris atsako už elektroninės skaičiavimo mašinos, jų sistemų ar kompiuterių tinklų eksploataciją. Toks asmuo dažniausiai būna elektroninės skaičiavimo mašinos, jų sistemų ar kompiuterių tinklo naudotojas, taip pat kitas asmuo, kuris, remdamasis darbo, tarnybinėmis pareigomis ar pagal atitinkamą susitarimą su elektroninės skaičiavimo mašinos, jų sistemų ar kompiuterių tinklo administratoriumi, vykdo veiksmus, susijusius su elektroninės skaičiavimo mašinos, jų sistemų ar kompiuterių tinklo darbo režimo palaikymu, informacijos atnaujinimu, apsauga ar kt.[143] Šio nusikaltimo subjektyvioji pusė gali pasireikšti ir neatsargia kaltės forma, o kvalifikuojančiu požymiu yra didelės žalos padarymas[144].

Prieš keletą metų kai kurie autoriai Ukrainos baudžiamąjį kodeksą kritikavo

[141] Prestuplenija v sfere ispolzovanija elektronno-vyčeslitelnykh mašin (kompjuterov), sistem i kompjuternykh setej. *Centr issledovanija problem kompjuternoj prestupnosti.*[interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/npkrus.htm>.

[142] Criminal code of Ukraine.[interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/documents/action/popup/id/16257/preview >.

[143] Prestuplenija v sfere ispolzovanija elektronno-vičeslitelnich mašin (kompiuterov), sistem i kompiuternich setej. *Centr issledovanija problem kompjuternoj prestupnosti.*[interaktyvus, žiūrėta 2011-06-27] <http://www.crime-research.org/library/npkrus.htm>.

[144] Melnik M. I. *Naučno-praktičeskij komentarij ygolovnogo kodeksa Ukraini.* Kiev:Kannon, A.C.K., 2001, p. 907.

dėl tokių trūkumų: anot *I. A. Varonovo*, Ukrainos baudžiamasis kodeksas nenustato baudžiamosios atsakomybės pagrindų už kompiuterinės informacijos blokavimą, t.y. kai teisėtas vartotojas negali prieiti prie kompiuterinės informacijos, nors ji yra kompiuterio atmintyje. Nuo kompiuterinės informacijos blokavimo reikėtų skirti kompiuterinės informacijos sugadinimą, nes tai du skirtingi dalykai[145]. Tačiau ši problema buvo išspręsta, Ukrainos baudžiamąjį kodeksą papildžius 363-1 straipsniu.

Be paminėtų straipsnių, Ukrainos baudžiamajame kodekse yra kriminalizuotos ir kitos pavojingos veikos panaudojant kompiuterius, pvz., 158 straipsnyje numatyta baudžiamoji atsakomybė už rinkimų dokumentų, referendumo dokumentų klastojimą ir kt.

3.2.4. Estija

Estija siejama su bene didžiausią atgarsį sukėlusiomis atakomis prieš informacines sistemas. Kaip minėta aukščiau, 2007 metais prieš keletą Estijos informacinių sistemų (daugiausia valstybinių) buvo suorganizuotos masinės kompiuterių atakos. Praėjus keleriems metams, Estijos užsienio reikalų ministras Europos-Azijos užsienio reikalų ministrų susitikime pabrėžė, kad 2007 metų atakos Estiją privertė elektroninių nusikaltimų grėsmę vertinti daug rimčiau[146]. Dėl to Estija yra viena iš tų valstybių, kurios skiria daug dėmesio kovai su elektroniniais nusikaltimais.

Estija jau prieš keletą metų buvo minima tarp tų valstybių, kurios iš esmės ar visiškai pakeitė savo įstatymus, nustatančius baudžiamąją atsakomybę už nusikaltimus elektroninėje erdvėje. Estijoje baudžiamoji atsakomybė už kompiuterinius nusikaltimus (iš kurių daugelio dispozicijos skirtos nustatyti baudžiamajai atsakomybei už nusikaltimus elektroninėje erdvėje) yra didžiąja dalimi nustatyta Estijos baudžiamojo kodekso 14 skyriuje „Nusikaltimai, susiję su kompiuteriais ir darbo vieta“ (angl. *Computer and work place related crimes*), kuris buvo parengtas remiantis Europos šalių (ypač Vokietijos) praktika ir apima:

- sukčiavimą panaudojant kompiuterius (par. 268);
- kompiuterių programos ar duomenų sunaikinimą (par. 269);
- sabotažą panaudojant kompiuterius (par. 270);
- neteisėtą kompiuterio, kompiuterių sistemos ar kompiuterųtinklo naudojimą (par. 271);
- kompiuterių tinklo sujungimų pažeidimą ar blokavimą (par. 272);
- kompiuterių virusų platinimą (par. 273);

[145] Voronov I. A. Nekotorije problemi deistvujuščego zakonodatelstva po vaprosam ugolovnoi otvetstvennosti za prestuplenija v sfere ispolzovanija elektronno-vičislitelnykh mašyn. [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Voron.htm>.

[146] Estonia called Asian countries to fight cybercrime. Estonian Ministry of foreign affairs. [interaktyvus, žiūrėta 2011-06-27]. <http://www.vm.ee/?q=en/node/11803>.

- slaptažodžių platinimą (par. 274);
- neteisingos, klaidinančios informacijos pateikimą verslo pasauliui (par. 275);
- informacijos pasisavinimą iš valstybės ar savivaldybės institucijos (par. 276)[147].

Taip pat Estijos baudžiamajame kodekse yra ir kitų straipsnių, pagal kuriuos gali kilti baudžiamoji atsakomybė už pavojingas veikas elektroninėje erdvėje: skyrius skirtas intelektinės nuosavybės apsaugai, nuostatos, skirtos kriminalizuoti medžiagos, susijusios su vaikų pornografija, gaminimą ir t.t.

Pažymėtina, jog dėl baudžiamosios teisės reformos nuo 2002 m. kovo mėn. Estijoje įsigaliojo naujasis baudžiamasis kodeksas. Šio kodekso nuostatos, susijusios su nusikaltimais elektroninėje erdvėje, paremtos senojo kodekso nuostatomis, tačiau naujajame kodekse jos ne išskirtos į vieną skirsnį, o išdėstytos įvairiuose skyriuose, daugiausia – nusikaltimų prieš nuosavybę skyriuje. Naujasis Estijos baudžiamasis kodeksas taip pat kriminalizuoja medžiagos, susijusios su vaikų pornografija, platinimą ar padarymą prieinama kitiems.

2004 metais Estijoje įsigaliojo 2001 metais ratifikuota Konvencija dėl elektroninių nusikaltimų[148]. Todėl Konvencija taip pat tapo ir Estijos teisės sistemos sudedamąja dalimi. Baudžiamojo kodekso pakeitimai, galutinai įgyvendinantys Konvencijos nuostatas, Estijoje buvo priimti tik 2008 metais. Vieni iš svarbiausių pakeitimų, kad Estijoje už elektroninius nusikaltimus atsakomybė numatyta ir juridiniam asmeniui, be to, padidintos bausmės už kai kuriuos elektroninius nusikaltimus[149].

3.2.5. Latvija

Latvija, kaip ir Lietuva ar Estija, yra ratifikavusi Konvenciją dėl elektroninių nusikaltimų. Konvencija Latvijoje įsigaliojo 2007 metais[150].

Latvijoje baudžiamoji atsakomybė nustatyta už šiuos nusikaltimus elektroninėje erdvėje:

- neteisėtą prieigą prie kompiuterių sistemos;
- neteisėtą kompiuterių programos pasisavinimą;
- žalos padarymą kompiuterių programai;
- kompiuterių viruso platinimą;

[147] Schjolberg S. The Legal Framework – Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries. Moss District Court, Norway. [interaktyvus, žiūrėta 2011-06-28]. <http://www.mosstingrett.no/info/legal.html>.
[148] Convention of Cybercrime. CETS No.:185, Status as of: 13/06/2011. [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=13/06/2011&CL=ENG>.
[149] Estonia changes in Penal Code. Baltic Legal Newsletter. Spring, 2008. [interaktyvus, žiūrėta 2011-06-27].
<http://www.infolex.lt/portal/ml/start.asp?act=legupd&lang=eng&biulid=144&srid=27&strid=858>.
[150] Convention of Cybercrime. CETS No.:185, Status as of: 13/06/2011. [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=15/06/2011&CL=ENG>.

➤ informacinių sistemų saugumo taisyklių pažeidimą.

Nusikaltimų sudėtys dėl elektroninių nusikaltimų Latvijoje nėra išskirtos į atskirą skirsnį ir išdėstytos šalia kitų nusikaltimų.

Latvijos baudžiamojo kodekso 241 straipsnyje nustatyta atsakomybė už savavališką prieigą prie kompiuterių sistemų. Šio straipsnio 1 dalyje nurodyta, jog baudžiamojon atsakomybėn traukiamas asmuo, kuris savavališkai prisijungia prie kompiuterių sistemos, jei tai susiję su apsaugos priemonių pažeidimu ar sukeliama didelė žala[151]. Kvalifikuotos sudėtys nustatytos tuo atveju, jei neteisėtai pasisavinama nuosavybė (2 dalis) ar prisijungimas atiekamas prie Valstybės informacinės sistemos (3 dalis).

Latvijos baudžiamojo kodekso 243 straipsnyje nustatyta baudžiamoji atsakomybė už įsikišimą į automatinės duomenų aprodorojimo sistemos darbą ar neteisėtus veiksmus su šiose sistemose tvarkoma informacija. Šio straipsnio 1 dalyje nurodyta, jog baudžiamojon atsakomybėn traukiamas asmuo, kuris neturėdamas tam teisės, pakeičia, padaro žalą ar sunaikina informaciją, išsaugotą automatinėje skaičiavimo sistemoje, ar žinodamas įveda klaidingą informaciją į automatinę sistemą, ar padaro žalą arba sunaikina informacinius įrenginius, kompiuterių programinę įrangą ar apsaugos sistemas, jei tokiais veiksmais padaroma didelė žala[152]. Straipsnio 2 dalyje numatyta baudžiamoji atsakomybė už įsikišimą į automatinės duomenų apdorojimo sistemos darbą, įvedant, persiunčiant, pakeičiant ar paslepiant informaciją, jei pažeidžiamos apsaugos sistemos arba sukeliami didelės vertės praradimai. Straipsnio 3 dalyje numatyta baudžiamoji atsakomybė už 1 ar 2 dalyse numatytus veiksmus, kurie įvykdomi grupės asmenų arba su tikslu pasisavinti nuosavybę arba jei sukeltos sunkios pasekmės. Straipsnio 4 dalyje numatyta baudžiamoji atsakomybė už 1 ar 2 dalyse numaytus veiksmus, jei veika nukreipta prieš Valstybės informacinę sistemą.

Kodekso 244 straipsnis nustato baudžiamąją atsakomybę už įrenginių (įskaitant programinę įrangą) gaminimą, adaptavimą, pardavimą ar saugojimą, ketinant įtakoti informacines sistemas, turint tikslą įvykdyti nusikaltimą[153]. Remiantis šio straipsnio 2 dalimi, atsakomybę sunkinantis požymis yra didelės žalos padarymas.

Prieš keletą metų galiojusioje dispozicijoje buvo minima tik viena iš kenkimo programų rūšių – virusas. Be viruso, nurodytas pasekmes gali sukelti ir loginės bombos, kirminai ir kt. Dėl šios priežasties ankstesnė redakcija nepagrįstai siaurino straipsnio veikimo sritį, dėl to tam tikros veikos galėjo neužtraukti baudžiamosios atsakomybės. Todėl Latvijos įstatymo leidėjas pakeitė ir papildė minimą straipsnį.

Taip pat papildomai į Latvijos baudžiamąjį kodeksą įrašytas244-1 straipsnis. Duomenų, programų ar įrangos įgijimas, vystymas, keitimas, saugojimas ar platinimas elektroninių ryšių tinklų galiniuose įrenginiuose, turint neteisėtą tikslą.

[151] Criminal Code of the Republic of Latvia. [interaktyvus, žiūrėta 2011-06-27]. 241 str. <http://www.legislationline.org/documents/section/criminal-codes>.
[152] Criminal Code of the Republic of Latvia. [interaktyvus, žiūrėta 2011-06-27]. 243 str. <http://www.legislationline.org/documents/section/criminal-codes>.
[153] Criminal Code of the Republic of Latvia. [interaktyvus, žiūrėta 2011-06-27]. art. 244. <http://www.legislationline.org/documents/section/criminal-codes>.

Kodekso 245 straipsnis nustato baudžiamąją atsakomybę už informacinių sistemų saugumo taisyklių pažeidimą. Pagal šio straipsnio 1 (ir vienintelę) dalį, baudžiamojon atsakomybėn traukiamas asmuo, kuris pažeidžia informacijos saugojimo arba apdorojimo procesą reglamentuojančias nuostatas, arba pažeidžia kitas kompiuterių sistemų saugumo nuostatas, jei veika įvykdoma asmens, kuris privalo tokių nuostatų laikytis, ir jei dėl to buvo įvykdyta vagystė, buvo sunaikinta ar padaryta žala informacijai, ar padaryta didelė žala[154].

Už sukčiavimą Latvijoje baudžiama pagal bendras sukčiavimo normas, numatytas Latvijos baudžiamojo kodekso 177 str. „Sukčiavimas". Sukčiavimas pabaudojant kompiuterį nėra išskirtas, o kvalifikuojančios sudėtys siejamos su didelės žalos padarymu ir kt. Ta pati situacija ir dėl klastojimo – Latvijos baudžiamojo kodekso 265 str.

Neteisėti veiksmai su pornografine medžiaga kriminalizuoti Latvijos baudžiamojo kodekso 166 str. Kai tuo tarpu, neteisėti veiksmai su vaikų pornografine medžiaga kriminalizuoti tos paties straipsnio antroje dalyje (kvalifikuojanti sudėtis). Tačiau, paminėtina, kad Latvijos įstatymo leidėjas nutarė nekriminalizuoti vaikų pornografijos laikymo – baudžiamoji atsakomybė už šią pavojingą veiką Latvijoje nėra nustatyta.

Manoma, kad Latvijos baudžiamojo kodekso nuostatos dėl elektroninių nusikaltimų visiškai įgyvendina Konvencijos dėl elektroninių nusikaltimų bei atitinkamų Europos Sąjungos dokumentų nuostatas[155].

3.2.6. Jungtinė Karalystė

Jungtinė Karalystė Konvenciją dėl elektroninių nusikaltimų ratifikavo tik 2011 m. gegužės 25 d.[156] Konvencijos įsigaliojimas numatytas 2011 m. rugsėjo 1 d.[157] Dėl šios priežasties atitinkami Jungtinės Karalystės teisės aktai pristatomi su prezumpcija, kad šie teisės aktai dar nėra derinti su Konvencijos nuostatomis.

Tačiau net ir specialiai neįgyvendinus Konvencijos Jungtinės Karalystės teisės sistemoje, ši valstybė laikoma viena iš pirmaujančių kovoje su elektroniniais nusikaltimais. Kadangi ši valstybė neturi baudžiamojo kodekso, todėl ir baudžiamosios teisės specialioji dalis objektyviai yra atskirų baudžiamosios teisės šaltinių – statutų ir teisminių precedentų bei juose išdėstytų atitinkamų normų nesusisteminta visuma[158].

Jungtinėje Karalystėje, remiantis 1990 m. priimtu Piktnaudžiavimo panaudojant kompiuterius įstatymu, baudžiamosios atsakomybės pagrindai nustatyti už šiuos pagrindinius nusikaltimus elektroninėje erdvėje:

[154] Criminal Code of the Republic of Latvia. [interaktyvus, žiūrėta 2011-06-27]. art. 245. <http://www.legislationline.org/documents/section/criminal-codes>.

[155] Lestrade Dr. Edward, The Cybercrime Phenomenon and Latvian Cybercrime Law. Available at SSRN. [interaktyvus, žiūrėta 2011-06-27]. p. 6. < http://ssrn.com/abstract=971182>.

[156] UK finally ratifies convention on cybercrime. *ComputerWeekly.com*, May 25, 2011[interaktyvus, žiūrėta 2011-06-15]. <http://www.computerweekly.com/blogs/when-it-meets-politics/2011/05/uk-finally-ratifies-the-conven.html >.

[157] Convention of Cybercrime. CETS No.:185, Status as of: 13/06/2011. [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/06/2011&CL=ENG>.

[158] Abramavičius A., et al. *Baudžiamoji teisė: specialioji dalis*. 2 knyga. Vilnius: Eugrimas, 2000, p. 527.

- ➤ neteisėtą prieigą prie kompiuterių sistemų;
- ➤ neteisėtą prieigą siekiant įvykdyti ar palengvinti kitų nusikaltimų įvykdymą;
- ➤ neteisėtą kompiuterių duomenų pakeitimą;
- ➤ kitus nusikaltimus elektroninėje erdvėje[159].

Remiantis paminėto įstatymo *1 skyriumi* „Neteisėta prieiga prie duomenų elektronine forma“, asmuo pripažįstamas kaltu, jei:

- atlieka veiksmus, siekdamas su kompiuteriu įvykdyti prieigą prie bet kokios kompiuterių programos ar kompiuterių duomenų, esančių kitame kompiuteryje;
- prieiga, kurią ketinama atlikti, yra neteisėta;
- asmuo supranta, jog atlieka veiksmus, siekdamas įvykdyti neteisėtą prieigą.

Reikia paminėti, jog šios normos taikymas veikoms elektroninėje erdvėje gali pasireikšti tuo, kad net nesėkmingas sistemlaužio bandymas įvykdyti neteisėtą prieigą gali būti įvertintas kaip nusikaltimas[160],[161]. Dažniausiai tam, kad įvykdytų neteisėtą prieigą, asmuo turi atlikti identifikavimo procedūrą. Jei nukentėjusiojo kompiuteris atmeta neteisėtą identifikavimą, galima manyti, jog asmuo privertė dirbti du kompiuterius: jo paties ir nukentėjusiojo. Nukentėjusiojo kompiuteris atliko funkciją – jis atmetė sistemlaužio bandymą patekti į kompiuterį. Todėl atsakomybę užtraukia netgi nesėkmingas bandymas[162]. *M. Wasik* nurodo, jog remiantis straipsnio dispozicija, panašu, kad baudžiamajai atsakomybei kilti nereikia įveikti jokių kompiuterių sistemos apsaugos priemonių – jų gali ir nebūti[163]. Tuo šio įstatymo nuostatos skiriasi nuo kai kurių kitų valstybių baudžiamųjų įstatymų nuostatų, kuriose reikalaujama, kad būtų pažeistos saugumo priemonės. Tačiau Jungtinės Karalystės teisės komisija yra konstatavusi, jog neteisėtos prieigos kriminalizavimas tik apsaugotos informacijos atžvilgiu būtų prilygintas absurdiškai situacijai, pvz., jei neužrakinto automobilio vagystė nebūtų pripažįstama nusikaltimu[164].

Kai kurie autoriai (pvz., *M. Wasik*) kritikuoja paminėtą nuostatą, teigdami, jog neteisėta prieiga kriminalizuota netikslingai, nes neteisėtas įsibrovimas į namus nėra nusikaltimas, o prieigą elektroniniu būdu galima laikyti tokių veiksmų analogija[165]. Tačiau nagrinėjamu atveju baudžiamosios teisės normomis yra apsaugomas privatumas, kompiuterių sistemos integralumas, todėl tokios normos įvedimas į baudžiamuosius

[159] Nathanson N., Gringras C. *The Laws of the Internet*. Butterworths, 1997, p. 267.
[160] Nathanson N., Gringras C. *The Laws of the Internet*. Butterworths, 1997, p. 217.
[161] Baibridge D. *Introduction to Computer Law*. Fourth edition. Pearson Education Limited, 2000, p. 315.
[162] Nathanson N., Gringras C. *The Laws of the Internet*. Butterworths, 1997, p. 217.
[163] Akdeniz Y., Walker C., Wall D. *The Internet, Law and Society.* Pearson Education Limited, 2000, p. 275.
[164] Akdeniz Y., Walker C., Wall D. *The Internet, Law and Society.* Pearson Education Limited, 2000, p. 277.
[165] Wasik M. Computer Crimes and Other Crimes Against Information Technology in United Kingdom. *International Review of Penal Law: Computer Crimes and Other Crimes Against Information Technology*. Wurzburg, Germany, 1992, p. 629.

įstatymus yra tikslingas.

Minėto įstatymo *2 skyriuje* „Neteisėta prieiga turint tikslą įvykdyti ar palengvinti kitų nusikaltimų įvykdymą“ nurodoma, jog asmuo laikomas kaltu, jei:

- įvykdo nusikaltimą, nurodytą 1 skyriuje, siekdamas įvykdyti kitą šiame skyriuje nurodytą nusikaltimą, ar
- palengvina tokio nusikaltimo įvykdymą[166].

Nusikaltimas, kurį siekiama įvykdyti, turi būti baudžiamas ne mažiau kaip 5 metais laisvės atėmimo. Į tokių nusikaltimų sąrašą įeina vagystė, sukčiavimas ir kt. Paminėtina, jog baudžiamoji atsakomybė už nurodytą nusikaltimą kyla, net jei tolesnio nusikaltimo įvykdymas yra neįmanomas, t.y. įstatymas nereikalauja žalos padarymo (užtenka vien tiktai tikslo)[167],[168]. 2 skyriaus nuostatos apima ir tokius veiksmus kaip kenkimo programų įvedimą į kompiuterių sistemą, turint nurodytą ketinimą[169].

Anksčiau paminėto įstatymo 3 *skyriuje* „Neteisėtas modifikavimas“ nurodoma, jog asmuo laikomas kaltu, jei:

- įvykdo veiksmą ir dėl to modifikuojamas bet kokio kompiuterio turinys, ir
- veiksmo vykdymo metu turi reikiamą ketinimą bei reikiamų žinių.

Piktnaudžiavimo kompiuteriais įstatyme „reikiamas ketinimas“ apibrėžiamas kaip ketinimas modifikuoti bet kokio kompiuterio turinį ir kartu susilpninti kompiuterio darbą, apriboti prieigą prie bet kokios programos ar duomenų bet kokiame kompiuteryje, pabloginti bet kokios programos darbą ar bet kokių duomenų patikimumą[170]. Taigi ši nuostata apima tokias veikas kaip virusų, kirminų, Trojos arklių ar loginių bombų įvedimą, ir reikia pažymėti, kad atsakomybei kilti užtenka vien tiktai ketinimo atlikti modifikaciją[171]. *M. Wasik* teigia, kad ši norma apima ir tuos atvejus, kai asmuo siekia blokuoti prieigą prie informacijos ar programų ar pan.[172]

N. Nathanson, C. Gringras kritikuoja Piktnaudžiavimo panaudojant kompiuterius įstatymą, nes šiame teisės akte neapibrėžta sąvoka „kompiuteris“. Tačiau šie autoriai nurodo, jog kai kalbama apie nusikaltimus internete, problemų neturėtų būti, nes internetas yra tarpusavyje sujungtų kompiuterių tinklas ir savaime suprantama, jog prie interneto gali būti prijungtas tik kompiuteris[173]. Minėti autoriai taip pat pateisina tokių sąvokų kaip „kompiuterių programa“ ar „duomenys“ nebuvimą. Šios sąvokos Jungtinės Karalystės teisės aktuose neapibrėžtos dėl to, jog baiminamasi, kad dėl staigaus

[166] Computer Missuse Act, 1990. [interaktyvus, žiūrėta 2011-06-27]. par. 2. <http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm >.
[167] Rowland D.; Macdonald E. *Information Technology Law*. Cavendish Publishing Limited, 1997, p. 347.
[168] Nathanson N., Gringras C. *The Laws of the Internet*. Butterworths, 1997, p. 218.
[169] Wasik M. Computer Crimes and Other Crimes Against Information Technology in United Kingdom. *International Review of Penal Law: Computer Crimes and Other Crimes Against Information Technology*. Wurzburg, Germany, 1992, p. 636.
[170] Computer Missuse Act, 1990. [interaktyvus, žiūrėta 2011-06-27]. sec. 3(2). <http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm >.
[171] Nathanson N., Gringras C. *The Laws of the Internet*. Butterworths, 1997, p. 231.
[172] Akdeniz Y., Walker C., Wall D. *The Internet, Law and Society*. Pearson Education Limited, 2000, p. 283.
[173] Nathanson N., Gringras C. *The Laws of the Internet*. Butterworths, 1997, p. 214.

technologijų pokyčio sąvokos taps pasenusios. Panašią poziciją išdėsto ir *D. Baibridge*, nurodydamas, jog teismai gali nustatyti šią sąvoką traktuoti atsižvelgiant į konkrečią situaciją[174]. *M. Wasik* laikosi nuomonės, jog problemų, susijusių su sąvokų nebuvimu, ateityje vis dėlto turėtų kilti, kartu pažymi, jog kol kas nebuvo bylų, kurių metu būtų iškelta kompiuterio apibrėžimo problema[175]. Jungtinė Karalystė priklauso precedentų teisinės sistemos valstybėms, toks sąvokos nebuvimas iš dalies pateisinamas, tuo tarpu tai vargu ar pritaikytina civilinės teisės tradicijos teisinei sistemai priklausančioms valstybėms. Elektroninės erdvės vystymasis bei technologinis progresas leidžia prie šios erdvės prijungti netgi tokius daiktus kaip automobilyje sumontuotas sistemas ir kt. Todėl norint išvengti problemų vertinant tam tikras veikas elektroninėje erdvėje, vis dėlto patartina teisės aktuose apibrėžti pagrindines sąvokas. Galima pasiremti Rusijos bei kitų valstybių pavyzdžiu, kur minėtos sąvokos teisės aktuose yra apibrėžtos, ir praktikoje dėl to problemų nekyla.

Už sukčiavimo veikas panaudojant kompiuterį atsakomybė nustatyta 1968 m. Vagystės įstatymo (angl. *Theft act*) 15-20 skyriuose bei 1978 m. Vagystės įstatymo 1 bei 2 skyriuose. Pavyzdžiui, 1978 m. Vagystės įstatymo 1(1) skyrius nustato, jog baudžiamojon atsakomybėn traukiamas asmuo, kuris nesąžiningai apgaulės būdu naudojasi kito asmens paslaugomis[176]. Tačiau literatūroje kritiškai vertinamos tos nuostatos, kurios reikalauja, jog sukčiavimo veika turi pasireikšti tam tikro asmens apgaule[177]. Šio požymio trūksta vykdant panašią veiką elektroninėje erdvėje, todėl įstatymai turi būti peržiūrėti.

Už pažeidimus, susijusius su neteisėtu turiniu (pornografine medžiaga ar pan.), atsakomybė nustatyta remiantis 1959 m. Nešvankių leidinių įstatymu, 1978 m. Vaikų apsaugos įstatymu ir kitais teisės aktais. Pavyzdžiui, remiantis Vaikų apsaugos įstatymu, pažeidimu pripažįstama tokia veika: nešvankaus turinio vaiko fotografijos demonstravimas ar platinimas arba turėjimas demonstravimo ar platinimo tikslais[178]. Tačiau *Y. Akdeniz* nurodo, jog egzistuojančių įstatymų taikymas veikoms elektroninėje erdvėje yra problemiškas[179]. *Y. Akdeniz* taip pat nurodo ir pozityvius dalykus įstatymų leidybos procese, susijusiame su nusikaltimais elektroninėje erdvėje, ypač su veikomis platinant, skelbiant ar pan. pornografinio turinio medžiagą. Autorė nurodo, jog anksčiau buvo sunku kvalifikuoti kai kurias veikas, susijusias su pornografine medžiaga, vykdomas internete. Tačiau 1994 metais buvo pakeista „skelbimo“ sąvoka. Pakeista sąvoka taikoma ir tiems atvejams, kai asmuo A patalpina duomenis siųsti ar įkelti į standųjį diską ir suteikia slaptažodį asmeniui B tam, kad šis galėtų prieiti prie nurodytų duomenų[180]. Tokiu būdu skelbimu tapo suprantamas ir neviešas medžiagos

[174] Baibridge D. *Introduction to Computer Law*. Fourth edition. Pearson Education Limited, 2000, p. 311.
[175] Akdeniz Y., Walker C., Wall, D. *The Internet, Law and Society*. Pearson Education Limited, 2000, p. 274.
[176] Baibridge D. *Introduction to Computer Law*. Fourth edition. Pearson Education Limited, 2000, p. 297.
[177] Inter-departmental Working Group on Computer Related Crime Report. Hon Kong, September, 2000. p. 39. [interaktyvus, žiūrėta 2011-06-28]. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.
[178] Baibridge D. *Introduction to Computer Law*. Fourth edition. Pearson Education Limited, 2000, p. 335.
[179] Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet. *The Journal of Information, Law and Technology (JILT)*, 1997 (1). p. 4 [interaktyvus, žiūrėta 2011-06-27] <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1>.
[180] Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet. *The Journal of Information, Law and Technology (JILT)*, 1997 (1). p. 6 [interaktyvus, žiūrėta 2011-06-27] <http://www2.warwick.ac.uk/fac/soc/law/elj/

patalpinimas, kai medžiaga prieinama tiktai tam tikram kiekiui asmenų, gaunančių prieigos slaptažodžius ar pan.

1978 m. Vaikų apsaugos įstatymas buvo priimtas atsižvelgiant į augančią vaikų pornografinės medžiagos problemą. Įstatymas daugiausiai skirtas vaikų pornografinių fotografijų problemai. 1994 metais Viešosios tvarkos įstatymu sąvoka „fotografija" buvo pakeista ir šiuo metu ji apima fotografijas elektronine forma[181]. Paminėtina, jog minimo įstatymo 84 skyrius skirtas vadinamajai vaikų pseudofotografijų problemai. Pseudofotografijos yra kuriamos kompiuterių programine įranga, naudojant kelias fotografijas. Pavyzdžiui, vaiko veidas gali būti perkeltas ant kito apsinuoginusio kūno, tuo tarpu kai minėtas vaikas buvo fotografuojamas su drabužiais[182]. Tokiu būdu buvo pašalinta įstatymų spraga, kai baudžiamojon atsakomybėn negalėjo būti patrauktas asmuo, kuris realiai nepanaudojo vaiko pornografinio turinio medžiagai kurti, o tik programine įranga sukūrė tokią medžiagą[183].

K. Akerman taip pat kritikuoja Jungtinės Karalystės teisės aktus, nurodydamas, jog šie aktai nenustato atsakomybės pagrindų už vadinamąsias DDoS veikas[184].

3.2.7. Jungtinės Amerikos Valstijos (JAV)

Netgi nepaisant to, jog Konvencija dėl elektroninių nusikaltimų JAV įsigaliojo 2007 metais[185], literatūroje nurodoma, jog JAV – viena iš pirmaujančių valstybių veikų, susijusių su kompiuteriais, kriminalizavimo srityje. JAV taip pat buvo pirmoji valstybė, kurioje dar 1977 metais buvo pasiūlytas pirmasis federalinis įstatymas, susijęs su nusikaltimais panaudojant kompiuterius[186]. Šiuo metu JAV atsakomybę už nusikaltimus elektroninėje erdvėje nustato keletas įstatymų[187]. Literatūroje nurodoma, jog už su kompiuteriais susijusius nusikaltimus atsakomybė numatyta daugiau nei 40 skirtingų federalinių teisės aktų[188]. Vienas iš pagrindinių federalinių įstatymų – 1986 m. Sukčiavimo ir piktnaudžiavimo panaudojant kompiuterius įstatymas, taip pat ir daug

jilt/1997_1/akdeniz1>.

[181] Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet. *The Journal of Information, Law and Technology (JILT)*, 1997 (1). p. 7 [interaktyvus, žiūrėta 2011-06-27] <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1>.

[182] Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet. *The Journal of Information, Law and Technology (JILT)*, 1997 (1). p. 8 [interaktyvus, žiūrėta 2011-06-27] <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1>.

[183] Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet. *The Journal of Information, Law and Technology (JILT)*, 1997 (1). p. 9 [interaktyvus, žiūrėta 2011-06-27] <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1>.

[184] Public Hearing on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Compabint Computer-related Crime. *Charlemagne Building*, 170, rue de la Loi, Brussels 1040, 7 March 2001.

[185] Convention on Cybercrime, CETS No.:185, status as of:18/6/2011. [interaktyvus, žiūrėta 2011-06-27] <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/2011&CL=ENG>.

[186] Schjolberg S. The Legal Framework – Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries, Moss District Court, Norway. [interaktyvus, žiūrėta 2011-6-18]. <http://www.mosstingrett.no/info/legal.html>.

[187] Štitilis D., Petrauskas R. Criminal Acts in Computer Systems and Their Legal Regulation. *Databases & information systems. Proceedings of the 4th IEEE international Baltic workshop*, Vol. 2, Vilnius: Technika, 2000, p. 234.

[188] Dillon S. A., Groene D.E., Hayward T. American Criminal law Review. Georgeton university law center, 1998, Vol. 35, p. 513.

kitų įstatymų[189]. Šioje valstybėje situacija kriminalizuojant veikas, padarytas naudojant internetą, yra geresnė nei daugelyje kitų. Čia beveik visos veikos, padarytos naudojant internetą, yra baudžiamos[190], nors kai kurių trūkumų neišvengiama.

Paminėtina, jog JAV pirmieji pakeitimai, susiję su nusikaltimais, susijusiais su kompiuteriais atsirado jau 1984 metais, kai buvo priimtos normos, nustatančios baudžiamosios atsakomybės pagrindus už tam tikras veikas prieš kompiuterių sistemas. Tačiau tuo metu buvo saugoma tik siaura informacijos dalis, t.y. tik ta informacija, kuri būdavo vyriausybės ar finansų institucijų kompiuteriuose. Šie trūkumai buvo pašalinti ir šiuo metu yra manoma, jog JAV Sukčiavimo ir piktnaudžiavimo panaudojant kompiuterius įstatymas kompleksiškai saugo kompiuterių sistemų ir duomenų vientisumą, konfidencialumą ir prieinamumą, nepaisant pasikėsinimo rūšies, kompiuterio savininko ar nusikaltėlio tikslo padaryti didelę žalą[191]. Pavyzdžiui, pagal šį įstatymą yra neteisėta ir baudžiama:

- prieiga neturint tam teisės (ar viršijant nustatytas teises) prie bet kokios kompiuterių sistemos, kai dėl to pasisavinama įstatymo saugoma ar valstybinė informacija;
- prieiga neturint tam teisės (ar viršijant nustatytas teises) prie bet kokios kompiuterių sistemos, kai dėl to pasisavinama finansinė informacija, laikoma finansų institucijoje, taip pat informacija apie paskolas ar informacija, susijusi su kreditinėmis kortelėmis;
- tyčinė prieiga neturint tam teisės prie JAV departamento ar agentūros kompiuterio, jei kompiuteris skirtas išimtinai šioms institucijoms naudoti, taip pat jei kompiuteris nėra skirtas išimtinai šioms institucijoms naudoti, kai dėl to yra paveikiamas vyriausybinės institucijos naudojimasis kompiuteriu;
- slaptažodžių ar kitos informacijos, kuria pasinaudojus galima neteisėtai patekti į kompiuterį, platinimas (siekiant apgaulės), jei dėl tokio platinimo yra paveikiama užsienio komercija arba komercija tarp valstijų ar toks kompiuteris yra naudojamas JAV vyriausybės[192],[193].

Atsakomybę už tam tikras veikas, atliekant neteisėtą prieigą, taip pat nustato ir Elektroninių ryšių slaptumo įstatymas. Remiantis šiuo įstatymu, bet kas, kas neteisėtai prieina prie įrenginio, per kurį tiekiamos elektroninių ryšių paslaugos, arba viršija įgaliojimus ir tokiu būdu prieina prie įrenginio bei pasisavina ar pakeičia kompiuterinę informaciją arba apriboja prieigą prie elektroninių ryšių, yra baudžiamas už nusikaltimą[194].

---

[189] Icove D., Seger K., VonStorch W. *Computer Crime: A Crimefighters Handbook*. Oreilly&Associates, Inc., 1995, p. 16.

190 Cavazos E. A. *Cyberspace and the Law: Your Rights and Duties in the On-line World*. London: The MIT Press, 1994, p. 108.

[191] Cavazos E. A. *Cyberspace and the Law: Your Rights and Duties in the On-line World*. London: The MIT Press, 1994, p. 108.

[192] Cavazos E. A. *Cyberspace and the Law: Your Rights and Duties in the On-line World*. London: The MIT Press, 1994, p. 107.

[193] Inter-departmental Working Group on Computer Related Crime Report. Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 29. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.

[194] Perrit H. *Law and the Information Superhighway*. Wiley&Sons, Inc., 1996, p. 579.

JAV įstatymuose apibrėžtos kai kurios sąvokos, susijusios su kompiuterių panaudojimu[195]. Tačiau *E. A. Cavazos* pažymi, jog JAV įstatymuose kol kas nėra apibrėžta, kas laikoma „neteisėta prieiga“, dėl to gali kilti interpretavimo problemų, ir kai kurios veikos nepatekti į šio federalinio įstatymo veikimo sritį. Be to, kritikuojamos kai kurios įstatymuose nurodytos sąvokos. Pavyzdžiui, *H. Perritt* nurodo, jog „kompiuterio“ sąvoka, pateikiama JAV įstatymų sąvado 1030 (e)(1) paragrafe, yra per plati, nes kompiuteriu galima laikyti netgi mikrobangų krosnelę, kurioje yra procesorius[196].

Paminėtina, jog JAV įstatymuose yra kriminalizuotos ir kitos veikos elektroninėje erdvėje. Pavyzdžiui, baudžiamosios atsakomybės pagrindai nustatyti už įrenginių, skirtų atlikti neteisėtai prieigai ar perimti kompiuterinei informacijai, turėjimą ar neteisėtą prekybą. Beje, šios nuostatos apima ne visas veikas, už kurias gali būti nustatyta atsakomybė pagal Nusikaltimų elektroninėje erdvėje konvenciją. Šios konvencijos 6 straipsnyje nurodyta, jog turi būti nustatyta atsakomybė ir už kitų įrenginių bei programų (tokių kaip virusai), skirtų sunaikinti duomenims ar sutrikdyti kompiuterių sistemų darbui, siekiant įvykdyti Konvencijoje nurodytus pažeidimus, turėjimą ar nelegalią prekybą[197].

Už veikas, susijusias su vaikų pornografine medžiaga, JAV baudžiamojon atsakomybėn traukiama remiantis 1996 m. Kongreso priimtu Vaikų pornografijos prevencijos įstatymu. Šis įstatymas kriminalizuoja vaikų pornografinės medžiagos, t.y. atvaizdų, sukurtų mechaniškai ar elektroniniu būdu, gaminimą, skelbimą, platinimą ar gavimą[198]. Paminėtina, jog nuostata dėl elektroniniu būdu sukurtų atvaizdų reiškia, kad kriminalizuojamos veikos, susijusios su pseudofotografijų panaudojimu.

JAV nusikaltimu taip pat laikomas autorių teisių pažeidimas elektroninėje erdvėje, jei tokiais veiksmais siekiama finansinės naudos. Tačiau kai pažeidžiant autorių teises finansinės naudos nesiekiama, tokie veiksmai pagal JAV įstatymus kol kas negali būti įvardyti kaip nusikaltimas. Prie tokios išvados prieita ir byloje *United States v. La Macchia*. Šioje byloje kaltinamasis patalpino internete neteisėtai nukopijuotą kūrinį, dėl to interneto vartotojai šį kūrinį galėjo laisvai nukopijuoti. Tačiau teismas konstatavo, jog kaltinamasis nepadarė jokio nusikaltimo, nes savo veiksmais nesiekė finansinės naudos[199]. Tačiau veika buvo įvardyta kaip Sukčiavimo panaudojant komunikacijas akto (angl. *Wire fraud statute*) pažeidimas. Taigi veika pažeidžiant autorių teises elektroninėje erdvėje, nors ir nesant komercinių tikslų, JAV vis dėlto įvardijama, nors ne nusikaltimu, tačiau kito įstatymo pažeidimu ir užtraukia šiame įstatyme nurodytas sankcijas.

[195] Inter-departmental Working Group on Computer Related Crime Report. Hong Kong, September, 2000.[interaktyvus, žiūrėta 2011-06-28]. p. 11. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.
[196] Perrit H. *Law and the Information Superhighway*. Wiley&Sons, Inc., 1996, p. 571.
[197] Frequently Asked Questions and Answers About the Council of Europe Convention Cybercrime. December 1, 2000. [interaktyvus, žiūrėta 2011-16-18]. <http://www.cybercrime.gov/COEFAQs.htm>.
[198] Dillon S. A., Groene D. E., Hayward T. American Criminal law Review. Georgeton university law center, 1998, Vol. 35, p. 519.
[199] Perrit H. Law and the Information Superhighway.- Wiley&Sons, Inc., 1996, p. 576.

3.2.8. Kanada

Kanada buvo viena iš pirmųjų valstybių, kuri į baudžiamąjį kodeksą įvedė naujas nuostatas, susijusias su kompiuteriniais nusikaltimais. Tai įvyko 1985 metais. Šiuo metu Kanada laikoma valstybe, kurioje baudžiamieji įstatymai nustato atsakomybės pagrindus už beveik visas pavojingas veikas elektroninėje erdvėje[200]. Baudžiamąją atsakomybę už elektroninius nusikaltimus Kanada nustatė nepaisant to, kad ši valstybė taip ir neratifikavo Konvencijos dėl elektroninių nusikaltimų. Kanada šią Konvenciją pasirašė dar 2001 metais[201], tačiau vėliau įstatymų leidėjas nesiėmė jokių veiksmų, kad ratifikuotų šią konvenciją.

Remiantis „McConnell International"[202] atliktais tyrimais, Kanadoje pakeitus ir papildžius įstatymus, baudžiamoji atsakomybė buvo nustatyta už šiuos nusikaltimų tipus, įskaitant, bet neapsiribojant:

- duomenų perėmimą;
- duomenų pakeitimą;
- duomenų vagystę;
- įsikišimą į informacijos apdorojimą kompiuterių tinkle;
- sabotažą kompiuterių tinkle;
- neteisėtą prieigą;
- viruso platinimą.

Remiantis Kanados baudžiamojo kodekso 342.1 str. „Neteisėtas kompiuterio naudojimas", nusikaltimu pripažįstama tokia apgavikiška ir neteisėta veika:

- panaudojant kompiuterį tiesiogiai ar netiesiogiai gaunama bet kokia paslauga;
- tiesiogiai ar netiesiogiai perimama kompiuterių sistema;
- kompiuterių sistema naudojama turint tikslą įvykdyti kitus nurodytus nusikaltimus[203].

Pažymėtina, kad tiek 341.2 straipsnyje, tiek kituose Kanados baudžiamojo kodekso straipsniuose, susijusiuose su elektroniniais nusikaltimais, atitinkamose straipsnių dalyse pateikiamos vartojamos sąvokos. Pavyzdžiui, 341.2 straipsnyje pateikiamos tokios sąvokos: „kompiuterinis slaptažodis", „kompiuterių programa", „kompiuterinė paslauga", „kompiuterių sistema" ir kt.[204] Viena vertus, toks sąvokų įstatyme pateikimas

[200] McConnell B., Plater-Zyberk H. Canadian Cyber Crime Laws Are Among the Strongest. [interaktyvus, žiūrėta 2011-16-18]. < http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/20010102.htm>.
[201] Convention on Cybercrime. CETS No.:185, status at of:18/6/2011. [interaktyvus, žiūrėta 2011-06-28]; <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/2011&CL=ENG>.
[202] McConnell International. [interaktyvus, žiūrėta 2011-06-28]. <http://www.mcconnellinternational.com>.
[203] Criminal Code of Canada. 342.1 str. [interaktyvus, žiūrėta 2011-06-28]. <http://www.legislationline.org/documents/section/criminal-codes>.
[204] Criminal Code of Canada [interaktyvus, žiūrėta 2011-06-28]. 342.1 str. 2 d. <http://www.legislationline.org/documents/section/criminal-codes>.

palengvina atitinkamų pavojingų veikų traktavimą. Kita vertus, taip sparčiai keičiantis technologijoms, sąvokos gali pasenti ir neatitikti realijų.

Kanados baudžiamojo kodekso 342.2. straipsnyje „Įrenginio, skirto įgyti kompiuterinėms paslaugoms, laikymas“ baudžiamoji atsakomybė numatyta už bet kokio instrumento ar įrenginio (ar jo komponento), skirto vykdyti nusikaltimams, numatytiems 342.1 straipsnyje, gaminimą, laikymą, pardavimą, platinimą neturint tam teisės[205].

Taip pat paminėtinas Kanados baudžiamojo kodekso 430 str. „Žalos padarymas“, nustatantis, jog baudžiamos yra šios veikos:

- duomenų sunaikinimas ar pakeitimas;
- duomenų turinio, reikšmės pakeitimas;
- įsiterpimas į duomenų apdorojimo procesą ir pan.

Kitos Kanados baudžiamojo kodekso nuostatos, kurios gali būti taikomos pavojingoms veikoms elektroninėje erdvėje:

- 184 str. – neteisėtas privačių komunikacijų perėmimas;
- 326 str. – telekomunikacijų paslaugų vagystė;
- 327 str. – įrenginio, skirto neteisėtai naudoti telekomunikacijų įrenginius ar paslaugas, turėjimas.

2001 m. Kanadoje buvo priimti baudžiamojo kodekso pakeitimai, skirti nustatyti baudžiamajai atsakomybei už vaikų pornografinės medžiagos naudojimą. Šiuo metu Kanados baudžiamasis kodeksas yra vienintelis teisės aktas, reglamentuojantis teisinę atsakomybę už vaikų pornografinės medžiagos naudojimą. Kanados baudžiamojo kodekso 163.1 skyriuje nurodytos trys pagrindinės veikos:

- vaikų pornografinės medžiagos paskelbimas;
- vaikų pornografinės medžiagos platinimas;
- vaikų pornografinės medžiagos turėjimas[206].

163.1 (2) dalyje kriminalizuotas vaikų pornografinės medžiagos kūrimas, spausdinimas, skelbimas ar turėjimas, ketinant šią medžiagą publikuoti (skelbti)[207]. 163.1 (3) dalyje – vaikų pornografinės medžiagos importavimas ar pardavimas platinimo tikslais. Už vaikų pornografinės medžiagos turėjimą (laikymą) baudžiamoji atsakomybė nustatyta Kanados baudžiamojo kodekso 163.1 (4) dalyje. Paminėtina, jog Kanados

[205] Criminal Code of Canada [interaktyvus, žiūrėta 2011-06-28]. 342.2 str. <http://www.legislationline.org/documents/section/criminal-codes>

[206] Racicot M., et al. The Cyberspace Is Not a „No Law Land“: a Study of the Issues of Liability For Content Circulating on the Internet.[interaktyvus]. 1997 [žiūrėta 2011-06-28], ISBN 0-622-25489-9, p.60. <http://www.google.lt/url?sa=t&source=web&cd=3&ved=0CCsQFjAC&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.17.4392%26rep%3Drep1%26type%3Dpdf&ei=dkQLTrjiDsGbOrmjve0D&usg=AFQjCNFy3irmgJF9Y8PgkBBjnMIUqzlx-g&sig2=PnF4NL2fuTa4yeXdNW683w.>.

[207] Criminal Code of Canada. [interaktyvus, žiūrėta 2011-06-28]. sec. 163.1(2). <http://www.legislationline.org/documents/section/criminal-codes>.

įstatymai kriminalizuoja ir pseudofotografijų naudojimą, kai fotografijos sukuriamos programine įranga[208].

Kanados teismai yra teigę, jog medžiagos platinimas internete, t.y. naujienų grupėse, tinklalapiuose ar elektroninio pašto grupėse, prilyginamas publikavimui (paskelbimui)[209]. *A. M. Gahtan, M. P. J. Kratz* taip pat pabrėžia tą faktą, jog paprasčiausias vaikų pornografinės medžiagos turėjimas (laikymas), netgi neketinant šios medžiagos platinti, yra baudžiamas. Tai reiškia, kad interneto vartotojas, kuris lankydamasis tinklalapyje, kuriame yra vaikų pornografinė medžiaga, išsaugo tokią medžiagą savo kompiuterio standžiajame diske, gali būti apkaltintas padaręs nusikaltimą[210].

Kanados baudžiamajame kodekse yra išspręsta sąvokos „vaikų pornografinė medžiaga“ traktavimo problema, nes kodekso 163.1 (1) dalyje pateikiama „vaikų pornografinės medžiagos“ sąvoka. Kodekse taip pat pateikiamos ir kitos sąvokos, susijusios su kompiuterių panaudojimu, pvz., apibrėžiama „kompiuterių sistemos“ sąvoka[211].

3.2.9. Italija

Po Prancūzijos, Italija buvo pirmoji Europoje, į savo teisinę sistemą įvedusi normas, nustatančias baudžiamosios atsakomybės pagrindus už nusikaltimus, susijusius su kompiuteriais. Be to, Italijoje 2008 metais buvo ratifikuota ir tais pačiais metais įsigaliojo Konvencija dėl elektroninių nusikaltimų[212]. Tokiu būdu šis tarptautinis teisės aktas tapo Italijos teisinės sistemos dalimi.

Šiuo metu baudžiamosios atsakomybės pagrindai už nusikaltimus elektroninėje erdvėje nurodyti šiuose Italijos baudžiamojo kodekso straipsniuose:

- 392 str. Šio straipsnio 3 dalis buvo pakeista, siekiant nustatyti atsakomybę už veikas, kai kompiuterių programa pakeičiama ar atliekami kiti veiksmai, kai pati programa priklauso kitam asmeniui[213].
- 420 str. Atakos prieš įrangą, skirtą viešai naudoti. Šis straipsnis Italijos parlamento buvo visiškai pakeistas, siekiant apsaugoti kompiuterizuotas ar elektronines sistemas, skirtas viešai naudoti, taip pat duomenis, informaciją ir programinę įrangą, esančią tose sistemose.

[208] Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet, 1997[interaktyvus, žiūrėta 2011-06-28]. p. 9. <http://papers.ssrn.com/sol3/Delivery.cfm/lp9704291.pdf?abstractid=41684&mirid=3>.

[209] Racicot M. et al. The Cyberspace Is Not a „No Law Land“: a Study of the Issues of Liability For Content Circulating on the Internet.[interaktyvus]. 1997 [žiūrėta 2011-06-28], ISBN 0-622-25489-9, p.65. <http://www.google.lt/url?sa=t&source=web&cd=3&ved=0CCsQFjAC&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.17.4392%26rep%3Drep1%26type%3Dpdf&ei=dkQLTrjiDsGbOrmjve0D&usg=AFQjCNFy3irmgJF9Y8PgkBBjnMIUqzlx-g&sig2=PnF4NL2fuTa4yeXdNW683w.>.

[210] Gahtan A. M., Kratz M. P. J. *Internet Law: A Practical Guide to Legal and Business Professionals*. Carswell: Thomson Proffesional Publishing, 1998, p. 286.

[211] Inter-departmental Working Group on Computer Related Crime Report. Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 11. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>. .

[212] Convention of Cybercrime. CETS No.:185, Status as of: 13/06/2011. [interaktyvus, žiūrėta 2011-06-27]. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/2011&CL=ENG.

[213] Tamburrini P. *European Computer Law. Information Technology Law Group/Europe*. New York: Transnational Publishers, Inc., 1996, p. 8 (2).

- 491-1 str. Kompiuteriniai dokumentai. Šiuo straipsniu kriminalizuotas viešųjų ir privačių dokumentų elektronine forma klastojimas.
- 615 str. Neteisėta prieiga prie kompiuterizuotų ar elektroninių sistemų. Remiantis šiuo straipsniu, atsakomybė kyla tik tada, kai pavojinga veika nukreipta prieš saugumo priemonėmis apsaugotą kompiuterių ar elektroninę sistemą, o ne bet kokią kompiuterių ar elektroninę sistemą.
- 615 str. Prieigos prie kompiuterių ar elektroninės sistemos kodų neteisėtas turėjimas ar platinimas. Pažymėtina, jog būtinas požymis – naudos sau ar kitam asmeniui siekimas ar tikslas padaryti žalą kitam asmeniui.
- 615 str. Programinės įrangos, skirtos sunaikinti ar sutrikdyti kompiuterių sistemų darbui, platinimas. Šis straipsnis nustato baudžiamąją atsakomybę už virusų, taip pat vadinamųjų kirminų platinimą.
- 616 str. Korespondencijos pažeidimas. Remiantis šiuo straipsniu, „korespondencija“ reiškia korespondenciją laišku, telegrama, kompiuteriu arba kompiuterių tinklu ar kitomis priemonėmis.
- 617 str. Neteisėtas kompiuterizuotų ar elektroninių komunikacijų perėmimas, pertraukimas. Įrangos, skirtos paminėtam perėmimui, diegimas.
- 635 str. Kompiuterizuotų ar elektroninių sistemų pažeidimas. Remiantis šiuo straipsniu, baudžiamoji atsakomybė kyla už kompiuterizuotų ar elektroninių sistemų ar programinės įrangos ar duomenų, priklausančių kitam asmeniui, sunaikinimą, pažeidimą, padarymą nenaudojamais.
- 640 str. Sukčiavimas panaudojant kompiuterius. Tai yra speciali sukčiavimo rūšis, susijusi su kompiuterizuotų ar elektroninių sistemų darbo pakeitimu.

Italijos baudžiamajame kodekse taip pat yra nuostatų, susijusių su intelektinės nuosavybės apsauga bei vaikų pornografija. Pavyzdžiui, baudžiamoji atsakomybė, remiantis Italijos baudžiamojo kodekso 269 str., kyla, kai platinama, reklamuojama (įskaitant ir kompiuterių tinklus) medžiaga, susijusi su vaikų (iki 18 metų) pornografija. Paminėtina, jog yra baudžiamas ir tokios pornografinės medžiagos turėjimas.

3.2.10. Australija

Australija nėra nei ratifikavusi Konvencijos dėl elektroninių nusikaltimų, nei pasirašiusi[214]. Taigi, šis tarptautinis teisės aktas tiesiogiai neveikia Australijos teisinės sistemos. Nepaisant to, 2001 metais Australijoje buvo priimtas Elektroninių nusikaltimų įstatymas Nr. 161[215], kuris pakeitė teisės aktus, reglamentuojančius pažeidimus panaudojant kompiuterį.

[214] Convention of Cybercrime. CETS No.:185, Status as of: 18/06/2011. [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/2011&CL=ENG>.
[215] Cybercrime Act No. 161, 2001 . [interaktyvus, žiūrėta 2011-06-28]. <http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112/sch1.html>.

Šiame įstatyme apibrėžta daugelis sąvokų, susijusių su nusikaltimais elektroninėje erdvėje, pavyzdžiui, „prieiga prie duomenų, laikomų kompiuteryje“, „duomenys“, „duomenys, laikomi kompiuteryje“, „duomenų saugojimo įrenginys“, „modifikavimas“, „neteisėta prieiga“ ir kt.

Pažeidimai panaudojant kompiuterį Elektroninių nusikaltimų įstatyme suskirstyti į dvi grupes, tai:

- sunkūs pažeidimai panaudojant kompiuterį (neteisėta prieiga, neteisėtas modifikavimas bei neteisėtas kenkimas elektroniniams ryšiams);
- kiti pažeidimai panaudojant kompiuterį (prieiga prie saugomų duomenų, jų modifikavimas; neteisėtas kenkimas kompiuteryje esantiems duomenims; duomenų turėjimas ar kontroliavimas, ketinant įvykdyti pažeidimą panaudojant kompiuterį; duomenų, siekiant įvykdyti nusikaltimą panaudojant kompiuterį, gaminimas, teikimas ar gavimas).

Elektroninių nusikaltimų įstatymo 477.1 str. nustatyti baudžiamosios atsakomybės pagrindai už neteisėtą prieigą, modifikavimą ar kenkimą, jei tokiais veiksmais ketinama vykdyti kitą sunkų nusikaltimą[216]. Atsakomybės pagrindai už neteisėtą prieigą nustatyti ir skyriuje „Kiti pažeidimai panaudojant kompiuterį“. Šio įstatymo 478.1 str. nurodyta, jog baudžiamąją atsakomybę užtraukia neteisėta prieiga prie saugomų duomenų arba tokių duomenų modifikavimas[217].

Kiti Australijos Elektroninių nusikaltimų įstatymo straipsniai, kuriuose numatyta baudžiamoji atsakomybė už elektroninius nusikaltimus:

- 477.2 straipsnis „Neteisėtas duomenų modifikavimas“;
- 477.3 straipsnis „Neteisėtas elektroninių komunikacijų pabloginimas“ (angl. *Impairment*);
- 478.2 straipsnis „Neteisėtas kompiuteryje laikomų duomenų pabloginimas“;
- 478.3 straipsnis „Duomenų laikymas ar kontroliaivmas turint tikslą įvykdyti kompiuterinį pažeidimą“;
- 478.4 straipsnis „Duomenų gavimas, gaminimas ar teikimas turint tikslą įvykdyti kompiuterinį pažeidimą“[218].

[216] Cybercrime Act No. 161, 2001 . art. 477.1. [interaktyvus, žiūrėta 2011-06-27]. <http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112/sch1.html >.
[217] Cybercrime Act No. 161, 2001 . art. 478.1.
[interaktyvus, žiūrėta 2011-06-27]. <http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112/sch1.html >.
[218] Cybercrime Act No. 161, 2001. [interaktyvus, žiūrėta 2011-06-28]. <http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112/sch1.html>.

3.2.11. Honkongas

Honkongo nėra sąraše tarp valstybių, pasirašiusių ar ratifikavusių Konvenciją dėl elektroninių nusikaltimų[219]. Nepaisant to, pagrindinės veikos, susijusios su nusikaltimais elektroninėje erdvėje, buvo kriminalizuotos 1993 metais, priėmus Dekretą dėl kompiuterinių nusikaltimų, kuris pakeitė Telekomunikacijų dekretą, Nusikaltimų dekretą bei Vagystės dekretą, dėl to buvo įvesta keletas naujų nusikaltimų bei papildyta kai kurių tradicinių nusikaltimų sudėčių veikimo sritis[220].

Dėl 1993 metų įstatymų pakeitimų bei papildymų (pvz., žala, padaroma nuosavybei) apimama ir žala duomenims elektronine forma (juos pakeičiant, ištrinant ar įvedant). Tačiau literatūroje kaip trūkumas minimas faktas, kad pagal Honkongo įstatymus duomenų elektronine forma vagystė nelaikoma nusikaltimu[221]. Tačiau siekiant kriminalizuoti veiką, pagrobiant kompiuterinę informaciją, tikslingiau ją išskirti į atskirą straipsnį, nes skirtingai nei tradicinės vagystės metu, kompiuterinė informacija gali būti tiktai nukopijuojama ir likti pas seną savininką, kai tuo tarpu tradicinės vagystės metu turto pasisavinimas suprantamas kitaip.

Literatūroje kritikuojamos įstatymo nuostatos, susijusios su baudžiamosios atsakomybės nustatymu už neteisėtą prieigą. Yra teigiama, jog turint omenyje didžiulę žalą, kurią gali sukelti neteisėta prieiga, įstatymo leidėjų nustatyta bausmė – 20 000 JAV dolerių bauda – yra neadekvati veikos pavojingumui, ir dėl to turi būti nustatyta laisvės atėmimo bausmė[222].

Honkongo įstatymai taip pat kritikuojami dėl to, kad nėra nustatytos sąvokos „kompiuteris“ ir „kompiuterių sistema“, tokiu būdu paliekant teisę šias sąvokas interpretuoti teismams. Literatūroje diskutuojama, jog, viena vertus, kompiuterio sąvokos apibrėžimas įstatymuose gali lemti situaciją, kad sąvoka bus per plati arba ją reikės dažnai keisti. Kita vertus, paliekant kompiuterio sąvoką laisvai interpretuoti, galima sulaukti labai skirtingų teismų sprendimų[223]. Kadangi kompiuteris dažniausiai reiškia vienintelę skaičiavimo mašiną, prie kurios prijungtas monitorius, kai tuo tarpu vystantis internetui informacija apdorojama ne tik tradiciniame kompiuteryje, literatūroje siūloma Honkonge vartoti sąvoką „informacinė sistema“, kuri geriau nurodytų technologijų pokyčius ir apimtų naujus įrenginius bei technologijas. Ši sąvoka jau yra apibrėžta Elektroninių sandorių dekrete. Todėl siūloma kituose įstatymuose, nustatančiuose baudžiamosios atsakomybės pagrindus už veikas elektroninėje erdvėje ir vartojančiuose sąvoką „kompiuteris“, vartoti terminą „informacinė sistema“[224]. Be to,

[219] Convention of Cybercrime. CETS No.:185, Status as of: 18/06/2011. [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/2011&CL=ENG>.

[220] Inter-departmental Working Group on Computer Related Crime Report // Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 5. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.

[221] Inter-departmental Working Group on Computer Related Crime Report // Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 29. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.

[222] Inter-departmental Working Group on Computer Related Crime Report // Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 9. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.

[223] Inter-departmental Working Group on Computer Related Crime Report // Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 12. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.

[224] Inter-departmental Working Group on Computer Related Crime Report. Hon Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 13. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.

problemų gali sukelti sąvokos „prieiga prie informacinės sistemos“ nebuvimas, todėl ją taip pat pageidautina nurodyti teisės aktuose.

Viena iš kritinių nuomonių – kol kas nėra baudžiamosios atsakomybės už neteisėtą informacijos perėmimą. Dėl šios priežasties baudžiamuosiuose įstatymuose siūloma nuostatas „duomenys, esantys kompiuteryje“ papildyti nuostatomis „įskaitant duomenis, siunčiamus kompiuteriu ar internetu“[225]. Tokiu būdu, beje, būtų išvengta saugomos informacijos vardijimo, pvz., informacija apie kreditinių kortelių numerius. Be to, turėtų būti kriminalizuojamas ir žinomos neteisėtos prieigos metu gautos informacijos elektronine forma pasisavinimas, išsaugojimas arba prekiavimas tokia informacija. Tokiomis nuostatomis būtų pašalintas įstatymų trūkumas, kai trečioji šalis gali nupirkti „pavogtą“ informaciją elektronine forma, nepadarydama jokio pažeidimo[226]. Taip pat yra manoma, jog esamų įstatymų nepakanka kvalifikuoti veiką elektroninėje erdvėje kaip sukčiavimo, nes galiojantys įstatymai reikalauja tam tikro asmens apgavimo, ko nebūna vykdant sukčiavimo veiką elektroninėje erdvėje.

Literatūroje taip pat pažymima, jog Honkonge nusikaltimu turėtų būti pripažįstamas ir bet kokio kompiuterių slaptažodžio ar prieigos kodo neteisėtiems tikslams pardavimas, platinimas ar padarymas prieinamais[227].

Paminėtina, kad nagrinėjant užsienio valstybių praktiką, nebuvo analizuoti tapatybės vagystės elektroninėje erdvėje kriminalizavimo aspektai. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas bus analizuojamas kituose leidiniuose. Plačiau apie šią pavojingą veiką supažindinama kito skyrelio pabaigoje.

3.3. Elektroninių nusikaltimų reglamentavimas Lietuvoje

Lietuvoje ši sritis gali būti reguliuojama reglamentuojant elektroninės informacijos saugos santykius. Kol kas šie santykiai reglamentuojami framgmentiškai (pvz., pavienės nuostatos Asmens duomenų teisinės apsaugos ar Elektroninių ryšių įstatymuose, negaliojanti elektroninės informacijos saugos strategija, nors tai yra vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų[228]). Holistinio elektroninės informacijos saugos teisinio reguliavimo apraiška galima vadinti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektą[229]. Minimas įstatymas turėjo reglamentuoti visuomeninius santykius, susijusius su elektroninių ryšių tinklų ir informacijos saugumu, nustatant bendruosius reikalavimus elektroninių

[225] Inter-departmental Working Group on Computer Related Crime Report // Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 33. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.
[226] Inter-departmental Working Group on Computer Related Crime Report // Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 34. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.
[227] Inter-departmental Working Group on Computer Related Crime Report // Hong Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. p. 34. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.
[228] Štitilis D., Paškauskas Ž. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija*, 2007, Nr. 2(92), p. 37.
[229] Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektas Nr.373-02, 2009-09-21[interaktyvus, žiūrėta 2011-06-28].
<http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=5050&p_query=&p_tr2=&p_org=&p_fix=n&p_gov=n>

ryšių tinklų ir informacijos saugumui užtikrinti, taip pat visuomeninius santykius, susijusius su valstybės ir savivaldybės institucijų ir įstaigų bei kritinių informacinių infrastruktūrų elektroninių ryšių tinklų ir informacijos saugumu, elektroninių ryšių tinklų ir informacijos saugumo auditu bei programinės įrangos saugumo vertinimu. Tačiau šis projektas nebuvo priimtas.

Vienas iš pagrindinių nacionalinių valstybių įstatymų leidėjų uždavinių kovojant su elektroniniais nusikaltimais – uždrausti šias pavojingas veikas nacionaliniuose baudžiamuosiuose kodeksuose. Todėl ši teisinio reguliavimo sritis aptariama toliau šiame mokomajame leidinyje.

Lietuvos Respublikos prisijungimas prie Konvencijos dėl elektroninių nusikaltimų gerokai paveikė Lietuvos nacionalinę baudžiamąją teisę. Nors dar iki Konvencijos pasirašymo priimtame naujajame Lietuvos Respublikos baudžiamajame kodekse jau buvo įvestas naujas skirsnis „Nusikaltimai informatikai“[230], kuriame nustatyta atsakomybė už nusikaltimus, keliančius grėsmę saugiam kompiuterinės informacijos apdorojimui, svarbūs Lietuvos Respublikos baudžiamojo kodekso papildymai buvo atlikti 2004 m. pradžioje. Įgyvendinant Konvenciją, nuo 2004 m. vasario 14 d. įsigaliojo nauji Lietuvos Respublikos baudžiamojo kodekso papildymai, kuriais į minėtą skirsnį įvestos dvi naujos veikos: neteisėtas prisijungimas prie kompiuterio ar kompiuterių tinklo (198-1 str.) bei neteisėtas disponavimas įrenginiais, kompiuterių programomis, slaptažodžiais, prisijungimo kodais ir kitais duomenimis, skirtais nusikaltimams daryti (198-2 str.). Buvo papildyti ir kiti „tradiciniai“ straipsniai, pvz., 309 str., nustatantis atsakomybę už disponavimą pornografinio turinio dalykais. Lietuvos Respublikos baudžiamojo kodekso ištrauka pateikiama priede Nr. 3.

Atsakomybė už pavojingas veikas, pažeidžiančias kompiuterinės informacijos ir kompiuterių sistemų konfidencialumą,vientisumą bei prieinamumą.

Baudžiamoji atsakomybė už neteisėtą prieigą (su tam tikromis realiomis pasekmėmis (žala)) gali kilti pagal kelis Lietuvos Respublikos baudžiamojo kodekso straipsnius. Tik įsigaliojus naujajam baudžiamaja kodeksui, nustatydamas baudžiamąją atsakomybę už neteisėtą prieigą, Lietuvos įstatymo leidėjas buvo pasirinkęs tokį veikos elektroninėje erdvėje kriminalizavimo kelią – reikalaujama realios žalos, t.y. kompiuterinės informacijos sunaikinimo, pakeitimo ar sugadinimo (Lietuvos Respublikos baudžiamojo kodekso 296 str.), kompiuterių programos sunaikinimo, pakeitimo ar sugadinimo (Lietuvos Respublikos baudžiamojo kodekso 197 str.) arba kompiuterinės informacijos pasisavinimo (Lietuvos Respublikos baudžiamojo kodekso 198 str.).

Tačiau kėsinantis į įstatymo saugomus teisinius gėrius, gali būti ne tik daroma reali žala, bet taip pat ir kilti tos žalos grėsmė. Tais atvejais, kai reali žala neatsiranda, o yra tiktai tokios žalos grėsmė, objekte irgi vyksta tam tikri pakeitimai. Pavojingumo pobūdį paprastai apibūdina kėsinimosi objekto vertingumas. Nusikaltimo objekto, į

[230] Iki 2004 m. vasario mėn. šį skirsnį sudarė trys straipsniai, numatantys baudžiamąją atsakomybę už kompiuterinės informacijos sunaikinimą ar pakeitimą (196 str.), kompiuterių programos sunaikinimą ar pakeitimą ir kompiuterių tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymą (197 str.) bei kompiuterinės informacijos pasisavinimą ar skleidimą (198 str.).

kurį kėsinamasi atliekant neteisėtą prieigą – visuomeninių santykių saugant, apdorojant kompiuterinę informaciją vertingumą yra pabrėžę *U. Sieber, D. Baibridge* ir kiti. Šio objekto apsaugos baudžiamosiomis normomis praktika (kai nepadaroma reali žala) nustatytoma vis daugiau valstybių. Be to, kriminalizuoti neteisėtą prieigą, kai nepadaroma reali žala, rekomenduojama ir tarptautiniuose norminiuose aktuose. Dėl to 2004 m. sausio 29 d. įstatymu Nr. IX-1992 Lietuvos Respublikos baudžiamasis kodeksas buvo papildytas nauju 198-1 straipsniu „Neteisėtas prisijungimas prie kompiuterio ar kompiuterių tinklo“.

Lietuva baudžiamosios teisės normomis saugo formalią kompiuterinės informacijos ir kompiuterių programų integralumo sritį, nustatydama atsakomybę Lietuvos Respublikos baudžiamojo kodekso 196 bei 197 straipsniuose. Šioms veikoms įvykdyti gali būti panaudojamos tokios kenkimo programos kaip Trojos arkliai, virusai, kirminai ir kt. Beje, 2004 metais papildžius Lietuvos Respublikos baudžiamojo kodekso 196 str., buvo kriminalizuotos ir vadinamosios DoS atakos.

Lietuvos Respublikos baudžiamojo kodekso 197 straipsnyje taip pat nustatyti baudžiamosios atsakomybės pagrindai už vadinamąsias sabotažo panaudojant kompiuterį veikas. Kompiuterių tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas ar pakeitimas siejamas su kompiuteryje esančios programos sunaikinimu, sugadinimu, pakeitimu ar tokios programos įdiegimu į kompiuterį arba kompiuterių tinklą.

Baudžiamajai atsakomybei kilti pagal Lietuvos Respublikos baudžiamojo kodekso 196 bei 197 straipsnių pirmąsias dalis įstatymo leidėjas reikalauja didelės žalos padarymo.

Baudžiamasis kodeksas saugo ir elektroninių ryšių privatumą – pavojingos veikos šioje srityje kriminalizuotos 166 str. „Neteisėtas susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimas“. Šio straipsnio, garantuojančio laisvą, normalų žmonių socialinį bendravimą, 1 d. nurodyta, jog baudžiamas yra „*tas, kas neteisėtai pažeidė asmens susirašinėjimo ar kitokiu paštu ar techninėmis priemonėmis siunčiamų pranešimų, siuntų slaptumą arba klausėsi pokalbių telefonu, arba naudojo kitas jų perėmimo formas*“. Informacijos perėmimą elektroninėje erdvėje galima laikyti „kita perėmimo forma“, todėl galima preziumuoti, jog ši nuostata taikoma apsikeitimams informacija elektroniniu paštu bei kitiems būdams.

Pavojingos yra veikos, kai tyčia atliekami tam tikri neteisėti veiksmai, susiję su įrenginiais ar prieigos duomenimis, turint tikslą įvykdyti kitus kompiuterinius nusikaltimus, buvo kriminalizuotos 2004 m. sausio 29 d., papildžius Lietuvos Respublikos baudžiamąjį kodeksą 198-2 straipsniu „Neteisėtas disponavimas įrenginiais, kompiuterių programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti“. Tai yra veikos, kai kuriami, platinami, panaudojami ir t.t. neteisėti įrenginiai/prieigos duomenys (slaptažodžių nulaužimo programos, neteisėtu būdu gauti slaptažodžiai ar pan.), skirti kompiuterių sistemų ar duomenų konfidencialumo, integruotumo ir prieinamumo pažeidimams įvykdyti.

Atsakomybės pagrindai, susiję su neteisėtu turiniu elektroninėje erdvėje.

Įstatymo leidėjas yra pasirinkęs veikų, susijusių su vaikų pornografijos platinimu internetu, kriminalizavimo tradiciniais straipsniais variantą. Naujojo Lietuvos Respublikos baudžiamojo kodekso 309 str. nustato baudžiamosios atsakomybės pagrindus už vaikų pornografijos viešą demonstravimą. Beje, šiuo straipsniu kriminalizuotos ir veikos, įvykdytos platinant vadinamąsias „pseudofotografijas", kuriose tam tikras asmuo pateikiamas kaip vaikas.

Atsakomybės pagrindai už veikas, susijusias su kompiuteriais.

Lietuvos įstatymo leidėjas Lietuvos Respublikos baudžiamajame kodekse sukčiavimo ir klastojimo veikas, vykdomas pasinaudojant elektronine erdve, kriminalizuoja tradicinėmis teisės normomis. Baudžiamoji atsakomybė už sukčiavimą nurodyta Lietuvos Respublikos baudžiamojo kodekso 182 str. Šio straipsnio 1 dalyje nurodoma, jog baudžiamojon atsakomybėn traukiamas tas, kas apgaule savo ar kitų naudai įgijo svetimą turtą ar turtinę teisę, išvengė turtinės prievolės ar ją panaikino.

Lietuvos Respublikos baudžiamajame kodekse baudžiamoji atsakomybė už klastojimą nurodyta XLIII skyriuje „Nusikaltimai ir baudžiamieji nusižengimai valdymo tvarkai, susiję su dokumentų ar matavimo prietaisų klastojimu". Baudžiamoji atsakomybė už dokumento klastojimą nustatyta Lietuvos Respublikos baudžiamojo kodekso 300 straipsnyje, kur nurodoma, jog baudžiamojon atsakomybėn traukiamas tas, kas pagamino netikrą dokumentą, suklastojo tikrą dokumentą arba netikrą ar suklastotą dokumentą panaudojo ar realizavo.

Atsakomybė, susijusi su autorių teisių bei gretutinių teisių pažeidimais.

Autorių teisių bei gretutinių teisių pažeidimo elektroninėje erdvėje veikas galima kvalifikuoti pagal Lietuvos Respublikos baudžiamojo kodekso XXIX skyriaus Nusikaltimai intelektinei ir pramoninei nuosavybei straipsnius. Šiame skyriuje nusikaltimais įvardytas autorystės pasisavinimas (191 str.); literatūros, mokslo, meno ar kitokio kūrinio neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas (192 str.); informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas (193 str.) bei neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas (194 str.). Lietuvos Respublikos baudžiamojo kodekso 192 str. nurodyta, jog baudžiamojon atsakomybėn traukiamas tas, kas neteisėtai atgamino literatūros, mokslo, meno ar kitokį kūrinį ar jo dalį arba importavo, eksportavo, platino, gabeno ar laikė komercijos tikslais neteisėtas jų kopijas, jeigu bendra kopijų vertė pagal teisėtų kopijų mažmenines kainas viršijo 100 MGL dydžio sumą.

Taip pat paminėtina tapatybės vagystės elektroninėje erdvėje problema. Asmens tapatybės vagystė elektroninėje erdvėje yra santykinai naujas socialinis-teisinis reiškinys, susijęs su vartotojų teisių, informacijos saugumo, privatumo, taisyklių, reglamentuojančių nepageidaujamos informacijos gavimą, ir kitais pažeidimais[231].

[231] Štitilis D. et al. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. *Socialinių mokslų studijos*, 2011, Nr. 3(1), p. 155.

Globalus elektroninės erdvės pobūdis ir specifinės jos savybės leidžia teisės pažeidėjams veikti gana saugioje aplinkoje, nukreipti savo veiksmus bet kuria linkme ir veikti bet kurioje vietoje, veikas atlikti labai plačiu mastu, visiškai nepaisant valstybių sienų ir jurisdikcijos. Todėl ir tapatybės vagystė elektroninėje erdvėje yra globali problema. Mokslinėje literatūroje nurodoma, jog tapatybės vagystės elektroninėje erdvėje pasekmės gali apimti daugelį visuomenės aspektų – nuo ekonomikos iki nacionalinio saugumo[232].

Pastaruoju metu pasauliniu mastu vyksta diskusijos, ar ši pavojinga veika turėtų būti kriminalizuota ir ar tokios veikos sudėties įtraukimas į valstybių baudžiamuosius įstatymus padėtų efektyviau kovoti su šiuo reiškiniu. Išsiskiria dvi konfrontuojančios pozicijos: vieni teigia, jog tapatybės vagystė turėtų būti kvalifikuojama kaip atskira, savo sudėtį turinti nusikalstama veika[233], t. y. siūlo šią veiką kriminalizuoti, argumentuodami, jog tais atvejais, kai užsienio valstybė neturi įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje kaip atskirą veiką, varžomos informaciją renkančios valstybės galimybės rinkti tapatybės vagystės elektroninėje erdvėje įrodymus atitinkamoje užsienio valstybėje. Teisėsaugos institucijoms tokiu atveju nėra suteikiama pakankamai įgaliojimų veiksmingai kovoti su tokio pobūdžio veikomis, apsunkinamas tokių veikų susekimas, tyrimas ir baudžiamasis persekiojimas nacionaliniu bei tarptautiniu lygiu. Tinkamai neįvertinus tapatybės vagystės, pasyviai laukiama kitų, dažnai sudėtingai ištiriamų tarptautinių nusikaltimų pasekmių ir tik tuomet pradedamos tirti kriminalizuotos veikos. Šios pozicijos oponentai tapatybės vagystę traktuoja kaip priemonę teisės pažeidimams ir (ar) nusikalstamoms veikoms atlikti ir teigia, jog ši veika patenka į jau kriminalizuotas veikas reglamentuojančių straipsnių veikimo sritį, todėl tapatybės vagystės elektroninėje erdvėje kriminalizuoti kaip savarankiškos veikos nebūtina.

Atkreiptinas dėmesys, kad Lietuvoje kol kas tapatybės vagystė elektroninėje erdvėje nėra kriminalizuota kaip savarankiškas nusikaltimas. Tačiau šios savarankiškos pavojingos veikos kriminalizavimas, kaip rodo kai kurių tarptautinių organizacijų ir užsienio valstybių praktika, yra netolimų diskusijų objektas.

4. ELEKTRONINIŲ NUSIKALTIMŲ PREVENCIJA

Plačiąja prasme, nusikaltimų prevencija – visa tai, kas padeda palaikyti teisėtvarką. Nusikaltimų prevenciją traktuojant plačiąja prasme, šį veika išskaidoma į daugelį socialinių procesų, todėl negalima išskirti jos specifinių bruožų. Kiti autoriai traktuoja prevenciją siaurąja prasme. Tokio požiūrio pagrindas – ryškus kryptingumas, kai

[232] Hoffman Sandra K. *Identity Theft: A Reference Handbook*. – *Santa Barbara, California*, 2010, p. 1.
[233] Štitilis D, Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai.* 2009, 50: 244–245.

prevencinėmis priemonėmis pripažįstamos tik tos priemonės, kurios užkerta kelią nusikaltimams[234]. Šiame mokomajame leidinyje prevencija bus traktuojama siauraja ir kai kuriais atvejais – plačiąja prasme.

Pagrindinis nusikaltimų prevencijos tikslas – saugoti tokias svarbias socialines vertybes, kaip valstybės, visuomenės ir piliečių interesai[235]. Elektroninių nusikaltimų atveju saugomos vertybės gali būti identifikuojamos pagal atitinkamus Lietuvos Respublikos baudžiamojo kodekso skyrius ir jų saugomas vertybes. Pavyzdžiui, XXX skyrius Saugomos vertybės apibendrintai gali būti įvardijamas kaip teisė į elektroninės informacijos ir elektroninių duomenų saugumą.

Nepaisant to, kad prevencijos priemonės įvairios, galima skirti dvi jų rūšis:

1) Bendroji nusikaltimų prevencija, kurios tikslas išaiškinti ir pašalinti nusikaltimų priežastis bei sąlygas. Tokia prevencija neturi konkretaus adresato.
2) Individualioji nusikaltimų prevencija, kurios tikslas – paveikti asmenis, linkusius daryti nusikaltimus[236].

Šiame mokomajame leidinyje daugiausia dėmesio bus kreipiama bendrajai elektroninių nusikaltimų prevencijai.

4.1. Elektroninių nusikaltimų tikimybė

Bendrąją elektroninių nusikaltimų prevenciją įmonėje ar organizacijoje galima būtų įvardyti kaip rizikos kompiuterių sistemoms nustatymą ir įvairių saugumo priemonių, kurios padės apsaugoti šias sistemas, įgyvendinimą.

Istoriškai kompiuterių sistemų apsaugos priemonės daugiau nukreiptos į informaciją, susijusią su nacionaliniu saugumu. Šiuo metu daug dėmesio skiriama informacijai ir duomenims, esantiems individualiose kompiuterių sistemose, taip pat organizacijų, finansinių, mokslinių ir kitų institucijų kompiuterių sistemose, apsaugoti.

Mažai organizacijų gali sau leisti išvystyti apsaugą, kuri apsaugotų jų kompiuterių sistemas nuo bet kokios rizikos (jei tokia apsauga iš viso yra galima). Tai daug kainuoja. Dažnai sulyginama apsaugos kaina su rizika. Saugumo lygis, su kuriuo organizacija sutinka, vadinamas prieinama rizika.

Elektroninių nusikaltimų prevencijos įgyvendinimas betarpiškai susijęs su rizikos analize. Trys žodžiai kartojasi kiekvienoje rizikos analizėje:

- grėsmės;
- pažeidžiamumai;
- kontrapriemonės.

[234] Bluvšteinas J., Bieliūnas E., Justickis V. ir kiti. *Kriminologija*. V.: Pradai, 1994, p. 152.
[235] Bluvšteinas J., Bieliūnas E., Justickis V. ir kiti. *Kriminologija*. V.: Pradai, 1994, p. 153.
[236] Bluvšteinas J., Bieliūnas E., Justickis V. ir kiti. *Kriminologija*. V.: Pradai, 1994, p. 153.

Grėsmė – tai galimas pavojus kompiuterių sistemai. Pavojus gali būti žmogus (vagis, profesionalus nusikaltėlis, hakeris), įvykis (gaisras, žaibas) ir kt., kas gali pakenkti kompiuterių sistemai. Pažeidžiamumas – vieta, kur kompiuterių sistema yra jautri pažeidimui. Grėsmė pasireiškia konkrečioje veikoje, kuri išnaudoja sistemos pažeidžiamumą. Kontrapriemonės – priemonės kompiuterių sistemos apsaugojimui: slaptažodžiai, durų užraktai.

Taigi rizikos analizė yra procesas, kurio metu atsakoma į klausimus: pirma, apie grėsmes, antra, apie pažeidžiamumą, ir, galiausiai, apie kontrapriemones, kurias panaudojus galima užkirsti kelią pavojui[237].

Į rizikos analizę taip pat įeina ir įvertinimas, kaip gerai organizacija pasiruošusi blogiausiam variantui, kartais vadinamas atsitiktinumų planavimu arba krizės vadovavimu.

Yra du rizikos analizės tipai:

- išankstinis įvertinimas – vykdomas prieš tai, kai dar neįvyko incidentas;
- pavėluotas įvertinimas – vykdomas jau po incidento.

Kompiuterių sistemos pažeidžiamos vietos ir grėsmės, kurios gali išnaudoti šias pažeidžiamas vietas, gali būti skirstomos į statines ir dinamines. Kai vykdoma rizikos analizė, ji bėgant laikui ir keičiantis sąlygoms turi keistis, nesvarbu ar organizacijos viduje, ar išorėje.

Besikeičiant aplinkai, reikia būti budriems. Patartina keisti rizikos analizę, jei atsitinka tokie įvykiai:

1. organizacijoje yra didelis personalo tekamumas. Reikia įvesti papildomus kvalifikacijos patikrinimus (jei tokių nėra), priimant naujus darbuotojus;
2. organizacija pradėjo valdyti, tvarkyti naują, svarbią informaciją;
3. organizacija susijungia su kita organizacija;
4. organizacijoje įvykdomas naujas elektroninis nusikaltimas;
5. organizacija tapo teroristų ar kitokių kovotojų taikiniu;
6. organizacijos kompiuterių techninėje ar programinėje įrangoje aptinkama pažeidžiama vieta ar virusas;
7. įvyksta tam tikri politiniai įvykiai, kurie turi įtakos organizacijai.

Vykdant rizikos analizę egzistuoja tam tikra tvarka. Tipinė rizikos analizė dalinama į penkis specifinius punktus:

1. klausimų uždavimas;
2. „žvalgybos pranešimų“ naudojimas;
3. pažeidžiamų vietų analizės vedimas;

[237] Icove D. *Computer crime: A Crimefighter`s Handbook*. O`Reylly Associates, Inc., 1995; p. 91

4. saugumo kontrapriemonių vystymas;
5. duomenų dokumentavimas ir sprendimai[238].

1. Kiekviena rizikos analizė prasideda nuo klausimų uždavimo. Pavyzdžiui, kas kėsinsis į šią kompiuterių sistemą? Kokia technika bus naudojamasi atakuojant kompiuterių sistemą? Ką bus stengiamasi pavogti ar sunaikinti?
2. Tai tam tikros išorinės informacijos naudojimas. Pavyzdžiui, sužinoma, kad konkurentai ieško hakerių, kurie įsiveržtų į kompiuterių sistemą ir t.t.
3. Kitas rizikos analizės laiptelis irgi yra labai specifinis. Nustačius grėsmes, kurias galima numatyti, sprendžiama, kur yra tam tikros pažeidžiamos vietos kompiuterių sistemoje. Netgi jei grėsmės gali pasirodyti mažesnės, reikia nustatyti visas galimas pažeidžiamas vietas, nes mažos grėsmės gali tapti didelėmis. Tikslas yra papunkčiui jas išvardyti. Jei išanalizuotos visos galimos pažeidžiamos vietos, yra daugiau šansų, kad kompiuterių sistemos bus apsaugotos nuo nenumatytų atvejų.
4. Dabar, kai yra žinomos kompiuterių sistemos pažeidžiamos vietos ir grėsmės, kurios gali jas išnaudoti, reikia vystyti saugumo kontrapriemones.Organizacija turi įvertinti, kiek rimtos yra grėsmės kompiuterių sistemai, kiek pažeidžiama gali būti sistema, kokie ištekliai realiai yra. Laipsnis, kuriuo stengiamasi užlopyti kompiuterių sistemos trūkumus, priklauso nuo trūkumų ir lėšų dydžio. Kartais rizikos analizėje galima išgirsti terminą „grėsmės laipsnis“ (lygis). Jei grėsmės lygis yra minimalus, išlaidos irgi greičiausiai bus minimalios. Jei grėsmės lygis yra aukštas, išlaidos bus daug didesnės.
5. Duomenų ir sprendimų dokumentavimas. Gera idėja duomenis ir sprendimus užrašyti. Pakanka ir atskiros suvestinės, parodančios esamas grėsmes kompiuterių sistemai, galimas pažeidžiamas vietas ir apsaugos kontrapriemones, kurios sumažintų riziką iki priimtino lygio.

Į rizikos analizę įeina pažeidžiamų vietų ir atsakomųjų priemonių nustatymas. Yra daug skirtingų pažeidžiamų vietų, nuo personalo problemų iki aparatinės ir programinės įrangos problemų. Kiekvienai reikia sukurti atitinkamas kontrapriemones. Bet pirmiausiai reikia jas visas nustatyti. Knygoje „Computer crime“ pateikiama lentelė, kurioje nurodyta daug pažeidžiamų vietų ir atsakomųjų priemonių. Pavyzdžiui, pažeidžiama vieta yra neautorizuota prieiga prie programų, o atsakomosios priemonės – vartotojo identifikacija, stebėjimas filmavimo kamerų pagalba ir kt.

4.2. Elektroninių nusikaltimų prevencijos priemonės

Atsakomosios arba saugumo, prevencinės priemonės yra kelių rūšių: „International review of criminal police“ šias priemones skirsto į 6 grupes (organizacijoje):

1. administracinis ir organizacinis saugumas;

[238] Icove D. *Computer crime: A Crimefighter`s Handbook*. O`Reylly Associates, Inc., 1995; p. 92

2. personalo saugumas;
3. fizinė apsauga;
4. komunikacijų-elektroninis saugumas (ryšių apsauga);
5. programinės įrangos saugumas;
6. procesų saugumas („Operacijų saugumas“)[239].

Remiantis duomenimis, analizuojant specialią literatūrą dėl klausimų, susijusių su elektroninių nusikaltimų teoriniais ir praktiniais aspektais, galima išskirti dvi pagrindines elektroninių nusikaltimų prevencijos priemones:

1. teisines;
2. organizacines-technines.

Teisinės elektroninių nusikaltimų prevencijos priemonės

Prie teisinių apsaugos priemonių reikia priskirti visus teisės normų aktus, taip pat vidines organizacijų taisykles, reglamentuojančias saugų kompiuterinės informacijos naudojimą ir platinimą bei saugų kompiuterių tinklų naudojimą ir kt.[240]

Tuo tarpu baudžiamųjų įstatymų normos dėl elektroninių nusikaltimų nustato svarbiausias socialines vertybes, kurių užtikrinimas ir yra elektroninių nusikaltimų prevencijos egzistavimo esmė. Kitaip tariant, baudžiamieji įstatymai nereguliuoja visuomeninių santykių elektroninių nusikaltimų prevencijos sferoje, bet nustato tos sferos ribas, atriboja nuo kitų socialinio valdymo sferų.

Organizacinės-techninės elektroninių nusikaltimų prevencijos priemonės

Šios priemonės skirstomos į tris grupes:

1. organizacines;
2. technines;
3. kompleksines[241].

1. Organizacinės priemonės

Į organizacines kompiuterių technikos apsaugos priemones įeina veiksmai parenkant, tikrinant ir instruktuojant personalą, vystant informacinių objektų atkūrimo planą išėjimo iš rikiuotės atveju, organizuojant programinį-techninį kompiuterio technikos priemonių aptarnavimą, nustatant atsakomybę asmenims, dirbantiems su kompiuterių technika, nustatant kompiuterių sistemų funkcionavimo konfidencialumo režimą, užtikrinant fizinės objektų apsaugos režimą, materialinį – techninį aprūpinimą.

[239] Jungtinių tautų tarptautinės kriminalinės policijos kompiuterinių nusikaltimų apžvalga. International review of criminal policy. United Nations Manual on the prevention and control of compute-related crime, p. 41[interaktyvus, žiūrėta 2011-06-28].
< http://www.bcbkuwait.com/english/int_regulations/UN/CompCrims_UN_Guide.pdf >.

[240] Kadangi šis klausimas jau buvo aptartas, jo plačiau nenagrinėsime.

[241] Petrauskas R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 51.

Organizacinės priemonės, savo ruožtu, skirstomos į:

1. bendras saugumo politikos vystymo priemones (organizacinis saugumas);
2. prevencijos priemones, nukreiptas į personalą (personalo saugumas);
3. procesų apsauga.

Prevencijos priemonių diegimas prasideda bendros saugumo politikos vystymu ir procedūros tam įgyvendinti nustatymu (**Administracinis ir organizacinis saugumas**). Įeina šie elementai:

1. procesų, užtikrinančių rizikos identifikavimą, vystymas;
2. individualių saugumo pareigų apibrėžimas bei atitinkamos atsakomybės paskirstymas;
3. riboto patekimo vietų nustatymas;
4. autentifikavimo procedūrų nustatymas;
5. nenumatytų atvejų planų rengimas ir t.t.

Prevencijos priemonės, nukreiptos į personalą (Personalo apsauga)

Ši apsauga numato asmens identifikaciją ir hierarchijos nustatymą prieinant prie skirtingos svarbos informacijos tiek asmenims, dirbantiems organizacijos viduje, tiek ir asmenims, kontaktuojantiems su organizacija iš išorės.

Apsauga personalo lygyje taip pat apima darbuotojų atranką, testavimą, mokymą, kvalifikacijos patikrinimą bei stebėjimą.

Didžiausia pažeidžiama vieta bet kokioje kompiuterių sistemoje ir didžiausia grėsmė kompiuterių saugumui yra žmonės. Kai kurie žmonės paprasčiausiai gali būti nemokšos, net to nenorėdami gali sunaikinti svarbią informaciją, esančią kompiuterių sistemose. Kiti žmonės gali piktavališkai pažeisti nustatytas taisykles.

Taigi yra daug žmonių tipų, kurie stato į pavojų kompiuterius ir informaciją, pradedant nuo naujų kompiuterių vartotojų, nepatenkintų darbuotojų iki profesionalių nusikaltėlių ir špionažo agentų.

Personalo saugumas yra svarbi kompiuterių sistemų apsaugos dalis. Tam sudaroma personalo saugumo programa, kuri turi būti nuolat vystoma. Dauguma aptiktų elektroninių nusikaltimų yra padaromi darbuotojų, jų motyvacijos gali būti skirtingos. Tačiau personalo saugumo programa turi apimti ne tik vidines grėsmes, bet ir išorines.

Dabar reikia įvertinti darbuotojus. Ar jie gerai testuojami prieš priimant į darbą? Netinkamų darbuotojų samdymas gali atnešti nemalonumų. Reikia turėti gerų vadovų, kurie įvertintų darbuotojų pasiruošimą ir moralę. Taip pat reikia mokyti darbuotojus, kad jie nepadarytų kvailų klaidų, kurios sužlugdytų failus ar programas.

Reikia žinoti, kad pasaulis daro didžiulę įtaką personalo saugumo programoms. Turint sudarytą gerą personalo saugumo programą, galima šiek tiek kontroliuoti įvykius, kai jie kelia grėsmę kompiuterių sistemoms. Grėsmė, susijusi su personalu, priklauso nuo kelių faktorių:

1. prieigos prie kompiuterių sistemų tipo;
2. pažeidėjo išsilavinimo;
3. pažeidėjo motyvacijos.

1. **Prieigos tipai.** Žala kompiuterių sistemoms gali būti padaryta naudojant įvairaus lygio prieigos prie kompiuterių sistemos būdus. Jei žmogus turi tiesioginę prieigą prie kompiuterių sistemos, grėsmė yra daug didesnė. Tačiau ir neturintys tiesioginės prieigos prie kompiuterių sistemos žmonės gali į ją įsilaužti, sugadinti failus, apkrėsti virusu ar padaryti fizinę žalą kompiuterių sistemai.

   Apribojant prieigą prie kompiuterių sistemos, bus efektyviai apsaugota ne tik nuo vagysčių, sabotažo ir kt., bet ir patys darbuotojai negalės padaryti atsitiktinių klaidų, sugadinti kitus failus ar duomenis, su kuriais jie nedirba.

2. **Kvalifikacija.** Kuo didesnė kvalifikacija, tuo didesnė grėsmė. Žiūrint iš kitos pusės, menkos kvalifikacijos darbuotojas, nepatikrinęs diskelio antivirusinėmis programomis, taip pat gali pridaryti daug žalos, tai yra užkrėsti virusu kompiuterių sistemą.

3. **Motyvacija.** Darbuotojai, kuriems patinka jų darbas ir kurių santykiai su darbdaviu geri, nėra linkę vykdyti vandalizmo aktų ar sabotuoti darbdavių kompiuterių sistemų. O štai kita dalis darbuotojų, kurie gavo papeikimus ar yra nepatenkinti dėl kitų priežasčių, kelia didelę grėsmę.

Ne visų elektroninių nusikaltimų motyvai yra neigiami tam tikros organizacijos atžvilgiu. Kai kurie nusikaltimai padaromi norint parodyti savo intelektualinius sugebėjimus,dėl pinigų.

Norint pagerinti personalo apsaugą, reikia:

- vadovauti tarnybos kvalifikacijos patikrinimams;
- sumoderninti informaciją šiems patikrinimams;
- patikrinti visas sutartis su pardavėjais, nustatyti, ar pardavėjai vadovauja savo darbuotojų patikrinimams;
- išdėstyti organizacijai saugumo filosofiją (geriau raštu);
- mokyti darbuotojus būti budriems ir pranešti apie visas įtartinas veikas;
- sukurti sistemas, kad būtų užkirstas kelias individams gauti prieigą prie aparatūros ir failų, kai jie yra vieni;
- mokyti prižiūrėtojus susipažinti su darbuotojų problemomis ir jas spręsti;
- atskirti teisėtos prieigos funkcijas;
- įvesti saugumo revizijos procedūras;
- tikėtis nepatenkintų darbuotojų, buvusių darbuotojų, klientų keršto;

- užtikrinti, kad naudojant kompiuterių sistemas būtų laikomasi visų taisyklių;
- įgyvendinti atostogų politikos ir kaitaliojimosi paskyrimus. Kai kurioms saugumo atakoms reikia ilgo laiko, kad būtų užbaigtos, bet ir jas galima užkirsti;
- apriboti prieigą prie labai svarbių kompiuterių sistemų ir duomenų; jeigu kam nors nereikia priėjimo prie kompiuterių kambario, kompiuterio arba failų, nesuteikti jam šio priėjimo.
- darbuotojui išeinant peržiūrėti, ar darbuotojas turi duomenis; neleisti jam jokios prieigos prie kompiuterių sistemos ateityje, ištrinti jo slaptažodžius; atsiimti raktus, priėjimo kontrolės korteles; patikrinti darbuotojo failus ir išsaugoti juos, jei prireiktų ateityje; jei darbuotojas buvo administratorius, pakeisti visus slaptažodžius sistemoje.

Procesų apsauga

Tai yra saugumo tipas, kuris užkerta kelią kompiuterių sistemų saugumo pažeidimams ir juos aptinka. Procesų apsaugą sudaro du pagrindiniai kompiuterių saugumo aspektai:

- būdai, kuriais galimos elektroninių nusikaltimų aukos supažindinamos su galimais kompiuteriniais nusikaltimais;
- būdai, kuriais nusikaltėliai faktiškai sulaikomi nuo nusikaltimo kompiuterių sistemose padarymo.

Procesų apsauga negali egzistuoti pati viena. Ji efektinga tik tada, kai yra integruota į organizacijos fizinės, personalo ir kt. saugumo programas. Iš tikrųjų procesų apsauga naudojama tam, kad padėtų šioms programoms veikti efektyviau. Yra keli paprasti būdai, kaip procesų apsauga gali sąveikauti su kitomis saugumo procedūromis:

- dažnai keisti savo kompiuterio slaptažodį, bet ne pagal tvarkaraštį, o daugiau atsitiktinai;
- jeigu pastatas yra paprasčiausiai atidarytas, reikia kontroliuoti priėjimą keletą valandų per savaitę, bet kad niekas nežinotų tų valandų;
- maskuoti procesų pavyzdžius, kad juos sunkiai būtų galima atspėti. Pavyzdžiui, užuot programą, tikrinančią autorizuotas programas, paleidus kasnakt 2 valandą, ją paleisti bet kada per 24 valandas, ir kiekvieną kartą programai suteikti skirtingą vardą;
- aktyviai saugoti informaciją, kuria gali pasinaudoti kompiuteriniai nusikaltėliai, planuodami nusikaltimą;
- formuluoti būdus, kurie aptiktų kompiuterinį nusikaltėlį, kai nusikaltimas jau įvyko arba tikėtina, kad įvyks.

Pagrindiniai procesų saugumo programos elementai:

- Nustatymas informacijos, esančios tam tikroje kompiuterių sistemoje, į kurią bandys kėsintis kompiuteriniai nusikaltėliai. Pavyzdžiui, kompiuterinių žaidimų gamintojai žino, kad naujausios žaidimų versijos yra labai patrauklus taikinys.
- Nustatyti metodus, kuriuos gali naudoti elektroninis nusikaltėlis, kad gautų reikiamą informaciją.
- Išvystyti procesų procedūras, kurios pasipriešintų elektroninių nusikaltėlių metodams, užkirstų prieigą prie informacijos ir aptiktų bet kokius saugumo pažeidimus.
- Įtraukti darbuotojus į programą. Jie turi žinoti, kad operacijų saugumas – ir apskritai kompiuterių saugumas – yra svarbi jų procesų dalis.

Užsienio praktika rodo, kad gana efektyvi prevencijos priemonė – kompiuterių saugumo specialisto pareigybės įkūrimas arba atitinkamų dalinių steigimas.

Kad būtų sudaryta efektinga operacijų saugumo programa, reikia išmokti mąstyti kaip nusikaltėliui:

- Kokie motyvai atakuoti tam tikrą taikinį?
- Ar didelės kvalifikacijos reikia, kad ataka būtų sėkminga?
- Kokia informacija reikalinga norint pasiruošti atakai?
- Kaip gali būti bandoma gauti šią informaciją?

Darbuotojams reikia suprasti, kam reikalinga tokia apsauga, kokie yra metodai, leidžiantys kompiuteriniams nusikaltėliams įsilaužti į kompiuterių sistemas, ir ką darbuotojai asmeniškai gali padaryti, kad užkirstų kelią tokiems įsilaužimams[242].

Yra dvi priežastys, kodėl darbuotojų informuotumas yra svarbus. Pirma, yra būdai, kuriais darbuotojai gali sulaikyti nusikaltėlius nuo įsiveržimo į kompiuterių sistemas, pavyzdžiui, darbuotojai turi būti atsargūs ir neužrašinėti viešai slaptažodžių arba neišmetinėti svarbių ataskaitų ir kitokių dokumentų į šiukšliadėžes. Antra, jei darbuotojai bus budrūs, jie gali pastebėti, kada žmogus kėsinasi į informaciją.

2. **Techninės priemonės**

Šias priemonės savo ruožtu skirstomos į:

1. fizines (aparatines);
2. programines;
3. kompleksines.

[242] Icove D. *Computer crime: A Crimefighter`s Handbook.* O`Reylly Associates, Inc., 1995; p. 145.

Fizinė apsauga

Įeina metodai, skirti apsaugoti aparatinėms ir kompiuterių technikos ryšių priemonėms nuo nelaukiamo fizinio pašalinių jėgų poveikio, taip pat užkertantys kelią galimam konfidencialios informacijos ir duomenų nutekėjimui.

Fizinė apsauga apsaugo visus su kompiuterių sistema susijusius įrengimus – pastatą, kompiuterio kambarį, patį kompiuterį ir kitą su juo susijusią įrangą (diskus, spausdintuvus), saugojimo įrenginius (diskus, atspausdintus tekstus), komunikacijų įrenginius (įvairius kabelius). Fizinės apsaugos priemonės apsaugo įrenginius nuo gamtos nelaimių, aplinkos problemų, nelaimingų atsitikimų ir tyčinės žalos[243].

Aparatinės (fizinės) apsaugos metodų realizacija dažniausiai atliekama panaudojant įvairius techninius specialios paskirties įtaisus:

- nepertraukiamo maitinimo šaltinius, saugančius nuo įtampos šuolių;
- aparatūros, ryšių linijų ir patalpų, kuriose yra kompiuteriai, ekranavimo aparatūrą;
- įrenginius, užtikrinančius tiktai sankcionuotą patekimą į saugomus objektus (šifruojamas spynas, asmens identifikacijos įrenginius);
- terminalų ir vartotojų identifikacijos ir fiksacijos, bandant gauti neteisėtą prieigą prie kompiuterių tinklo, įrenginiai;
- apsauginės-gaisrinės signalizacijos priemonės (efektyvios apsaugant kompiuterių tinklus nuo neteisėtos prieigos ir t.t.).

Kompiuterių sistemos fizinė apsauga yra konkretus ženklas darbuotojams ir klientams, kad į apsaugą žiūrima rimtai.

Fizinės apsaugos priemonės naudojamos ir nelaimių prevencijai, o galiausiai jų žalai sumažinti. Fizinės apsaugos priemonės yra nuo paprastų iki kompleksinių: gaisro gesinimo sistemų diegimas, žemės drebėjimo kontrapriemonių diegimas, priėjimo prie pastato, kompiuterių kabineto kontroliavimas ir t. t. Gamtos ir aplinkos pavojai yra rimta grėsmė bet kokiems kompiuterių įrenginiams, jie dažniausiai patenka į elektroninių nusikaltimų tyrėjų akiratį tik jei buvo naudojami tyčinei žalai padaryti. Pavyzdžiui, kas nors gali tyčia sukelti gaisrą arba išjungti elektrą ar oro kondicionavimo sistemą.

Fizinė apsauga nuo žmonių yra gana sudėtinga. Pirma gynybos nuo įsilaužėlių linija yra neprileisti jų prie pastato ar kompiuterių kambario. Tai nėra taip paprasta, kaip būdavo tais laikais, kai dauguma organizacijų turėjo vieną kompiuterį gerai rakinamame kambaryje. Šiomis dienomis daugumoje organizacijų vos ne kiekvienas darbuotojas turi kompiuterį. Todėl čia sunku užtikrinti jų apsaugą.

Kad patektų į pastatą ar užrakintą kompiuterių kambarį, naudotojas turi praeiti tam tikro tipo identifikacijos testą. Yra trys klasikiniai saviidentifikavimo būdai:

[243] Petrauskas R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 56.

- kažkas, ką tu žinai – slaptažodis;
- kažkas, ką tu turi – raktas, ženklelis, kortelė;
- kažkas, kas tu esi – pvz.: papiliarinis raštas.

Visos šios identifikavimo priemonės gali būti naudojamos kompiuterių sistemų fizinei apsaugai užtikrinti.

Didelę grėsmę kelia gamtos nelaimės – ugnis, potvynis, žaibas, žemės drebėjimas. Dauguma gamtos pavojų yra pavojingesni kompiuterių sistemoms, negu kito tipo įrangai, nes kompiuteriai yra jautresni dūmams, dulkėms, vibracijai, vandeniui ir kitoms grėsmėms. Rizika kompiuteriams yra didesnė, juose sukaupta informacija, kurios netekimas gali daug kainuoti, netgi sužlugdyti organizaciją (jei incidentas įvyko joje).

Kai kurios gamtos nelaimės yra labiau tikėtinos, negu kitos. Svarstant savo geografinę padėtį, reikia sudaryti fizinio saugumo planus. Pavyzdžiui, vietovėse, kur gresia potvyniai, kompiuteriai turi būti aukštesniuose aukštuose.

Aplinkos grėsmės, tokios kaip elektra, oro kondicionavimo sistemos, taip pat turi būti fizinio saugumo plano dalis. Elektra yra specifinė kompiuterių sistemų grėsmė. Kompiuterių įrenginiai yra labai jautrūs bet kokiam elektros nutraukimui ar srovės pakitimui. Taip pat reikia rūpintis ir temperatūros kontroliavimu bei drėgme tose vietose, kur laikomos kompiuterių sistemos.

Koncentrinis priėjimo žiedas. Kai vertinama bet kokių įrengimų (taip pat ir kompiuterių sistemų) fizinė apsauga, naudojamas koncentrinis priėjimo žiedas. Pradedama nuo žiedo, kuris yra toliausiai nuo kompiuterių sistemos – nuo žemės sklypo krašto arba nuo gatvės; ir sistemingai einama arčiau prie pagrindinio taško. Yra trys natūralios kliūtys tarp kiekvieno apskritimo krašto ir taikinio. Ar tie barjerai – tai žmonės, ar priėjimo kontrolės sistemos? Kad būtų atsakyta į šį klausimą, reikia nagrinėti kiekvieną žiedą. Jei vienas iš koncentrinių žiedų yra aplink pastatą nuo žemės sklypo krašto iki pastato išorinės sienos, ir jei yra apsaugos darbuotojas prie įėjimo į žemės sklypą, tada šis darbuotojas yra vienas iš priėjimo kontrolės taškų, kuriuos nusikaltėliams reikia įveikti.

Kitas koncentrinis žiedas yra pati išorinė siena. Jei durys ir langai yra uždaryti, įėjimas apribotas tam tikrais būdais. Tai yra tolesnis priėjimo kontrolės taškas. Atliekant sistemingą žiedo kontrolės apžvalgą, galima sužinoti, kaip nusikaltėlis gavo priėjimą prie kompiuterių sistemos. Yra įrodyta, kad labiausiai neapsaugoti stiklai. Atlikdamas savo pagrindinę funkciją – praleisti šviesą – stiklas neapsaugo nuo smalsių žvilgsnių, fotografavimo, akustinių ir elektromagnetinių signalų perėmimo[244]. Langą lengva išdaužti ir tai gali traumuoti žmones, sugadinti kompiuterių sistemas. Pagal statistiką 85 % visų neteisėtų įsibrovimų įvyksta per langus. Visus šiuos trūkumus lengva pašalinti naudojant apsaugines plėveles.

[244] Timec B. V. Sdelai svoi ofis bezopasen. *Zashhita informacii*, 1997, 1. p. 37.

Vertinant kompiuterių sistemos fizinį saugumą, dažniausiai sužinoma, kad keli pažeidžiami taškai neišvengiamai yra ir už kompiuterių kambario ribų: tai elektros sistema ir kt. Dar viena pažeidžiama vieta yra kabeliai.

Labai svarbus momentas yra fizinio saugumo sistemų bandymas. Užuot laukus, kada įvyks elektroninis nusikaltimas, galima patikrinti saugumą. Yra trys fizinio saugumo programos testavimo būdai[245]:

1. sistemingi fizinio saugumo patikrinimai;
2. atsitiktiniai fizinio saugumo patikrinimai;
3. prasiskverbimo testai.

1. Reguliarius fizinės apaugos patikrinimus – fizinio saugumo apžiūrą – dažniausiai vykdo kompanijos darbuotojas pagal iš anksto parengtą sąrašą. Šis sąrašas padeda užtikrinti, kad visos galimos pažeidžiamos vietos patikrintos. Sistema bus efektyvesnė, jei apžiūrą atliks žmonės, nedirbantys tikrinamoje vietoje. Pavyzdžiui, penktame aukšte dirbantys žmonės gali vykdyti ketvirto aukšto apžiūrą.

   Kartais fizinio saugumo patikrinimui įvykdyti samdomi ekspertai. Tai patartina daryti, įvykus dideliems praradimams arba suplanavus esminius fizinio saugumo pakeitimus. Profesionalios komandos ataskaita yra daug geresnė už savos komandos ataskaitą, nes pastaroji gali pasiūlyti ką nors naudingesnio.

2. Atsitiktiniai saugumo patikrinimai. Priėjimo kontrolės sistemos gali būti labai sudėtingos, bet jei darbuotojai palieka atidarytas duris, sistema yra neveikianti. Tokiu atveju naudingi atsitiktiniai saugumo patikrinimai.

3. Prasiskverbimo testus vykdo profesionalai didelės rizikos kompiuterių sistemose (pavyzdžiui, karinių padalinių ir kt.).

Daug žalos padaro gamtos nelaimės. Toliau pateikta keletas rekomendacijų, kaip sumažinti šios grėsmės keliamą žalą.

1. Jei grėsmė yra ugnis ir dūmai:
   - naudoti mūrines sienas, kur tik galima;
   - įrengti ugnies užtvaras;
   - įrengti dūmų detektorius arčiau kompiuterių sistemų ir periodiškai juos tikrinti;
   - užtikrinti, kad dūmų aktyvuota gaisro sistema automatiškai išjungia kompiuterių sistemas ir oro kondicionavimą;
   - laikyti nešiojamas gaisro gesinimo priemones netoli kompiuterių sistemų ir užtikrinti, kad visi žinotų, kur jos yra;

[245] Icove D. *Computer crime: A Crimefighter`s Handbook*. O`Reylly Associates, Inc., 1995, p. 107.

- įgyvendinti nerūkymo politiką, kad nebūtų rūkoma arti kompiuterių sistemų;
- stengtis nenaudoti lengvai degančių baldų;
- laikyti kompiuterių duomenis ugniai atspariuose konteineriuose.

2. Jeigu grėsmė yra vanduo:
   - įrengti kompiuterių sistemas aukštesniuose pastato aukštuose;
   - įrengti pogrindinį drenažą;
   - jei kompiuteris sušlapo, leisti jam visiškai išdžiūti prieš įjungiant.
3. Jeigu grėsmė yra žaibavimas:
   - jei pradeda žaibuoti, išjungti kompiuterį, tada visai išjungti iš tinklo. Žaibas sukaupia didžiulę energiją, todėl kyla grėsmė kompiuterių sistemai, net jei ji išjungta ir turi elektros apsaugą;
   - saugoti diskelius nuo magnetinių laukų, kai žaibas trenkia į pastatą. Juos reikia laikyti toliau nuo plieninių pastato dalių.

Aplinkos nelaimės taip pat gali padaryti didelę žalą.

1. Jei grėsmė yra elektra:
   - kompiuterių sistema gali nukentėti, jei gaus per daug arba per mažai energijos. Reikia įrengti elektros įrenginį, kuris „sugertų“ per didelį energijos kiekį, o jei energija dingtų, aprūpintų kompiuterį ja ir jį būtų galima išjungti;
   - įrengti voltažo reguliatorių savo kompiuterių energijos aprūpinimo sistemoje.
2. Jei grėsmė yra apšildymas arba oro kondicionavimas:
   - laikyti kompiuterius priimtinoje temperatūroje (10-26 laipsnių šilumoje);
   - palaikyti 35-50 % drėgmę;
   - įrengti kompiuterių kambariuose atskiras oro kondicionavimo sistemas;
   - įrengti daviklius, reaguojančius į nenormalius temperatūros ar drėgmės pokyčius;
   - aprūpinti šildymo ir oro kondicionavimo sistemas filtrais, kad apsaugotų nuo dulkių.

Daug žalos kompiuterių sistemoms padaro ir vadinamieji įsiveržėliai – žmonės, be leidimų įvairiais būdais patenkantys prie kompiuterių sistemų. Kad to neįvyktų, reikia laikytis šių taisyklių:

- pastatyti specialias atsargumo priemones duryse, vedančiose į kambarius, kuriuose yra kompiuterių sistemos;

- kambarių sienos turi būti tvirtos;
- kambarių lubos ir grindys turi būti tvirtos;
- oro kondicionavimo langeliai turi būti maži;
- laikyti kompiuterių sistemas toliau nuo langų. Juos lengva išdaužti, ir jei nusikaltėlis juos išdaužia, jau vien langas gali daug kainuoti. Žmonės taip pat gali žiūrėti pro langus ir nuskaityti informaciją;
- skirti apsaugos darbuotojus kritiškuose taškuose, tokiuose kaip išėjimas;
- įrengti priėjimo prie kompiuterių sistemų kontrolės sistemas, naudojančias korteles, pirštо antspaudų skenavimą ar balso pavyzdžius;
- įrengti standartinius įsilaužėlių signalizatorius;
- įrengti televizijos stebėjimo sistemą[246].

Programinė apsauga

Programinės įrangos apsauga skirta užtikrinti kompiuterių sistemos saugumui programiniu lygmeniu[247]. Ši apsauga apima:

- identifikacijos mechanizmus, nustatančius teisėtus vartotojus (slaptažodžių pagalba);
- hierarchijos nustatymą, t.y. užtikrinimą, kad vartotojai neprieitų prie tų informacijos resursų, prie kurių jie neturi teisės prieiti;
- aptikimo priemones, nustatančias saugumo pažeidimus programiniu lygmeniu;
- kitas priemones.

Programinės apsaugos priemonės skirtos betarpiškai informacijos apsaugai trimis kryptimis:

1. aparatūros;
2. programinio aprūpinimo;
3. duomenų ir valdymo programų.

Perduodamos informacijos apsaugai paprastai naudojami įvairūs šifravimo metodai. Kaip rodo praktika, šifravimas yra gana patikima apsaugos priemonė.

Visos apsaugos programos, atliekančios prieigos prie kompiuterių informacijos valdymą, funkcionuoja atsakymo į klausimą principu: kas gali atlikti, kokias operacijas ir t.t.

[246] Icove D. *Computer crime: A Crimefighter`s Handbook*. O`Reylly Associates, Inc., 1995; p. 112.
[247] Česna R., Štitilis D. *Kompiuterinės informacijos ir elektroninio dokumento apsauga viešajame administravime*. Vilnius: Lietuvos teisės akademija, 2000, p. 55.

Prieiga gali būti nustatyta kaip:

- bendra;
- priklausoma nuo įvykio;
- priklausoma nuo duomenų turinio;
- iš dalies priklausoma (pvz.: vartotojui prieiga leidžiama vieną ar nustatytą skaičių kartų);
- pagal vartotojo vardą ar kitus požymius;
- priklausoma nuo pareigų;
- pagal leidimą (pvz.: slaptažodį);
- pagal procedūrą.

Vienomis iš efektyviausių priemonių prieš neteisėtą prieigą laikytinos registracijos priemonės. Šiam tikslui labiausiai tinka naujos specialios paskirties operacinės sistemos, plačiai taikomos užsienio šalyse, vadinamasis monitoringas (automatiškas galimos kompiuterių grėsmės stebėjimas).

Stebėjimą vykdo pati operacinė sistema, be to, ji apdoroja įvesties ir išvesties informaciją bei kontroliuoja ištrynimo procesus. OS fiksuoja neteisėtos prieigos laiką ir programines priemones, kuriomis buvo atliktas prieiga. Be to, ji tuojau pat apie grėsmę informuoja kompiuterių saugumo tarnybas, tuo pat metu išvesdama reikalingus duomenis.

Kaip vieną iš problemų, susijusių su programine apsauga, reikėtų paminėti ir apsaugos nuo kompiuterių virusų problemą. Čia reikia aktyviai naudoti specialias antivirusines programas. Tačiau atkreiptinas dėmesys į tai, jog antivirusinės programos aptinka jau esančius virusus, kirminus ir kitas kenkimo programas, o nuo užkrėtimo tokiomis kenkimo programomis apsaugoti negali[248].

Be antivirusinių programų, apsaugai reikia naudoti ir kompleksines organizacines-technines priemones:

- informuoti visus įstaigos darbuotojus, naudojančius kompiuterių technikos priemones, apie pavojų ir galimą žalą užsikrėtimo virusu atveju;
- uždrausti atsinešti į darbą programinių priemonių;
- uždrausti naudoti ir kompiuterio atmintyje saugoti kompiuterinius žaidimus;
- visi iš išorinio kompiuterių tinklo patenkantys failai turi būti tikrinami;
- archyvuoti duomenis;

[248] Ghosh S., Turrini E. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag, 2010, p. 110.

- nuolat tikrinti, ar vykdomos nustatytos taisyklės ir taikyti poveikio priemones asmenims, tyčia ar ne pirmą kartą pažeidusiems šias taisykles[249].

Prie programinių techninių apsaugos priemonių taip pat priskiriamas šifravimas, užkardos (angl. *firewall*) ir kt.

3. Kompleksinės priemonės

Kompleksinė apsauga verčia sukurti vieningą sistemą, kuri galėtų atremti visas galimas atakas, nukreiptas į kompiuterių sistemą – nuo durų išlaužimo ir aparatinės įrangos pavogimo iki informacijos vagystės iš kompiuterių sistemos. Į kompleksinę apsaugą integruojamos visos aukščiau paminėtos apsaugos priemonės[250].

[249] Icove D. *Computer crime: A Crimefighter`s Handbook*. O`Reylly Associates, Inc., 1995, p. 87-153.
[250] Petrauskas R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 61.

Literatūra

1. Abramavičius A., et al. *Baudžiamoji teisė: specialioji dalis*. 2 knyga. Vilnius: Eugrimas, 2000.
2. Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems Strasbourg, 28.I.2003 [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>.
3. Aiškinamasis raštas dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo [interaktyvus, žiūrėta 2011-06-27]. <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=223058>.
4. Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet, 1997[interaktyvus, žiūrėta 2011-06-28]. <http://papers.ssrn.com/sol3/Delivery.cfm/lp9704291.pdf?abstractid=41684&mirid=3>.
5. Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet. *The Journal of Information, Law and Technology (JILT)*, 1997 (1) [interaktyvus, žiūrėta 2011-06-27] <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1>.
6. Akdeniz Y., Walker C., Wall D. *The Internet, Law and Society.* Pearson Education Limited, 2000.
7. Baibridge D. *Introduction to Computer Law*. Fourth edition. Pearson Education Limited, 2000.
8. Bluvšteinas J., Bieliūnas E., Justickis V. ir kiti. *Kriminologija*. V.: Pradai, 1994.
9. Brenner S. W. *Cybercrime. Criminal Threats from Cyberspace*. Library of Congress Cataloging, 2010.
10. Brenner S. W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. Oxford University Press, 2009.
11. Britz T. M. *Computer Forensics and Cyber Crime: An Introduction*. Pearson Education, 2009.
12. Broadhurst R. Content crimes: criminality and sencorship in Asia. *The Challenge of Cybercrime Conference* on 15-17 September, 2004. Palais de l`Europe, Strasbourg, France [interaktyvus, žiūrėta 2011-06-27]. 10 p. <http://ceps.anu.edu.au/publications/pdfs/broadhurst_pubs/broadhurst-content_cybercrimes.pdf>.
13. Cavazos E. A. *Cyberspace and the Law: Your Rights and Duties in the On-line World*. London: The MIT Press, 1994.
14. Čepčugov D. MVD Onlain. *InterNet magazine*, 2001, 14. [interaktyvus, žiūrėta 2011-05-10]. <http://www.gagin.ru/internet/14/3.html>.

15. Černov A. V. Nekotorije voprosi ugolovno-pravovoj kvalifikaciji kompiuternich mošenničetv. *Sovetskoje gosudarstvo i pravo*, 1989, 6.

16. Česna R., Štitilis D. *Kompiuterinės informacijos ir elektroninio dokumento apsauga viešajame administravime*. Vilnius: Lietuvos teisės akademija, 2000.

17. Communication from the Commision 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 Infrastructuresand Combating Computer-related Crime. Brusssels, 2001.01.26. COM (2000)890 final. [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF>.

18. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions Towards a general policy on the fight against cyber crime. Brussels, 2007.05.22, COM (2007) 267 final. [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

19. Computer Missuse Act, 1990. [interaktyvus, žiūrėta 2011-06-27]. <http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm >.

20. Computer-related crime. Council of Europe. Recomendation No. R(89)9, adopted by Committee of Ministers of the Council of Europe on 13 September 1989 [interaktyvus]. Strasbourg, 1990 [žiūrėta 2011-06-21]. <http://www.oas.org/juridico/english/89-9&final%20Report.pdf>.

21. Convention of Cybercrime CETS No.: 185, Status as of : 10/05/2011. [interaktyvus, žiūrėta 2011-06-27]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=10/05/2011&CL=ENG>.

22. Convention on Cybercrime. [interaktyvus, žiūrėta 2011-06-21]. 16 str. 1 d. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm >.

23. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT>.

24. Council of Europe. Committee of Ministers. Recommendation No. R (95)13 of the Committee of Ministers to member States concerning Problems of Criminal Procedural law Connected with Information Technology [ineraktyvus, žiūrėta 2011-06-27]. <https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2>.

25. Criminal Code of Canada. [interaktyvus, žiūrėta 2011-06-28]. <http://www.legislationline.org/documents/section/criminal-codes>.

26. Criminal Code of the Republic of Latvia. [interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/documents/section/criminal-codes>.

27. Criminal Code of the Republic of Poland. [interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/documents/section/criminal-codes/country/10 >.

28. Criminal code of Ukraine.[interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/documents/action/popup/id/16257/preview >.

29. CSI computer crime survey 2008. [interaktyvus, žiūrėta 2011-06-28]. <http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf>.

30. Cybercrime Act No. 161, 2001 . [interaktyvus, žiūrėta 2011-06-28]. <http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112/sch1.html>.

31. Dillon S. A., Groene D. E., Hayward T. American Criminal law Review. Georgeton university law center, 1998, Vol. 35, p. 513.

32. Dlia borby s kiberprestupnostju nužny popravki v UK. *Centr issledovanija problem kompjuternoj prestupnosti.*[interaktyvus}. 2011-05-17 [žiūrėta 2011-06-27]. <http://www.crime-research.ru/news/17.05.2011/7235/>.

33. Estonia called Asian countries to fight cybercrime. Estonian Ministry of foreign affairs. [interaktyvus, žiūrėta 2011-06-27]. <http://www.vm.ee/?q=en/node/11803>.

34. Estonia changes in Penal Code. *Baltic Legal Newslette,*. Spring, 2008. [interaktyvus, žiūrėta 2011-06-27]. <http://www.infolex.lt/portal/ml/start.asp?act=legupd&lang=eng&biulid=144&srid=27&strid=858>.

35. European Government CERTs (EGC) group. [interaktyvus, žiūrėta 2011-06-27]. <http://www.egc-group.org/>.

36. Europos Parlamento ir Tarybos direktyva dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo pasiūlymas. Briuselis, 2010.9.30 KOM (2010) 517 galutinis. [interaktyvus, žiūrėta 2011-06-27]. <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_lt.pdf>.

37. Explanatory Report to the Convention on Cybercrime (adopted 8 November 2001,the Convention has been opened for signature in Budapest, on 23 November 2001). [interaktyvus, žiūrėta 2011-06-21]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

38. Federal Law on Information, Informatization and the Protection of Information No. 24-FZ [interaktyvus, žiūrėta 2011-06-27]. str. 6. <http://www.fas.org/irp/world/russia/docs/law_info.htm>.

39. Frequently Asked Questions and Answers About the Council of Europe Convention Cybercrime. December 1, 2000. [interaktyvus, žiūrėta 2011-16-18]. <http://www.cybercrime.gov/COEFAQs.htm>.

40. Gahtan A. M., Kratz M. P. J. *Internet Law: A Practical Guide to Legal and Business Professionals*. Carswell: Thomson Proffesional Publishing, 1998.

41. Ghosh S., Turrini E. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag, 2010.

42. Global Risks 2008*,* 2008 m. pasaulinių grėsmių ataskaita. [interaktyvus, žiūrėta 2011-06-27]. <http://www.scribd.com/doc/6310131/Global-Risk-Report-2008>.

43. Gončarov D. Kvalifikacija chiščenij, soveršajemich s pomoščju kompjuterov. [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Goncharov.htm>.

44. Graham J. *Cyber Fraud: Tactics, Techniques and Procedures*. Taylor&Francis Group, 2009.

45. Higgins G. E. *Cybercrime: An Introduction to an Emerging Phenomen*. Library of Congress Cataloging, 2010.

46. Hoffman Sandra K. *Identity Theft: A Reference Handbook. – Santa Barbara, California*, 2010.

47. Icove D. *Computer crime: A Crimefighter`s Handbook*. O`Reylly Associates, Inc., 1995.

48. Icove D., Seger K., VonStorch W. *Computer Crime: A Crimefighters Handbook*. Oreilly&Associates, Inc., 1995.

49. Identity Theft Protection (2007) [interaktyvus, žiūrėta 2011-06-27]. <http://www.identitytheftsecurity.com/protect.shtml#phone>.

50. Iljin I. V. *Viktimologičeskaja profilaktika ekonomičeskogo mošenničestva*: Disertacija kand. jurid. nauk. N.Novgorod, 2000.

51. Inter-departmental Working Group on Computer Related Crime Report. Hon Kong, September, 2000. [interaktyvus, žiūrėta 2011-06-28]. <http://www.hkcsi.org.hk/reports/reports/computer_crime.htm.>.

52. International review of criminal policy - United Nations Manual on the prevention and control of compute-related crime. Jungtinių tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalga[interaktyvus, žiūrėta 2011-06-21]. <http://www.uncjin.org/Documents/irpc4344.pdf>.

53. Jungtinių tautų tarptautinės kriminalinės policijos kompiuterinių nusikaltimų apžvalga. International review of criminal policy. United Nations Manual on the prevention and control of compute-related crime. [interaktyvus, žiūrėta 2011-06-28]. < http://www.bcbkuwait.com/english/int_regulations/UN/CompCrims_UN_Guide.pdf >.

54. Karelina M. M. Prestuplenije v sfere kompiuternoi informaciji.*Centr issledovanija problem kompjuternoj prestupnosti.*[interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/CodeRu.htm>.

55. Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006.

56. Kočoj S., Saveljev D. Otvetsvennost za neprovomernij dostup k kompiuternoj informaciji. *Rosijskaja justicija*, 1999, 1.

57. Komisijos komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“. Briuselis, 2009.03.30, KOM (2009) 149 galutinis. [interaktyvus, žiūrėta2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:PDF>.

58. Komisijos komunikatas Europos parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei regionų komitetui. Dėl kovos su nepageidaujamu e. paštu, šnipinėjimo programomis ir žalinga programine įranga COM (2006) 688 galutinis 2006-11-15, Briuselis [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:LT:PDF>.

59. Komissarov V. S. Prestuplenija v sfere kompiuternoi informaciji: ponetije i otvetstvennost. *Juridičeskij mir*, 1998, fevral.

60. Konvencijos dėl elektroninių nusikaltimų Papildomas Protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo. *Valstybės žinios*. 2006-07-05, Nr. 75-2850. [interaktyvus, žiūrėta 2011-06-27]. <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=279838>.

61. Kosinski J. Some Aspects of Computer Crime in Poland. *The Second International Scientific Practical Conference Information Society 2000 and League of Investors*, Vilnius, October 23-24, 2000, p. 124.

62. Kriminalnij kodeks Ukrainy. *Oficialnij vestnik Ukrainy*, 2001.

63. Krylov V. V. Informacionnye kompiuternyje prestuplenija. M., 1997.

64. Kshetri N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, 2010.

65. Kshetri N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, 2010.

66. Lestrade Dr. Edward, The Cybercrime Phenomenon and Latvian Cybercrime Law. Available at SSRN. [interaktyvus, žiūrėta 2011-06-27]. <http://ssrn.com/abstract=971182>.

67. Lietuvos Respublikos baudžiamojo proceso kodekso 154 straipsnio pakeitimo ir papildymo įstatymas Nr. IX-1993. *Valstybės žinios*, 2002, Nr. 37-1341.

68. Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektas Nr.373-02, 2009-09-21[interaktyvus, žiūrėta 2011-06-28]. <http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=5050&p_query=&p_tr2=&p_org=&p_fix=n&p_gov=n>.

69. Lietuvos Respublikos įstatymas dėl Konvencijos dėl elektroninių nusikaltimų papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, ratifikavimo. *Valstybės žinios*. 2006, Nr. 75-2848.

70. Maxwell W. *Electronic Communications: The New EU Framework*. New York: Oceana Publications, Inc., Dobbs Ferry, 2002.

71. McConnell International. [interaktyvus, žiūrėta 2011-06-28]. <http://www.mcconnellinternational.com>.

72. McConnell B., Plater-Zyberk H. Canadian Cyber Crime Laws Are Among the Strongest. [interaktyvus, žiūrėta 2011-16-18]. <http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/20010102.htm>.

73. Melnik M. I. *Naučno-praktičeskij komentarij ugolovnogo kodeksa Ukraini*. Kiev: Kannon, A.C.K, 2001.

74. Nathanson N., Gringras C. *The Laws of the Internet*. Butterworths, 1997.

75. Naumov V. Otečestvennoje zakonodatelstvo v borbe s kompiuternimu prestuplenijami [interaktyvus, žiūrėta 2011-06-27]. <http://www.russianlaw.net/law/doc/a01.htm>.

76. Navickytė L. Lietuva šviesolaidinį internetą Europoje diegia apsrčiausiai. *Diena* [interaktyvus]. 2010-02-25 [žiūrėta 2011-06-27]. < http://www.diena.lt/naujienos/mokslas-ir-it/lietuva-sviesolaidini-interneta-europoje-diegia-sparciausiai-papildyta-265149>.

77. Orlov P., et al. K opredeleniju vida i razmera nakazanija za prestuplenija v sfere ispolzovanija elektronnoi-vičislitelnoj techniki (kompjuterov), sistem i kompjiuternykh setej v svjazi s prinjatijam novogo ugolovnogo kodeksa Ukrainy. *Centr issledovanija problem kompiuternoj prestupnosti*. [interaktyvus, žiūrėta 2011-06-27] <http://www.crime-research.org/library/End.htm>.

78. Otečestvennoje zakonodatelstvo v borbe s kompiuternimu prestuplenijami. [interaktyvus, žiūrėta 2011-06-27]. <http://www.russianlaw.net/law/doc/a01.htm>.

79. Perrit H. *Law and the Information Superhighway*. Wiley&Sons, Inc., 1996.

80. Petrauskas, R., Štitilis D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000.

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

82. Prestuplenija v sfere ispolzovanija elektronno-vyčeslitelnykh mašin (kompjuterov), sistem i kompjuternykh setej. *Centr issledovanija problem kompjuternoj prestupnosti.*[interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/npkrus.htm>.

83. Public Hearing on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Compabint Computer-related Crime. *Charlemagne Building*, 170, rue de la Loi, Brussels 1040, 7 March 2001.

84. Racicot M., et al. The Cyberspace Is Not a „No Law Land“: a Study of the Issues of Liability For Content Circulating on the Internet.[interaktyvus]. 1997 [žiūrėta 2011-06-28], ISBN 0-622-25489-9. <http://www.google.lt/url?sa=t&source=web&cd=3&ved=0CCsQFjAC&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.17.4392%26rep%3Drep1%26type%3Dpdf&ei=dkQLTrjiDsGbOrmjve0D&usg=AFQjCNFy3irmgJF9Y8PgkBBjnMIUqzlx-g&sig2=PnF4NL2fuTa4yeXdNW683w.>.

85. Report from the Comission to the Council Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems. Brussels, 2008.07.14 COM (2008) 448 final. [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:EN:PDF>.

86. Rowland D., Macdonald E. *Information Technology Law*. Cavendish Publishing Limited, 1997.

87. Sauliūnas D., et al. *Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004.

88. Schjolberg S. The Legal Framework – Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries, Moss District Court, Norway. [interaktyvus, žiūrėta 2011-6-18]. <http://www.mosstingrett.no/info/legal.html>.

89. Sieber U. *Computer Crime and Criminal Information Law – The New Trends in International Risks and Information Society* [interaktyvus, žiūrėta 2011-06-21]. <http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html>.

90. Spivakov A. I. Rosijskoje zakonodatelstvo v borbe s kompiuternimi prestuplenijami. *Centr issledovanija problem kompjuternoj prestupnosti.* 2001 [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Spivak.htm>.

91. Štitilis D. IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui. *Socialinių mokslų studijos*, 2009, 1(1).

92. Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai. *Jurisprudencija*, 2003, 47(39).

93. Štitilis D. Neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimas. *Informacijos mokslai*, 2003, 26.

94. Štitilis D. Privataus gyvenimo elektroniniuose ryšiuose ribojimas nusikaltimų tyrimo tikslais. *Jurisprudencija*, 2006, 9(87).

95. Štitilis D. Teisinės atsakomybės pagrindų už neteisėtas veikas elektroninėje erdvėje nustatymo prolemos. Disertacija. Vilnius: 2002.

96. Štitilis D., et al. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. *Socialinių mokslų studijos*, 2011, Nr. 3(1).

97. Štitilis D., Krikščiūnas R., Petrauskas R. Kai kurie Konvencijos dėl elektroninių nusikaltimų procesoteisės skirsnio įgyvendinimo Lietuvoje aspektai. *Jurisprudencija*, 2005, 67(59).

98. Štitilis D., Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*, 2009, 50.

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

100. Štitilis D., Petrauskas R. Criminal Acts in Computer Systems and Their Legal Regulation. *Databases & information systems. Proceedings of the 4th IEEE international Baltic workshop*, Vol. 2, Vilnius: Technika, 2000.

101. Štitilis D., Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai.* 2009, 50245.

102. Survey on the Cybercrime Convention (CETS 185) and its additional protocol (CETS 189). European Committee on Crime Problems. [interaktyvus, žiūrėta 2011-06-28]. <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_en.asp>.

103. Tamburrini P. *European Computer Law. Information Technology Law Group/ Europe*. New York: Transnational Publishers, Inc., 1996.

104. The Criminal code of the Russian Federation, str. 272. [interaktyvus, žiūrėta 2011-06-27]. <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.

105. Timec B. V. Sdelai svoi ofis bezopasen. *Zashhita informacii*, 1997, 1.

106. Tuniso informacinės visuomenės darbotvarkė.[interaktyvus]. 2005-11-18 [žiūrėta 2011-06-27]. <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>.

107. UK finally ratifies convention on cybercrime. *ComputerWeekly.com*, May 25, 2011[interaktyvus, žiūrėta 2011-06-15]. <http://www.computerweekly.com/blogs/when-it-meets-politics/2011/05/uk-finally-ratifies-the-conven.html>.

108. UK loses over 43 bilion dollars a year to cybercrime. *In the World News* [interaktyvus]. 2011-02-18 [žiūrėta 2011-06-20]. <http://www.intheworldnews.com/uk-loses-over-43-billion-dollars-a-year-to-cyber-crime/341153/>.

109. Volevodz A. G. *Protivodeistvije kompiuternim prestuplenijam*. Moskva: Jurlitinform, 2002.

110. Voronov I. A. Nekotorije problemi deistvujuščego zakonodatelstva po vaprosam ugolovnoi otvetstvennosti za prestuplenija v sfere ispolzovanija elektronno-vičislitelnykh mašyn. [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Voron.htm>.

111. Wasik M. Computer Crimes and Other Crimes Against Information Technology in United Kingdom. *International Review of Penal Law: Computer Crimes and Other Crimes Against Information Technology*. Wurzburg, Germany, 1992.

112. Williams M. *Virtually criminal: Crime, deviance and regulation online*. New York: Routledge, 2006.

113. Žalioji knyga. Apie Europos programą dėl ypatingos svarbos infrastruktūros objektų apsaugos. Briuselis, 2005.11.17 KOM (2005) 576 (galutinis). [interaktyvus, žiūrėta 2011-06-27]. <http://eur-lex.europa.eu/LexUriServ/site/lt/com/2005/com2005_0576lt01.pdf>.

114. Zavidov B. O ponetiji mošenničestva i jego modifikacijach v ugolovnom prave. *Pravo i ekonomika*, 1998, 11.

115. Zykov D. Ponjatie obmana, soveršajemogo pri kompjuternom mošenničestve. *Centr issledovanija problem kompjuternoj prestupnosti.* [interaktyvus, žiūrėta 2011-06-27]. <http://www.crime-research.org/library/Zikov1.htm>.

PRIEDAI

Priedas Nr. 1

KONVENCIJA DĖL ELEKTRONINIŲ NUSIKALTIMŲ

2001 11 23, Budapeštas

PREAMBULĖ

Europos Tarybos valstybės narės ir kitos šią Konvenciją pasirašiusios valstybės,

TURĖDAMOS omenyje, kad Europos Tarybos tikslas – siekti didesnės savo narių vienybės;

PRIPAŽINDAMOS skatinimo bendradarbiauti su kitomis šios Konvencijos šalimis svarbą;

ĮSITIKINUSIOS, kad būtina pirmenybę teikti bendros baudžiamosios politikos, kuria siekiama apsaugoti visuomenę nuo elektroninių nusikaltimų, *inter alia* priimant tinkamus teisės aktus ir skatinant tarptautinį bendradarbiavimą, vykdymui;

MATYDAMOS dideles permainas, vykstančias dėl kompiuterių tinklų skaitmeninio keitimo, susiliejimo ir nuolatinės globalizacijos;

SUSIRŪPINUSIOS, kad kompiuteriniai tinklai ir elektroninė informacija taip pat gali būti naudojami daryti nusikaltimams ir kad tokių nusikaltimų įrodymai gali būti saugomi šiuose tinkluose ir jais perduodami;

PRIPAŽINDAMOS, kad valstybėms ir privačiam verslui būtina bendradarbiauti kovojant su elektroniniais nusikaltimais ir būtinybę ginti teisėtus interesus naudojant bei plėtojant informacines technologijas;

MANYDAMOS, kad norint sėkmingai kovoti su elektroniniais nusikaltimais reikia tarptautiniu mastu daugiau, greičiau ir sklandžiau bendradarbiauti baudžiamosiose bylose;

ĮSITIKINUSIOS, kad ši Konvencija, nustatydama joje apibūdintų veikų baudžiamumą, suteikdama pakankamai įgaliojimų veiksmingai kovoti su tokiais nusikaltimais, palengvindama jų susekimą, tyrimą bei baudžiamąjį persekiojimą nacionaliniu bei tarptautiniu lygiu ir pateikdama greito bei patikimo tarptautinio bendradarbiavimo gaires, yra reikalinga, kad būtų sustabdyti veiksmai, nukreipti prieš kompiuterinių sistemų, tinklų ir kompiuterinių duomenų konfidencialumą, vientisumą ir prieinamumą, taip pat kad nebūtų leista netinkamai naudoti tokių sistemų, tinklų ir duomenų;

SUPRASDAMOS poreikį užtikrinti tinkamą balansą tarp teisėsaugos interesų ir pagarbos pagrindinėms žmogaus teisėms, įtvirtintoms 1950 m. Europos Tarybos Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje, 1966 m. Jungtinių Tautų tarptautiniame pilietinių ir politinių teisių pakte ir kitose taikytinose tarptautinėse žmogaus teisių sutartyse, kurios dar kartą patvirtina kiekvieno asmens teisę laisvai laikytis savo nuomonės, taip pat laisvai reikšti savo mintis ir įsitikinimus, nepaisant valstybių sienų, gauti bei perduoti visokią informaciją ir idėjas ir teisę į tai, kad būtų gerbiamas jo asmeninis gyvenimas;

SUPRASDAMOS, be kita ko, būtinybę apsaugoti asmens duomenis, kaip nustatyta 1981 m. Europos Tarybos konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu;

ATSIŽVELGDAMOS į 1989 m. Jungtinių Tautų vaiko teisių konvenciją ir 1999 m. Tarptautinės darbo organizacijos blogiausių vaikų darbo formų konvenciją;

ATSIŽVELGDAMOS į galiojančias Europos Tarybos konvencijas dėl bendradarbiavimo baudžiamojoje srityje, taip pat į panašias sutartis, sudarytas tarp Europos Tarybos valstybių narių ir kitų valstybių, ir PAŽYMĖDAMOS, jog šios Konvencijos tikslas – papildyti šias konvencijas, kad nusikaltimų, susijusių su kompiuterinėmis sistemomis ir duomenimis, tyrimas ir nagrinėjimas būtų atliekami veiksmingiau ir kad šių nusikaltimų įrodymus būtų galima rinkti elektroniniu pavidalu;

PRITARDAMOS naujausiems poslinkiams, skatinantiems tarptautinį supratimą ir bendradarbiavimą kovojant su elektroniniais nusikaltimais, tarp jų Jungtinių Tautų, OECD, Europos Sąjungos ir G8 veiksmus;

ATSIMINDAMOS Rekomendaciją Nr. R(85) 10, skirtą praktiniam Europos konvencijos dėl savitarpio pagalbos baudžiamosiose bylose taikymui vykdant teismo pavedimus dėl telekomunikacinių priemonių pasiklausymo, Rekomendaciją Nr. R(88) 2 dėl autorių teisių ir gretutinių teisių pažeidimų, Rekomendaciją Nr. R(87) 15, reglamentuojančią asmens duomenų naudojimą policijos pajėgose, Rekomendaciją Nr. R(95) 4 dėl asmens duomenų apsaugos telekomunikacijų paslaugų srityje, ypač telefono ryšio paslaugų srityje, taip pat Rekomendaciją Nr. R(89) 9 dėl kompiuterinių nusikaltimų, kurioje pateikiamos rekomendacijos valstybių įstatymų leidybos institucijoms dėl kai kurių kompiuterinių nusikaltimų apibrėžimų, ir Rekomendaciją Nr. R(95) 13 dėl baudžiamojo proceso teisės problemų, susijusių su informacijos technologijomis;

ATSIŽVELGDAMOS į Rezoliuciją Nr. 1, priimtą Europos valstybių teisingumo ministrų 21-ojoje konferencijoje (1997 m. birželis, Praha), rekomendavusią Ministrų Komitetui paremti darbą, kurį Europos nusikalstamumo problemų komitetas (CDPC) atlieka elektroninių nusikaltimų srityje siekdamas vienodinti nacionalinės baudžiamosios teisės nuostatas ir tokių nusikaltimų tyrimui taikyti veiksmingas priemones, taip pat Rezoliuciją Nr. 3, priimtą Europos valstybių teisingumo ministrų 23-iojoje konferencijoje (2000 m. birželis, Londonas), kurioje besiderančios šalys raginamos toliau ieškoti tinkamų sprendimų, kad kuo daugiau valstybių galėtų tapti šios Konvencijos Šalimis, ir pripažįstamas reikalas turėti greitai ir gerai veikiančią tarptautinio bendradarbiavimo

sistemą, kurioje būtų deramai atsižvelgiama į kovos su elektroniniais nusikaltimais ypatumus;

ATSIŽVELGDAMOS, be to, į Europos Tarybos valstybių ir jų vyriausybių vadovų veiksmų planą, priimtą antrajame viršūnių susitikime (1997 m. spalio 10–11 d., Strasbūras), kuriuo siekiama bendro atsako į naujų informacinių technologijų plėtrą, pagrįsto Europos Tarybos kriterijais ir vertybėmis,

s u s i t a r ė:

I SKYRIUS. SĄVOKŲ VARTOJIMAS

1 straipsnis. Sąvokų apibrėžimai

Šioje Konvencijoje:

a) „kompiuterinė sistema“ – tai įtaisas arba tarpusavyje sujungtų ar susijusių įtaisų grupė, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja duomenis;

b) „kompiuteriniai duomenys“ – tai bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat programa, pagal kurią kompiuterinė sistema gali vykdyti tam tikrą funkciją;

c) „paslaugos teikėjas“ – tai:

   i) bet kuris viešasis ar privatus subjektas, teikiantis savo paslaugos vartotojams galimybę bendrauti pasinaudojant kompiuterine sistema;

   ii) bet kuris kitas subjektas, apdorojantis arba saugantis tokios ryšio paslaugos arba tokios paslaugos vartotojų kompiuterinius duomenis;

d) „srauto duomenys“ – tai visi kompiuteriniai duomenys, perduodami kompiuterine sistema, suformuoti kompiuterinės sistemos, kuri sudaro ryšio grandinės dalį, ir rodantys perduotos informacijos kilmę, paskirtį, perdavimo kelią, laiką, datą, dydį, trukmę arba pagrindinės paslaugos rūšį.

II SKYRIUS. PRIEMONĖS, KURIŲ REIKIA IMTIS NACIONALINIU LYGIU

1 skirsnis. Materialioji baudžiamoji teisė

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

2 straipsnis. Neteisėta prieiga

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą

prieigą prie visos kompiuterinės sistemos arba jos dalies. Šalis gali reikalauti, kad toks nusikaltimas būtų padarytas pažeidžiant apsaugos priemones, ketinant gauti kompiuterinius duomenis ar turint kitą nesąžiningą ketinimą, arba kad jis būtų susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema.

3 straipsnis. Neteisėta perimtis

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą neviešo kompiuterinių duomenų perdavimo į kompiuterinę sistemą, iš jos ir jos viduje perimtį techninėmis priemonėmis, taip pat už elektromagnetinės emisijos iš kompiuterinės sistemos, perduodančios tokius kompiuterinius duomenis, perimtį. Šalis gali reikalauti, kad toks nusikaltimas būtų padarytas turint nesąžiningą ketinimą arba susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema.

4 straipsnis. Poveikis duomenims

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterinių duomenų sugadinimą, sunaikinimą, apgadinimą, pakeitimą arba galimybės naudotis tokiais duomenimis panaikinimą.
2. Šalis gali pasilikti teisę reikalauti, kad veika, apibūdinta šio straipsnio 1 dalyje, turi padaryti didelę žalą.

5 straipsnis. Poveikis sistemai

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą didelį kompiuterinės sistemos darbo trukdymą įvedant, perduodant, sugadinant, sunaikinant, apgadinant, pakeičiant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis.

6 straipsnis. Netinkamas įtaisų naudojimas

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą:

a) gaminimą, pardavimą, įsigijimą naudoti, įvežimą, platinimą arba kitokį galimybės naudotis suteikimą:
   i) įtaiso, įskaitant kompiuterinę programą, sukurto ar pritaikyto pirmiausia 2–5 straipsniuose apibūdintiems nusikaltimams daryti;
   ii) kompiuterio slaptažodžio, prieigos kodo arba panašių duomenų, kuriais galima prieiti prie visos kompiuterinės sistemos arba jos dalies,

   kai ketinama juos panaudoti 2–5 straipsniuose apibūdintiems nusikaltimams daryti, ir

b) a punkto i ir ii papunkčiuose minimo dalyko turėjimą ketinant jį panaudoti 2–5 straipsniuose apibūdintiems nusikaltimams daryti. Šalis, vadovaudamasi savo

teise, gali reikalauti, kad baudžiamoji atsakomybė būtų užtraukiama tik turint keletą tokių dalykų.

2. Šis straipsnis negali būti aiškinamas kaip užtraukiantis baudžiamąją atsakomybę kai šio straipsnio 1 dalyje minimas gaminimas, pardavimas, įsigijimas naudoti, įvežimas, platinimas ir kitoks galimybės naudotis suteikimas arba turėjimas nėra skirtas daryti nusikaltimui, apibūdintam šios Konvencijos 2–5 straipsniuose, o tik sankcionuotam kompiuterinės sistemos tikrinimui arba jos apsaugai.
3. Kiekviena Šalis gali pasilikti teisę netaikyti šio straipsnio 1 dalies, jei ši išlyga nesiejama su pardavimu, platinimu arba kitokiu galimybės naudoti šio straipsnio 1 dalies a punkto ii papunktyje nurodytas priemones sudarymą.

2 dalis. Kompiuteriniai nusikaltimai

7 straipsnis. Kompiuterinės klastotės

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterių duomenų įvedimą, pakeitimą, sunaikinimą arba galimybės naudotis tokia informacija panaikinimą, kurių pasekmė yra neautentiški duomenys, su tikslu, kad jie būtų laikomi autentiškais, ar jais būtų naudojamasi teisėtiems tikslams, nepriklausomai nuo to, ar šie duomenys yra tiesiogiai skaitomi ir suprantami. Šalis gali reikalauti, kad baudžiamoji atsakomybė užtraukiama tik esant ketinimui apgauti ar panašiam nesąžiningam ketinimui.

8 straipsnis. Kompiuterinis sukčiavimas

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningus ir neteisėtus veiksmus, sąlygojusius kito asmens nuosavybės praradimą:

a) įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis;
b) paveikiant kompiuterinės sistemos darbą,

nesąžiningai arba nedorai ketinant gauti neteisėtos ekonominės naudos sau arba kitam asmeniui.

3 dalis. Turinio nusikaltimai

9 straipsnis. Nusikaltimai, susiję su vaikų pornografija

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už tokią sąmoningą ir neteisėtą veiką:

a) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, gaminimą turint tikslą platinti per kompiuterinę sistemą;

b) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, siūlymą arba pateikimą per kompiuterinę sistemą;

c) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, platinimą arba perdavimą per kompiuterinę sistemą;

d) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, įsigijimą per kompiuterinę sistemą sau arba kitam asmeniui;

e) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, laikymą kompiuterinėje sistemoje arba kokioje nors kompiuterinių duomenų atmeniojoje terpėje.

2. Šio straipsnio 1 dalyje „pornografinio turinio produkcija, kurioje atvaizduotas vaikas“ – tai pornografinė medžiaga, vizualiai vaizduojanti:

   a) aiškiai seksualų nepilnamečio elgesį;

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

   c) tikroviškus nepilnamečio aiškiai seksualaus elgesio vaizdus.

3. Šio straipsnio 2 dalyje sąvoka „nepilnametis“ reiškia visus asmenis iki 18 metų. Tačiau bet kuri Šalis gali nustatyti žemesnę amžiaus ribą, ir tas amžius negali būti mažiau nei 16 metų.

4. Kiekviena Šalis gali pasilikti teisę netaikyti visų arba kai kurių šio straipsnio 1 dalies d bei e punktų ir 2 dalies b bei c punktų.

4 dalis. Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais

10 straipsnis. Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už autorių teisių pažeidimus, kaip apibrėžta tos Šalies teisėje laikantis įsipareigojimų, kuriuos ji prisiėmė pagal Berno konvencijos dėl literatūros ir meno kūrinių apsaugos Paryžiaus aktą, priimtą 1971 m. liepos 24 d., Sutartį dėl intelektinės nuosavybės teisių prekyboje aspektų ir WIPO autorių teisių sutartį, išskyrus moralines teises, suteikiamas tokių konvencijų, kai tokie veiksmai atliekami sąmoningai, komerciniais tikslais ir naudojantis kompiuterių sistema.

2. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už gretutinių teisių pažeidimus, kaip apibrėžta tos Šalies teisėje laikantis įsipareigojimų, kuriuos ji prisiėmė pagal Romoje sudarytą Tarptautinę konvenciją dėl atlikėjų, fonogramų gamintojų ir transliuojančiųjų organizacijų apsaugos (Romos konvencija), Sutartį dėl intelektinės nuosavybės teisių prekyboje aspektų ir WIPO atlikimų ir fonogramų sutartį, išskyrus moralines teises, suteikiamas tokių konvencijų, kai tokie veiksmai atliekami sąmoningai, komerciniais tikslais ir naudojantis kompiuterių sistema.

3. Šalis gali pasilikti teisę ribotomis aplinkybėmis nenustatyti baudžiamosios atsakomybės, užtraukiamos pagal šio straipsnio 1 ir 2 dalis, jeigu esama kitų veiksmingų priemonių ir jeigu tokia išlyga nepažeidžia Šalies tarptautinių įsipareigojimų, išvardytų tarptautiniuose dokumentuose, minimuose šio straipsnio 1 ir 2 dalyse.

5 dalis. Papildoma atsakomybė ir sankcijos

11 straipsnis. Pasikėsinimas ir bendrininkavimas arba kurstymas

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos teisės aktus nustatyti baudžiamajai atsakomybei už sąmoningą bendrininkavimą arba kurstymą daryti nusikaltimus, išvardytus šios Konvencijos 2–10 straipsniuose, ketinant tuos nusikaltimus padaryti.
2. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos teisės aktus nustatyti baudžiamajai atsakomybei už sąmoningą pasikėsinimą daryti nusikaltimus, išvardytus šios Konvencijos 3–5, 7, 8 straipsniuose, 9 straipsnio 1 dalies a ir c punktuose.
3. Kiekviena Šalis pasilieka teisę netaikyti visos šio straipsnio 2 dalies arba kai kurių jos nuostatų.

12 straipsnis. Juridinio asmens atsakomybė

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinant, kad juridinis asmuo galėtų būti patrauktas atsakomybėn už nusikaltimus, minimus šioje Konvencijoje ir padarytus jo naudai fizinio asmens, veikiančio individualiai arba kaip juridinio asmens organo dalis ir einančio vadovaujančias pareigas juridiniame asmenyje, paremtas teise:
   a) atstovauti šiam juridiniam asmeniui;
   b) priimti sprendimus šio juridinio asmens vardu;
   c) kontroliuoti juridinio asmens veiklą.
2. Be jau minėtų 1 dalyje atvejų, kiekviena Šalis imasi priemonių, reikalingų užtikrinti, kad juridinis asmuo galėtų būti patrauktas atsakomybėn, kai dėl šio straipsnio 1 dalyje minimo fizinio asmens nepakankamos priežiūros arba kontrolės jurinio asmens įgaliotam fiziniam asmeniui buvo galima juridinio asmens naudai padaryti šioje Konvencijoje nustatytą nusikaltimą.
3. Atsižvelgiant į Šalies teisės principus, juridinio asmens atsakomybė gali būti baudžiamoji, civilinė arba administracinė.
4. Tokia atsakomybė nepašalina fizinių asmenų, padariusių nusikaltimą, baudžiamosios atsakomybės.

13 straipsnis. Sankcijos ir priemonės

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinti, kad už 2–11 straipsniuose minimus nusikaltimus būtų taikomos veiksmingos, proporcingos ir atgrasančios sankcijos, įskaitant laisvės atėmimą.
2. Kiekviena Šalis užtikrina, kad juridiniams asmenims, traukiamiems atsakomybėn pagal 12 straipsnį, būtų taikomos veiksmingos, proporcingos ir atgrasančios baudžiamosios arba nebaudžiamosios sankcijos arba priemonės, įskaitant pinigines baudas.

2 skirsnis. Proceso teisė

1 dalis. Bendrosios nuostatos

14 straipsnis. Procesinių nuostatų taikymo sritis

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti nustatyti šiame skirsnyje numatytiems įgaliojimams ir procedūroms konkretiems nusikaltimams tirti ar nagrinėti.
2. Išskyrus 21 straipsnyje konkrečiai nustatytus atvejus, kiekviena Šalis šio straipsnio 1 dalyje minimus įgaliojimus ir procedūras taiko:
   a) nusikaltimams, nustatytiems šios Konvencijos 2–11 straipsniuose;
   b) kitiems nusikaltimams, padarytiems naudojantis kompiuterine sistema,
   c) nusikaltimo įrodymų rinkimui elektroniniu pavidalu.
3. a) Kiekviena Šalis gali pasilikti teisę 20 straipsnyje minimas priemones taikyti tiktai išlygoje nurodytiems nusikaltimams arba nusikaltimų kategorijoms, jeigu tokių nusikaltimų arba nusikaltimų kategorijų apimtis nėra siauresnė nei nusikaltimų, kuriems ji taiko 21 straipsnyje minimas priemones. Kiekviena Šalis apsvarsto, kaip apriboti tokią išlygą, kad būtų galima kuo plačiau taikyti 20 straipsnyje minimas priemones.

   b) Jeigu Šalis dėl jos teisės aktuose, galiojančiuose šios Konvencijos priėmimo metu, esančių apribojimų negali 20 ir 21 straipsniuose minimų priemonių taikyti informacijai, perduodamai paslaugos teikėjo kompiuterinėje sistemoje, kuri:
      i) veikia uždaros vartotojų grupės naudai,
      ii) nenaudoja viešųjų ryšių tinklų ir nėra sujungta su kita vieša ar privačia kompiuterine sistema,

   ta Šalis gali pasilikti teisę netaikyti šių priemonių tokiai informacijai. Kiekviena Šalis apsvarsto, kaip apriboti tokią išlygą, kad būtų galima kuo plačiau taikyti 20 ir 21 straipsniuose minimas priemones.

15 straipsnis. Sąlygos ir garantijos

1. Kiekviena Šalis užtikrina, kad šiame skirsnyje numatytų įgaliojimų ir procedūrų nustatymas, vykdymas ir taikymas priklausytų nuo sąlygų ir garantijų, numatytų tos valstybės vidaus teisėje, kurios laiduoja tinkamą žmogaus teisių ir laisvių apsaugą, įskaitant teises, kylančias iš įsipareigojimų, prisiimtų pagal 1950 m. Europos Tarybos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją, 1966 m. Jungtinių Tautų tarptautinį pilietinių ir politinių teisių paktą bei kitus taikytinus tarptautinius žmogaus teisių dokumentus, ir pagal kurias laikomasi proporcingumo principo.
2. Prie tokių sąlygų ir garantijų, tinkamai atsižvelgiant į įgaliojimo arba procedūros pobūdį, *inter alia* yra priskiriama teisminė arba kitokia nepriklausoma priežiūra, jų taikymą pateisinantys pagrindai ir tokio įgaliojimo arba tokios procedūros taikymo srities bei trukmės apribojimas.
3. Tiek, kiek tai neprieštarauja visuomenės interesams, ypač tinkamam teisingumo vykdymui, kiekviena Šalis apsvarsto šiame skirsnyje minimų įgaliojimų ir procedūrų poveikį trečiųjų šalių teisėms, įsipareigojimams ir teisėtiems interesams.

2 dalis. Operatyvus laikomųjų kompiuterinių duomenų išsaugojimas

16 straipsnis. Operatyvus laikomųjų kompiuterinių duomenų išsaugojimas

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgalinant jos kompetentingas institucijas nurodyti arba panašiai pasirūpinti operatyviu konkrečių kompiuterinių duomenų, įskaitant srauto duomenis, laikomus kompiuterinėje sistemoje, išsaugojimu, ypač kai yra pagrindo manyti, jog tie kompiuteriniai duomenys gali būti nesunkiai prarasti arba pakeisti.
2. Kai vykdydama šio straipsnio 1 dalį Šalis kuriam nors asmeniui nurodo išsaugoti tam tikrus to asmens turimus ir valdomus kompiuterinius duomenis, Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad tas asmuo būtų įpareigotas išsaugoti ir išlaikyti tokių kompiuterių duomenų vientisumą tiek laiko, kiek tai yra reikalinga, ne ilgiau kaip 90 dienų, kad kompetentingos institucijos galėtų pareikalauti juos atskleisti. Šalis gali numatyti, kad toks nurodymas vėliau gali būti kartojamas.
3. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad kompiuterinių duomenų saugotojas arba kitas juos saugantis asmuo būtų įpareigotas išlaikyti tokių procedūrų slaptumą tiek laiko, kiek numatyta pagal tos Šalies vidaus teisę.
4. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

17 straipsnis. Operatyvus srauto duomenų išsaugojimas ir dalinis atskleidimas

1. Pagal 16 straipsnį būtinų išsaugoti srauto duomenų atžvilgiu kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti:
   a) užtikrinti, kad toks operatyvus srauto duomenų išsaugojimas yra galimas, nepaisant to, ar tokią informaciją perdavė vienas ar daugiau paslaugos teikėjų;
   b) užtikrinti, kad kompetentingai Šalies institucijai arba jos paskirtam asmeniui būtų operatyviai atskleista pakankamai srauto duomenų, leidžiančių Šaliai nustatyti paslaugos teikėjus ir tos informacijos perdavimo kelią.
3. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

3 dalis. Nurodymas dėl duomenų pateikimo

18 straipsnis. Nurodymas dėl duomenų pateikimo

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas nurodyti:
   a) jos teritorijoje esančiam asmeniui pateikti konkrečiai nurodytus to asmens turimus arba valdomus kompiuterinius duomenis, laikomus kompiuterinėje sistemoje arba kompiuterinių duomenų atmeniojoje terpėje;
   b) paslaugos teikėjui, tos Šalies teritorijoje siūlančiam savo paslaugas, pateikti jo turimą arba valdomą abonentinę informaciją, susijusią su tokiomis paslaugomis.
2. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.
3. Šiame straipsnyje „abonentinė informacija“ – tai bet kuri kompiuterinių duomenų ar kitokio pavidalo (išskyrus srauto arba turinio duomenis) informacija, turima paslaugos teikėjo ir susijusi su jo paslaugų abonentais, iš kurios galima nustatyti:
   a) naudotos ryšio paslaugos tipą, taikytas technines priemones ir naudojimo laiką;
   b) abonento tapatybę, pašto ar geografinės padėties adresą, telefono ir bet kokį kitą prieigos numerį, informaciją apie sąskaitas ir mokėjimus, gaunamą paslaugos sutarties arba susitarimo pagrindu;
   c) bet kurią kitą informaciją ryšių aparatūros įrengimo vietoje, turimą pagal paslaugos sutartį arba susitarimą.

4 dalis. Laikomųjų kompiuterinių duomenų paieška ir poėmis

19 straipsnis. Laikomųjų kompiuterinių duomenų paieška ir poėmis

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas apieškoti ar panašiai ištirti:
   a) kompiuterinę sistemą arba jos dalį ir joje laikomus kompiuterinius duomenis;
   b) kompiuterinių duomenų atmeniąją terpę, kurioje tos Šalies teritorijoje gali būti laikomi kompiuteriniai duomenys.
2. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinti, kad jos institucijoms pagal šio straipsnio 1 dalies a punktą apieškant ar panašiai tiriant konkrečią kompiuterinę sistemą arba jos dalį ir turint priežasčių manyti, kad ieškomi duomenys laikomi tos Šalies teritorijoje esančioje kitoje kompiuterinėje sistemoje arba jos dalyje ir kad tokie duomenys yra teisėtai prieinami naudojant pirmąją sistemą, tokios institucijos galėtų operatyviai išplėsti paiešką ar panašų tyrimą į kitą sistemą.
3. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgalinant jos kompetentingas institucijas areštuoti arba panašiai išsaugoti kompiuterinius duomenis, gautus pagal šio straipsnio 1 arba 2 dalį. Prie šių priemonių priskiriami įgaliojimai:
   a) areštuoti arba panašiai išsaugoti kompiuterinę sistemą arba jos dalį, arba kompiuterių duomenų atmeniąją terpę;
   b) pasidaryti ir pasilaikyti tokių kompiuterinių duomenų kopiją;
   c) išsaugoti atitinkamų kompiuterinių duomenų vientisumą;
   d) padaryti tokius kompiuterių duomenis neprieinamus arba pašalinti juos iš apieškotos kompiuterinės sistemos.
4. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas nurodyti bet kuriam asmeniui, žinančiam apie tokios kompiuterinės sistemos veikimą arba apie priemones, kurių buvo imtasi joje esantiems kompiuteriniams duomenims apsaugoti, pateikti, kiek tai pagrįsta, informaciją, reikalingą, kad būtų galima taikyti šio straipsnio 1 ir 2 dalyse minimas priemones.
5. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

5 dalis. Kompiuterinių duomenų surinkimas realiuoju laiku

20 straipsnis. Srauto duomenų surinkimas realiuoju laiku

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas:

a) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti;

b) priversti paslaugos teikėją pagal jo technines galimybes:

i) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti arba

ii) bendradarbiauti su kompetentinga institucija ir padėti jai surinkti arba įrašyti

realiuoju laiku srauto duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterine sistema.

2. Jeigu Šalis dėl savo teisinės sistemos principų negali taikyti šio straipsnio 1 dalies a punkte minimų priemonių, ji gali priimti tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad jos teritorijoje realiuoju laiku, naudojant technines priemones, būtų surinkti ir įrašyti srauto duomenys, susiję su konkrečia toje teritorijoje perduodama informacija.

3. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įpareigoti paslaugos teikėją laikyti paslaptyje bet kurių šiame straipsnyje minimų įgaliojimų vykdymą ir bet kurią informaciją apie jų vykdymą.

4. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

21 straipsnis. Turinio duomenų perimtis

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad dėl sunkių nusikaltimų, apibrėžtų tos Šalies vidaus teisėje, kompetentingos institucijos būtų įgalintos:

a) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti

b) priversti paslaugos teikėją pagal jo turimas technines galimybes:

i) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti arba

ii) bendradarbiauti su kompetentingomis institucijomis ir padėti jai surinkti arba įrašyti

realiuoju laiku turinio duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodamus naudojantis kompiuterine sistema.

2. Jeigu Šalis dėl savo teisinės sistemos principų negali taikyti šio straipsnio 1 dalies a punkte minimų priemonių, ji gali priimti tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad jos teritorijoje realiuoju laiku, naudojant technines priemones būtų surinkti ir įrašyti turinio duomenys, susiję su konkrečia toje teritorijoje perduodama informacija.

3. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įpareigojant paslaugos teikėją laikyti paslaptyje bet kurių šiame straipsnyje minimų įgaliojimų vykdymą ir bet kurią informaciją apie jų vykdymą.

4. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

3 skirsnis. Jurisdikcija

22 straipsnis. Jurisdikcija

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti nustatyti jurisdikciją šios Konvencijos 2–11 straipsniuose nurodytiems nusikaltimams, kai nusikaltimas padarytas:
   a) jos teritorijoje;
   b) laive, plaukiojančiame su tos Šalies vėliava;
   c) orlaivyje, įregistruotame pagal tos Šalies įstatymus;
   d) tos Šalies piliečio, jeigu padarius nusikaltimą yra baudžiama pagal baudžiamuosius įstatymus arba jeigu toks nusikaltimas yra padarytas už bet kurios valstybės teritorinės jurisdikcijos.
2. Kiekviena Šalis gali pasilikti teisę netaikyti arba tik tam tikrais atvejais arba tam tikromis aplinkybėmis taikyti jurisdikcijos taisykles, nustatytas šio straipsnio 1 dalies b–d punktuose, arba dalį šių taisyklių.
3. Kiekviena Šalis priima tokias priemones, kurių gali prireikti nustatyti jurisdikciją šios Konvencijos 24 straipsnio 1 dalyje nurodytiems nusikaltimams, kai įtariamasis yra jos teritorijoje ir ji, gavusi prašymą jį išduoti, kitai Šaliai jo neišduoda vien dėl jo pilietybės.
4. Ši Konvencija nepašalina jokios baudžiamosios jurisdikcijos, vykdomos pagal vidaus teisę.
5. Kai dėl tariamo nusikaltimo, nustatyto pagal šią Konvenciją, teisę į jurisdikciją pareiškia daugiau nei viena Šalis, tos Šalys prireikus tarpusavyje konsultuojasi siekdamos nustatyti labiausiai persekiojimui tinkamą jurisdikciją.

III SKYRIUS. TARPTAUTINIS BENDRADARBIAVIMAS

1 skirsnis. Bendrieji principai

1 dalis. Bendrieji tarptautinio bendradarbiavimo principai

23 straipsnis. Bendrieji tarptautinio bendradarbiavimo principai

Tirdamos nusikaltimus, susijusius su kompiuterinėmis sistemomis ir duomenimis, arba persekiodamos, arba rinkdamos nusikaltimo įrodymus elektroniniu pavidalu, Šalys kuo didesniu mastu bendradarbiauja tarpusavyje, vadovaudamosi šio skyriaus nuostatomis, taikydamos atitinkamus tarptautinius dokumentus dėl tarptautinio

bendradarbiavimo baudžiamosiose bylose, susitarimus, pagrįstus vienodais ar abipusiais teisės aktais, ir vidaus teisę.

2 dalis. Ekstradicijos principai

24 straipsnis. Ekstradicija

1. a) Šis straipsnis taikomas ekstradicijai tarp Šalių už nusikaltimus, nurodytus šios Konvencijos 2–11 straipsniuose, jeigu pagal abiejų susijusių Šalių įstatymus už tokius nusikaltimus baudžiama maksimalia, mažiausiai vienerių metų, laisvės atėmimo bausme arba griežtesne bausme.

   b) Kai pagal susitarimą, pagrįstą vienodais ar abipusiais teisės aktais, arba pagal ekstradicijos sutartį, taip pat pagal Europos konvenciją dėl ekstradicijos (ETS Nr. 24), taikomą tarp dviejų ar daugiau šalių, kitokia mažiausia bausmė būtų taikoma, tokia pagal tokį susitarimą ar sutartį mažiausia bausmė ir taikoma.

2. Šio straipsnio 1 dalyje apibūdinti nusikaltimai laikomi nusikaltimais, už kuriuos išduodama, visose sutartyse dėl ekstradicijos tarp dviejų ar daugiau Šalių. Šalys įsipareigoja tokius nusikaltimus kaip nusikaltimus, už kuriuos išduodama, įtraukti į visas sutartis dėl ekstradicijos, sudaromas tarp dviejų ar daugiau Šalių.

3. Jeigu Šalis, siejanti ekstradiciją su sutartimi, gauna prašymą dėl ekstradicijos iš kitos Šalies, su kuria nėra sudariusi sutarties dėl ekstradicijos, ji gali šią Konvenciją laikyti teisiniu pagrindu ekstradicijai už bet kurį nusikaltimą, nurodytą šio straipsnio 1 dalyje.

4. Šalys, nesiejančios ekstradicijos su sutartimi, šio straipsnio 1 dalyje minimus nusikaltimus tarpusavyje pripažįsta nusikaltimais, už kuriuos išduodama.

5. Ekstradicija vykdoma pagal prašomosios Šalies teisėje arba taikytinose ekstradicijos sutartyse nustatytas sąlygas, įskaitant pagrindus, kuriems esant prašomoji Šalis gali atsisakyti vykdyti ekstradiciją.

6. Jeigu asmenį, padariusį šio straipsnio 1 dalyje minimą nusikaltimą, atsisakoma išduoti vien dėl jo pilietybės arba dėl to, kad prašomoji Šalis mano, jog tas nusikaltimas priklauso jos jurisdikcijai, prašomoji Šalis prašančiosios Šalies prašymu perduoda bylą savo kompetentingoms institucijoms, kad jos vykdytų baudžiamąjį persekiojimą ir tinkamu laiku praneša prašančiajai Šaliai galutinį jo rezultatą. Šios institucijos priima sprendimą ir atlieka tyrimą bei bylos nagrinėjimą tokiu pat būdu, kaip ir panašiose baudžiamosiose bylose, sprendžiamose pagal tos Šalies teisę.

7. a) Nesant sutarties Šalys, pasirašydamos arba deponuodamos šios Konvencijos ratifikavimo, priėmimo, patvirtinimo arba prisijungimo prie jos dokumentus, Europos Tarybos Generaliniam Sekretoriui praneša kiekvienos institucijos, atsakingos už prašymo išduoti arba laikinai suimti asmenį pateikimą arba gavimą, pavadinimą ir adresus.

b) Europos Tarybos Generalinis Sekretorius sudaro ir atnaujina Šalių nurodytą institucijų registrą. Kiekviena Šalis pasirūpina, kad informacija registre visuomet būtų teisinga.

3 dalis. Bendrieji savitarpio pagalbos principai

25 straipsnis. Bendrieji savitarpio pagalbos principai

1. Atlikdamos tyrimą arba nagrinėdamos bylas dėl nusikaltimų, susijusių su kompiuterinėmis sistemomis ir duomenimis, arba rinkdamos nusikaltimo įrodymus elektroniniu pavidalu, Šalys teikia viena kitai didžiausią įmanomą pagalbą.
2. Kiekviena Šalis taip pat priima tokius teisės aktus ir tokias priemones, kurių gali prireikti 27–35 straipsniuose nustatytiems įsipareigojimams vykdyti.
3. Skubiais atvejais kiekviena Šalis gali perduoti savitarpio pagalbos arba su tuo susijusios informacijos prašymus operatyviomis ryšio priemonėmis, tarp jų faksimiliniu ryšiu arba elektroniniu paštu, jeigu tomis priemonėmis galima užtikrinti tinkamą informacijos saugumą bei autentiškumą (naudojant, kai tai reikalinga, šifravimą), ir prašomosios Šalies prašymu tokią informaciją oficialiai patvirtina. Prašomoji Šalis prašymą priima ir į jį atsako bet kuria tokia operatyvia ryšio priemone.
4. Jeigu šio skyriaus straipsniuose kitaip nenurodyta, savitarpio pagalba teikiama pagal prašomosios Šalies teisėje arba taikytinose savitarpio pagalbos sutartyse nustatytas sąlygas, įskaitant pagrindus, kuriems esant prašomoji Šalis gali atsisakyti bendradarbiauti. Prašomoji Šalis nesinaudoja teise atsisakyti teikti savitarpio pagalbą dėl 2–11 straipsniuose minimų nusikaltimų, remdamasi tiktai tuo, kad prašymas susijęs su nusikaltimu, kurį ji laiko finansiniu nusikaltimu.
5. Kai pagal šio skyriaus nuostatas prašomajai Šaliai leidžiama savitarpio pagalbos teikimą sieti su dvigubo baudžiamumo buvimu, tokia sąlyga laikoma įvykdyta, neatsižvelgiant į tai, ar jos įstatymai priskiria tą nusikaltimą tai pačiai nusikaltimų kategorijai ir vadina tais pačiais terminais, kaip ir prašančioji Šalis, jeigu sudarantis nusikaltimo pagrindą elgesys, dėl kurio prašoma pagalbos, pagal jos įstatymus yra nusikaltimas.

26 straipsnis. Savanoriškas informavimas

1. Kiekviena Šalis, kiek tai leidžia jos vidaus teisė, gali be ankstesnio prašymo perduoti kitai Šaliai informaciją, gautą per savo pačios atliekamus tyrimus, jeigu ji mano, kad tokios informacijos atskleidimas padėtų ją gavusiai Šaliai pradėti arba atlikti tyrimą ar nagrinėti bylas dėl pagal šią Konvenciją nustatytų nusikaltimų, arba paskatintų tą Šalį pagal šį skyrių pateikti prašymą bendradarbiauti.
2. Prieš teikdama tokią informaciją, teikiančioji Šalis gali prašyti, kad būtų išsaugotas jos konfidencialumas arba kad ji būtų naudojama tik nurodytomis

sąlygomis. Jeigu informaciją gaunanti Šalis negali įvykdyti tokio prašymo, ji apie tai praneša teikiančiajai Šaliai, kuri tada sprendžia, ar, nepaisant to, tokią informaciją teikti. Jeigu informaciją gaunanti Šalis sutinka, kad informacija būtų naudojama nurodytomis sąlygomis, ji privalo laikytis tų sąlygų.

4 dalis. Savitarpio pagalbos prašymų pateikimo tvarka, kai nėra taikytinų tarptautinių susitarimų

27 straipsnis. Savitarpio pagalbos prašymų pateikimo tvarka, kai nėra taikytinų tarptautinių susitarimų

1. Jeigu tarp prašančiosios ir prašomosios Šalių nėra savitarpio pagalbos sutarties arba susitarimo, pagrįsto vienodais ar abipusiais teisės aktais, taikomos šio straipsnio 2–9 dalių nuostatos. Jeigu tokia sutartis, susitarimas arba teisės aktai yra, šio straipsnio nuostatos netaikomos, nebent susijusios Šalys susitartų vietoj jų taikyti kurią nors arba visą likusią šio straipsnio dalį.
2. a) Kiekviena Šalis paskiria centrinę instituciją arba institucijas, atsakingas už savitarpio pagalbos prašymų ir atsakymų į juos siuntimą, tokių prašymų vykdymą arba jų perdavimą vykdyti kompetentingoms institucijoms.
   b) Centrinės institucijos vienos su kitomis bendradarbiauja tiesiogiai.
   c) Kiekviena Šalis, pasirašydama arba deponuodama šios Konvencijos ratifikavimo, priėmimo, patvirtinimo ar prisijungimo dokumentą, Europos Tarybos Generaliniam Sekretoriui praneša institucijų, paskirtų pagal šią straipsnio dalį, pavadinimus ir adresus.
   d) Europos Tarybos Generalinis Sekretorius sudaro ir atnaujina Šalių nurodytų centrinių institucijų registrą. Kiekviena Šalis pasirūpina, kad informacija registre visuomet būtų teisinga.
3. Pagal šį straipsnį siunčiami savitarpio pagalbos prašymai vykdomi prašančiosios Šalies nurodyta tvarka, išskyrus atvejus, kai ji nesuderinama su prašomosios Šalies teise.
4. Be 25 straipsnio 4 dalyje išvardytų atsisakymo pagrindų, prašomoji Šalis gali atsisakyti teikti pagalbą, jeigu:
   a) prašymas susijęs su nusikaltimu, kurį prašomoji Šalis laiko politiniu nusikaltimu arba nusikaltimu, susijusiu su politiniu nusikaltimu;
   b) ta Šalis mano, kad prašymo vykdymas pakenktų jos suverenumui, saugumui, viešajai tvarkai arba kitiems svarbiems interesams.
5. Prašomoji Šalis gali atidėti prašymo vykdymą, jeigu jį vykdant būtų pakenkta jos institucijų atliekamam nusikaltimų tyrimui arba bylų nagrinėjimui.
6. Prieš atsakydama teikti pagalbą arba atidėdama jos teikimą prašomoji Šalis, kai reikia, pasitarusi su prašančiąja Šalimi, apsvarsto galimybę patenkinti prašymą iš dalies arba tokiomis sąlygomis, kokias ji laiko reikalingomis.

7. Prašomoji Šalis nedelsdama informuoja prašančiąją Šalį apie pagalbos prašymo vykdymo rezultatą. Jeigu prašymą atsisakoma vykdyti arba jo vykdymas atidedamas, nurodomos to nevykdymo arba atidėjimo priežastys. Prašomoji Šalis taip pat informuoja prašančiąją Šalį apie priežastis, dėl kurių neįmanoma įvykdyti prašymo arba dėl kurių jo vykdymas gali būti labai uždelstas.
8. Prašančioji Šalis gali prašyti, kad prašomoji Šalis išsaugotų pagal šio skyriaus nuostatas pateikto prašymo ir jo turinio konfidencialumą tiek, kiek to reikia prašymui vykdyti. Jeigu prašomoji Šalis negali patenkinti konfidencialumo sąlygos, ji nedelsdama apie tai praneša prašančiajai Šaliai, kuri tada sprendžia, ar prašymą vis dėlto reikėtų vykdyti.
9. a) Skubiu atveju savitarpio pagalbos ar su ja susijusios informacijos prašymus prašančiosios Šalies teisminės institucijos gali siųsti tiesiogiai tokioms prašomosios Šalies institucijoms. Tokiais atvejais kopija tuo pačiu metu per prašančiosios Šalies centrinę instituciją yra siunčiama prašomosios Šalies centrinei institucijai.

   b) Šioje straipsnio dalyje minimi prašymai arba pranešimai gali būti perduodami per Tarptautinę kriminalinės policijos organizaciją (Interpolą).

   c) Kai prašymas pateikiamas pagal šios straipsnio dalies a punktą, o institucija neturi įgaliojimų jį nagrinėti, ji perduoda prašymą kompetentingai nacionalinei institucijai ir apie tai tiesiogiai informuoja prašančiąją Šalį.

   d) Jeigu šioje straipsnio dalyje minimi prašymai arba pranešimai nėra susiję su prievartos priemonėmis, juos kompetentinga prašančiosios Šalies institucija tiesiogiai perduoda kompetentingai prašomosios Šalies institucijai.

   e) Kiekviena Šalis, pasirašydama arba deponuodama šios Konvencijos ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumentus, Europos Tarybos Generaliniam Sekretoriui gali pranešti, kad, siekiant didesnio veiksmingumo, šioje straipsnio dalyje minimi prašymai turi būti siunčiami jos centrinei institucijai.

28 straipsnis. Konfidencialumas ir informacijos naudojimo apribojimas

1. Jeigu tarp prašančiosios ir prašomosios Šalių nėra savitarpio pagalbos sutarties arba susitarimo, pagrįsto vienodais ir abipusiais teisės aktais, taikomos šio straipsnio nuostatos. Jeigu tokia sutartis, susitarimas arba teisės aktai yra, šio straipsnio nuostatos netaikomos, nebent Šalys susitartų vietoj jų taikyti kurią nors arba visą likusią šio straipsnio dalį.
2. Atsakydama į prašymą suteikti informaciją arba medžiagą, prašomoji Šalis gali nustatyti sąlygą, kad:

   a) būtų išsaugomas jos konfidencialumas tais atvejais, kai savitarpio teisinės pagalbos prašymas negalėtų būti vykdomas nesant tokios sąlygos;

b) ji būtų naudojama tik prašyme nurodytam tyrimui arba bylų nagrinėjimui.

3. Jeigu prašančioji Šalis negali įvykdyti šio straipsnio 2 dalyje minimos sąlygos, ji apie tai nedelsdama praneša kitai Šaliai, kuri tada sprendžia, ar, nepaisant to, teikti tokią informaciją. Jeigu prašančioji Šalis sutinka su tokia sąlyga, ji privalo jos laikytis.
4. Kiekviena Šalis, kuri teikia informaciją arba medžiagą laikydamasi šio straipsnio 2 dalyje minimos sąlygos, gali, remdamasi ta sąlyga, paprašyti kitą Šalį paaiškinti, kam tokia informacija arba medžiaga reikalinga.

2 skirsnis. Specialiosios nuostatos

1 dalis. Savitarpio pagalba dėl laikinųjų priemonių

29 straipsnis. Operatyvus laikomųjų kompiuterinių duomenų išsaugojimas

1. Šalis gali prašyti kitą Šalį nurodyti operatyviai išsaugoti duomenis, laikomus kompiuterinėje sistemoje, kuri yra tos kitos Šalies teritorijoje ir dėl kurios prašančioji Šalis ketina pateikti savitarpio pagalbos prašymą, susijusį su tokių duomenų paieška arba panašia prieiga, areštu ar panašiu poėmiu arba su jų atskleidimu, arba prašyti kitaip pasirūpinti tokių duomenų išsaugojimu.
2. Pagal šio straipsnio 1 dalį pateikiamame prašyme išsaugoti duomenis nurodoma:
   a) išsaugoti duomenis prašanti institucija;
   b) nusikaltimas, dėl kurio atliekamas tyrimas arba vyksta procesas, ir trumpas susijusių faktų apibendrinimas;
   c) išsaugotini laikomieji kompiuteriniai duomenys ir jų sąsaja su nusikaltimu;
   d) bet kuri turima informacija, leidžianti nustatyti laikomųjų kompiuterinių duomenų saugotoją arba kompiuterinės sistemos vietą;
   e) būtinybė išsaugoti duomenis;
   f) Šalies ketinimas pateikti savitarpio pagalbos prašymą, susijusį su laikomųjų kompiuterinių duomenų paieška arba panašia prieiga, areštu ar panašiu poėmiu arba su jų atskleidimu.
3. Gavusi kitos Šalies prašymą, prašomoji Šalis imasi visų reikalingų priemonių, kad, vadovaudamasi savo vidaus teise, operatyviai išsaugotų nurodytus duomenis. Atsakant į prašymą, nereikalaujama dvigubo baudžiamumo, kaip tokio išsaugojimo sąlygos.
4. Šalis, kuri atsakymą į savitarpio pagalbos prašymą, susijusį su duomenų paieška arba panašia prieiga, areštu ar panašiu poėmiu arba su jų atskleidimu, sieja su dvigubo baudžiamumo sąlyga, gali nusikaltimų, išskyrus nurodytuosius

šios Konvencijos 2–11 straipsniuose, atžvilgiu pasilikti teisę atmesti pagal šį straipsnį pateiktą prašymą išsaugoti duomenis, kai ji turi pagrindo manyti, kad atskleidimo metu dvigubo baudžiamumo sąlyga negali būti įvykdyta.

5. Be to, prašymas dėl išsaugojimo gali būti atmestas, tik jeigu:
   a) prašymas pateiktas dėl nusikaltimo, kurį prašomoji Šalis laiko politiniu nusikaltimu arba nusikaltimu, susijusiu su politiniu nusikaltimu;
   b) prašomoji Šalis mano, kad prašymo vykdymas galėtų pakenkti jos suverenumui, saugumui, viešajai tvarkai arba kitiems svarbiems interesams.
6. Jeigu prašomoji Šalis mano, kad išsaugojimas neužtikrins duomenų prieinamumo ateityje arba sukels pavojų prašančiosios Šalies tyrimo konfidencialumui ar kitaip jam pakenks, ji nedelsdama apie tai praneša prašančiajai Šaliai, kuri tada sprendžia, ar prašymą vis dėlto reikėtų vykdyti.
7. Atsakant į šio straipsnio 1 dalyje minimą prašymą, duomenys išsaugojami ne mažiau kaip 60 dienų, kad prašančioji Šalis galėtų pateikti prašymą dėl duomenų paieškos arba panašios prieigos, arešto ar panašaus poėmio arba dėl jų atskleidimo. Gavus tokį prašymą, tokie duomenys saugojami iki sprendimo dėl prašymo priėmimo.

30 straipsnis. Operatyvus išsaugotų srauto duomenų atskleidimas

1. Jeigu vykdydama pagal 29 straipsnį pateiktą prašymą išsaugoti srauto duomenis, susijusius su tam tikra informacija, prašomoji Šalis sužino, kad su šios informacijos perdavimu yra susijęs kitoje valstybėje esantis paslaugos teikėjas, ji operatyviai atskleidžia prašančiajai Šaliai pakankamai srauto duomenų, leidžiančių nustatyti paslaugos teikėją ir tos informacijos perdavimo kelią.
2. Atsisakyti atskleisti srauto duomenis pagal šio straipsnio 1 dalį galima tik tais atvejais, kai:
   a) prašymas pateiktas dėl nusikaltimo, kurį prašomoji Šalis laiko politiniu nusikaltimu arba nusikaltimu, susijusiu su politiniu nusikaltimu;
   b) prašomoji Šalis mano, kad prašymo vykdymas galėtų pakenkti jos suverenumui, saugumui, viešajai tvarkai arba kitiems svarbiems interesams.

2 dalis. Savitarpio pagalba atliekant tyrimą

31 straipsnis. Savitarpio pagalba dėl laikomųjų kompiuterių duomenų prieigos

1. Šalis gali pateikti kitai Šaliai prašymą dėl duomenų, laikomų kompiuterinėje sistemoje, kuri yra prašomosios Šalies teritorijoje, paieškos arba panašios

prieigos, arešto ar panašaus poėmio ir atskleidimo, taip pat ir dėl duomenų, kurie buvo išsaugoti pagal 29 straipsnį.

2. Atsakydama į prašymą, prašomoji Šalis vadovaujasi tarptautiniais dokumentais, susitarimais ir įstatymais, nurodytais 23 straipsnyje, ir atitinkamomis šio skyriaus nuostatomis.
3. Į prašymą operatyviai atsakoma tais atvejais, kai:
   a) yra pagrindo manyti, kad reikalingi duomenys gali būti nesunkiai prarasti arba pakeisti;
   b) operatyvus bendradarbiavimas yra numatytas šio straipsnio 2 dalyje nurodytuose dokumentuose, susitarimuose ir įstatymuose.

32 straipsnis. Tarptautinė laikomųjų kompiuterių duomenų prieiga gavus sutikimą arba esant viešajai prieigai

Kiekviena Šalis be oficialaus kitos Šalies leidimo gali:

a) prieiti prie viešai prieinamų (atviras šaltinis) laikomųjų kompiuterinių duomenų, kad ir kokioje geografinėje vietoje jie būtų;
b) per savo teritorijoje esančią kompiuterinę sistemą prieiti prie laikomųjų kompiuterių duomenų, esančių kitoje Šalyje, arba gauti tuos duomenis, jeigu ta Šalis gauna asmens, teisiškai įgalioto per tokią kompiuterių sistemą atskleisti tai Šaliai tokius duomenis, teisėtą ir sąmoningą sutikimą.

33 straipsnis. Savitarpio pagalba, teikiama dėl srauto duomenų rinkimo realiuoju laiku

1. Šalys teikia savitarpio pagalbą realiuoju laiku renkant srauto duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterine sistema. Atsižvelgiant į šio straipsnio 2 dalies nuostatas, pagalba teikiama laikantis šalies vidaus teisėje nustatytos tvarkos ir sąlygų.
2. Kiekviena Šalis tokią pagalbą teikia bent tų baudžiamųjų nusikaltimų atvejais, kai srauto duomenys realiuoju laiku būtų renkami toje valstybėje nagrinėjamose panašiose bylose.

34 straipsnis. Savitarpio pagalba, teikiama dėl turinio duomenų perimties

Šalys teikia savitarpio pagalbą realiuoju laiku renkant arba įrašant turinio duomenis, susijusius su konkrečia informacija, perduodama kompiuterine sistema, kiek tai leidžia jų taikytinos sutartys ir vidaus įstatymai.

3 dalis. 24/7 tinklas

35 straipsnis. 24/7 tinklas

1. Kad būtų galima teikti skubią pagalbą tyrimui ar bylų nagrinėjimui, susijusiems su nusikaltimais kompiuterinėms sistemoms ir duomenims, arba nusikaltimo įrodymų rinkimui elektroniniu pavidalu, kiekviena Šalis paskiria ryšio punktą, veikiantį visą parą 7 dienas per savaitę. Be kita ko, tokia pagalba apima toliau išvardytų dalykų palengvinimą arba, jeigu tai leidžia valstybės vidaus teisė ir praktika, tiesiogiai:
   a) techninių konsultacijų teikimą;
   b) duomenų išsaugojimą pagal 29 ir 30 straipsnius;
   c) įrodymų rinkimą, teisinės informacijos teikimą ir įtariamųjų buvimo vietos nustatymą.
2. a) Šalies ryšio punktas turi galimybę palaikyti operatyvų ryšį su kitos Šalies ryšio punktu.
   b) Jeigu Šalies paskirtas ryšio punktas nėra tos Šalies institucijos arba institucijų, atsakingų už tarptautinę savitarpio pagalbą arba ekstradiciją, dalis, toks ryšio punktas pasirūpina, kad galėtų operatyviai bendradarbiauti su tokia institucija arba institucijomis.
3. Kad palengvintų tinklo darbą, kiekviena Šalis parūpina apmokytą personalą ir įrangą jam.

IV SKYRIUS. BAIGIAMOSIOS NUOSTATOS

36 straipsnis. Pasirašymas ir įsigaliojimas

1. Šią Konvenciją gali pasirašyti Europos Tarybos valstybės narės ir prie jos rengimo prisidėjusios valstybės, kurios nėra narės.
2. Ši Konvencija turi būti ratifikuojama, priimama arba patvirtinama. Ratifikavimo, priėmimo arba patvirtinimo dokumentai deponuojami Europos Tarybos Generaliniam Sekretoriui.
3. Ši Konvencija įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai penkios valstybės, tarp jų ne mažiau kaip trys Europos Tarybos narės, pagal šio straipsnio 1 ir 2 dalis pareiškė sutikimą įsipareigoti pagal šią Konvenciją.
4. Kiekvienai šią Konvenciją pasirašiusiai valstybei, kuri vėliau pareiškė sutikimą įsipareigoti pagal ją, Konvencija įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai ji pagal šio straipsnio 1 ir 2 dalis pareiškia sutikimą įsipareigoti pagal šią Konvenciją.

37 straipsnis. Prisijungimas prie Konvencijos

1. Šiai Konvencijai įsigaliojus, Europos Tarybos Ministrų Komitetas, pasikonsultavęs su šios Konvencijos Susitariančiosiomis Šalimis ir gavęs vieningą jų sutikimą, gali pakviesti bet kurią valstybę, kuri nėra Tarybos narė ir neprisidėjo prie šios Konvencijos rengimo, prisijungti prie jos. Sprendimas priimamas pritarus Europos Tarybos statuto 20 straipsnio d punkte nustatytai daugumai ir vieningai balsavus Susitariančiųjų Šalių atstovams, kurie yra teisėti Ministrų Komiteto nariai.
2. Ši Konvencija prie jos pagal šio straipsnio 1 dalį prisijungusiai valstybei įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai Europos Tarybos Generaliniam Sekretoriui deponuojamas prisijungimo dokumentas.

38 straipsnis. Teritorinis taikymas

1. Kiekviena valstybė pasirašymo metu arba deponuodama savo ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumentą, gali nurodyti teritoriją arba teritorijas, kurioms ši Konvencija taikoma.
2. Kiekviena valstybė bet kada vėliau gali Europos Tarybos Generaliniam Sekretoriui adresuotu pareiškimu išplėsti šios Konvencijos taikymą bet kuriai kitai tame pareiškime nurodytai teritorijai. Tokiai teritorijai Konvencija įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai Generalinis Sekretorius gauna tokį pareiškimą.
3. Kiekvienas pareiškimas pagal dvi pirmesnes šio straipsnio dalis kiekvienai tokiame pareiškime nurodytai teritorijai gali būti atšauktas Europos Tarybos Generaliniam Sekretoriui adresuotu pranešimu. Atšaukimas įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai Generalinis Sekretorius gauna tokį pranešimą.

39 straipsnis. Konvencijos galiojimas

1. Šios Konvencijos tikslas – papildyti taikytinas daugiašales ir dvišales Šalių sutartis bei susitarimus, tarp jų:
   - Europos konvenciją dėl ekstradicijos, pateiktą pasirašyti 1957 m. gruodžio 13 d. Paryžiuje (ETS Nr. 24);
   - Europos konvenciją dėl savitarpio pagalbos baudžiamosiose bylose, pateiktą pasirašyti 1959 m. balandžio 20 d. Strasbūre (ETS Nr. 30);
   - Europos konvencijos dėl savitarpio pagalbos baudžiamosiose bylose papildomą protokolą, pateiktą pasirašyti 1978 m. kovo 17 d. Strasbūre (ETS Nr. 99).
2. Jeigu dvi ar daugiau Šalių jau yra sudariusios susitarimą arba sutartį šios Konvencijos reglamentuojamais klausimais arba kitaip nustačiusios savo

santykius šioje srityje, arba tai padarytų ateityje, jos taip pat turi teisę taikyti tą susitarimą arba sutartį ir pagal juos reglamentuoti savo santykius. Tačiau jeigu šios Konvencijos reglamentuojamais klausimais Šalys nustato savo santykius kitaip, nei jie reglamentuojami šioje Konvencijoje, jos privalo juos tvarkyti taip, kad jie neprieštarautų šios Konvencijos tikslams ir nuostatoms.

3. Ši Konvencija niekaip nekeičia kitų Šalies teisių, apribojimų, pareigų ir įsipareigojimų.

40 straipsnis. Pareiškimai

Kiekviena valstybė pasirašydama šią Konvenciją arba deponuodama savo ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumentą gali Europos Tarybos Generaliniam Sekretoriui adresuotu rašytiniu pranešimu pareikšti, kad ji pasilieka teisę reikalauti papildomų sąlygų, kaip nustatyta 2 ir 3 straipsniuose, 6 straipsnio 1 dalies b punkte, 7 straipsnyje, 9 straipsnio 3 dalyje ir 27 straipsnio 9 dalies e punkte.

41 straipsnis. Konvencijos galiojimas federacinėje valstybėje

1. Federacinė valstybė gali pasilikti teisę prisiimti įsipareigojimus pagal šios Konvencijos II skyrių, neprieštaraujančius pagrindiniams principams, kuriais grindžiami santykiai tarp jos centrinės vyriausybės ir ją sudarančių valstybių ar kitų panašių teritorinių vienetų, jeigu ji tebėra pasirengusi bendradarbiauti pagal III skyrių.
2. Darydama šio straipsnio 1 dalyje nurodytą išlygą, federacinė valstybė gali netaikyti tokių šios išlygos sąlygų, kurios atmeta arba iš esmės sumažina jos įsipareigojimus imtis II skyriuje nurodytų priemonių. Apskritai ji plačiai ir veiksmingai užtikrina šių priemonių vykdymą.
3. Apie tas Konvencijos nuostatas, kurių taikymas priklauso federaciją sudarančių valstybių arba panašių teritorinių vienetų, pagal jos konstituciją neįpareigotų vykdyti įstatymų leidybos funkcijų, jurisdikcijai, federacijos vyriausybė informuoja kompetentingas tokių valstybių institucijas, palankiai vertindama tokias nuostatas ir skatindama tokias valstybes imtis tinkamų veiksmų joms įgyvendinti.

42 straipsnis. Išlygos

Kiekviena valstybė pasirašydama šią Konvenciją arba deponuodama savo ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumentą, gali Europos Tarybos Generaliniam Sekretoriui adresuotu rašytiniu pranešimu pareikšti, kad ji pasilieka teisę daryti 4 straipsnio 2 dalyje, 6 straipsnio 3 dalyje, 9 straipsnio 4 dalyje, 10 straipsnio 3 dalyje, 11 straipsnio 3 dalyje, 14 straipsnio 3 dalyje, 22 straipsnio 2 dalyje, 29 straipsnio 4 dalyje ir 41 straipsnio 1 dalyje nurodytas išlygas. Jokių kitų išlygų daryti negalima.

43 straipsnis. Išlygų statusas ir atšaukimas

1. Šalis, padariusi 42 straipsnyje nurodytą išlygą, gali Generaliniam Sekretoriui adresuotu pranešimu visai arba iš dalies ją atšaukti. Toks atšaukimas įsigalioja nuo tos dienos, kai Generalinis Sekretorius gauna tokį pranešimą. Jeigu pranešime nurodoma, jog išlyga atšaukiama nuo jame nustatytos datos ir tokia data yra vėlesnė nei ta, kai pranešimą gauna Generalinis Sekretorius, išlygos atšaukimas įsigalioja vėlesnę dieną.
2. Kai tik leidžia aplinkybės, Šalis, padariusi 42 straipsnyje nurodytą išlygą, visai arba iš dalies ją atšaukia.
3. Europos Tarybos Generalinis Sekretorius periodiškai klausia Šalių, padariusių vieną ar daugiau 42 straipsnyje nurodytų išlygų, apie galimybę tokią išlygą arba išlygas atšaukti.

44 straipsnis. Pakeitimai

1. Kiekviena Šalis gali siūlyti šios Konvencijos pakeitimus, apie kuriuos Europos Tarybos Generalinis Sekretorius praneša Europos Tarybos valstybėms narėms, prie šios Konvencijos rengimo prisidėjusioms valstybėms, kurios nėra narės, ir valstybėms, pagal šios Konvencijos 37 straipsnį prisijungusioms arba pakviestoms prisijungti prie jos.
2. Apie kiekvieną Šalies siūlomą pakeitimą pranešama Europos nusikalstamumo problemų komitetui (CDPC), kuris savo nuomonę dėl siūlomo pakeitimo perduoda Ministrų Komitetui.
3. Ministrų Komitetas apsvarsto siūlomą pakeitimą bei Europos nusikalstamumo problemų komiteto (CDPC) pateiktą nuomonę ir, pasikonsultavęs su nepriklausančioms Europos Tarybai Konvencijos Šalimis, gali tokį pakeitimą priimti.
4. Kiekvieno pakeitimo tekstas, Ministrų Komiteto priimtas pagal šio straipsnio 3 dalį, perduodamas Šalims, kad jos pareikštų sutikimą.
5. Kiekvienas pakeitimas, priimtas pagal šio straipsnio 3 dalį, įsigalioja praėjus trisdešimčiai dienų nuo tos dienos, kai visos Šalys Generaliniam Sekretoriui pareiškia savo sutikimą.

45 straipsnis. Ginčų sprendimas

1. Europos nusikalstamumo problemų komitetas (CDPC) yra nuolat informuojamas apie šios Konvencijos aiškinimą ir taikymą.
2. Tarp Šalių kilus ginčui dėl šios Konvencijos aiškinimo arba taikymo, jos stengiasi ginčą išspręsti derybomis arba kitomis taikiomis joms priimtinomis ginčų sprendimo priemonėmis, be kita ko, pateikdamos ginčą Europos nusikalstamumo problemų komitetui (CDPC), arbitražiniam teismui, kurio

sprendimai Šalims privalomi, arba Tarptautiniam Teisingumo Teismui, jei Šalys taip susitarė.

46 straipsnis. Šalių konsultacijos

1. Prireikus Šalys periodiškai konsultuojasi, kad palengvintų:
   a) veiksmingą šios Konvencijos taikymą ir vykdymą, taip pat dėl to kylančių problemų ir pagal šia Konvenciją padarytų pareiškimų arba išlygų poveikio nustatymą;
   b) keitimąsi informacija apie svarbius teisės, politikos arba technikos pokyčius, susijusius su elektroniniais nusikaltimais ir įrodymų rinkimu elektroniniu pavidalu;
   c) galimų Konvencijos papildymų arba pakeitimų svarstymą.
2. Europos nusikalstamumo problemų komitetas (CDPC) periodiškai informuojamas apie šio straipsnio 1 dalyje minimų konsultacijų rezultatus.
3. Europos nusikalstamumo problemų komitetas (CDPC) prireikus tarpininkauja šio straipsnio 1 dalyje minimose konsultacijose ir imasi reikalingų priemonių, kad padėtų Šalims papildyti arba iš dalies pakeisti šią Konvenciją. Ne vėliau kaip praėjus trejiems metams nuo šios Konvencijos įsigaliojimo Europos nusikalstamumo problemų komitetas (CDPC), bendradarbiaudamas su Šalimis, persvarsto visas Konvencijos nuostatas ir, jei būtina, siūlo atitinkamus pakeitimus.
4. Išskyrus atvejus, kai išlaidas padengia Europos Tarybos, šio straipsnio 1 dalies nuostatų vykdymo išlaidas Šalys padengia jų sutartu būdu.
5. Vykdyti pagal šį straipsnį nustatytas funkcijas Šalims padeda Europos Tarybos Sekretoriatas.

47 straipsnis. Denonsavimas

1. Kiekviena Šalis bet kada Europos Tarybos Generaliniam Sekretoriui adresuotu pranešimu gali denonsuoti šią Konvenciją.
2. Toks denonsavimas įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai Generalinis Sekretorius gauna pranešimą.

48 straipsnis. Pranešimas

Europos Tarybos Generalinis Sekretorius Europos Tarybos valstybėms narėms, valstybėms, prisidėjusioms prie šios Konvencijos rengimo, kurios nėra narės, ir visoms valstybėms, prisijungusioms arba pakviestoms prie jos prisijungti, praneša apie:

   a) kiekvieną pasirašymą;
   b) kiekvieno ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumento deponavimą;

c) kiekvieną šios Konvencijos įsigaliojimo pagal 36 ir 37 straipsnius datą;

d) kiekvieną pagal 40 straipsnį padarytą pareiškimą arba pagal 42 straipsnį padarytą išlygą;

e) bet kurį kitą veiksmą, pranešimą arba informaciją, susijusią su šia Konvencija.

Tai paliudydami, toliau nurodyti tinkamai įgalioti asmenys pasirašė šią Konvenciją.

Priimta 2001 m. lapkričio 23 d. Budapešte anglų ir prancūzų kalbomis, abu tekstai yra autentiški, vienu egzemplioriumi, kuris deponuojamas Europos Tarybos archyvuose. Europos Tarybos Generalinis Sekretorius patvirtintas kopijas siunčia kiekvienai Europos Tarybos valstybei narei, prie šios Konvencijos rengimo prisidėjusioms valstybėms, kurios nėra valstybės narės, ir kiekvienai prie šios Konvencijos prisijungti pakviestai valstybei.

EUROPOS BENDRIJŲ KOMISIJA

Briuselis, 30.3.2009

KOM(2009) 149
galutinis

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI BEI 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}

(pateikta Komisijos)

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI BEI REGIONŲ KOMITETUI

dėl ypatingos svarbos informacinės infrastruktūros apsaugos

„Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“

1. Įžanga

Mūsų kasdienis gyvenimas vis labiau susijęs su informacinėmis ir komunikacinėmis technologijomis (IKT). Europos ekonomikai ir visuomenei gyvybiškai svarbios kai kurios iš tų IKT sistemų, paslaugų, tinklų ir infrastruktūros objektų (trumpai tariant, IKT infrastruktūros objektų), nes jos naudojamos teikti būtiniausias prekes ir paslaugas arba yra kitų ypatingos svarbos infrastruktūros objektų laikančioji konstrukcija. Paprastai jos laikomos ypatingos svarbos informacinės infrastruktūros objektais[251], nes jeigu jos būtų sugadintos arba sunaikintos, tai turėtų sunkių pasekmių gyvybiškai svarbioms visuomenės funkcijoms. Naujausi pavyzdžiai: 2007 m. didelio masto kibernetiniai Estijos antpuoliai, 2008 m. įvykę incidentai, kai buvo nutraukti tarpžemyniniai kabeliai.

2008 m. Pasaulio ekonomikos forume apskaičiuota, kad ypatingos svarbos informacinės infrastruktūros avarijos, kuri pasaulio ūkiui kainuotų apytiksliai 250 mlrd. JAV dolerių[252], tikimybė per artimiausią dešimtmetį yra 10–20 %.

Šiame komunikate daugiausiai dėmesio skirta prevencijai, parengčiai bei informavimui ir sudarytas neatidėliotinų veiksmų planas, kaip didinti ypatingos svarbos informacinės infrastruktūros objektų saugumą ir atsparumą. Tokie tikslai dera su Tarybos ir Europos Parlamento prašymu pradėta diskusija, kurioje siekiama išnagrinėti sudėtingus tinklų ir informacijos saugumo politikos uždavinius bei prioritetus ir nutarti, kokių priemonių dėl tų uždavinių ir prioritetų reikia ES lygmeniu. Be to, pasiūlytais veiksmais papildomi veiksmai, kuriais siekiama užkirsti kelią prieš ypatingos svarbos informacinės infrastruktūros objektus nukreiptai nusikalstamai ir teroristinei veiklai, su ja kovoti ir už ją persekioti baudžiamąja tvarka, ir užtikrinama sąveika su dabartinėmis bei būsimomis tinklų ir informacijos saugumo ES mokslinių tyrimų pastangomis ir su tarptautinėmis šios srities iniciatyvomis.

2. Politinės aplinkybės

Komisija formuoja Europos politiką siekdama didesnio informacinės visuomenės

[251] Ypatingos svarbos informacinės infrastruktūros objektų apibrėžtis pasiūlyta COM (2005) 576 (galutinis).
[252] *Global Risks 2008* (2008 m. pasaulinių grėsmių ataskaita).

saugumo ir pasitikėjimo ja. Dar 2005 m. Komisija[253] pabrėžė neatidėliotiną poreikį koordinuoti pastangas, kad suinteresuotosios šalys labiau pasitikėtų ir pasikliautų elektroniniu ryšiu bei paslaugomis. Tuo tikslu 2006 m. priimta saugios informacinės visuomenės strategija[254]. Pagrindiniams jos elementams, įskaitant IKT infrastruktūros objektų saugumą ir atsparumą, pritarta Tarybos rezoliucijoje 2007/068/01. Tačiau vien suinteresuotųjų šalių atsakomybės ir jų įgyvendinimo veiksmų nepakanka. Be to, šioje strategijoje taktiniu ir veiklos lygmenimis sustiprinamas Europos tinklų ir informacijos apsaugos agentūros (ENISA) vaidmuo; šios 2004 m. įsteigtos agentūros uždavinys – padėti užtikrinti aukšto ir veiksmingo lygio tinklo ir informacijos saugumą Bendrijoje ir formuoti ES piliečiams, vartotojams, įmonėms ir valdžios institucijoms naudingą tinklo ir informacijos saugumo kultūrą.

2008 m. ENISA įgaliojimai tokiomis pačiomis sąlygomis pratęsti iki 2012 m. kovo mėn.[255] Tuo pat metu Taryba ir Europos Parlamentas paragino toliau tęsti diskusijas dėl ENISA ateities ir dėl bendros Europos pastangų krypties siekiant didesnio tinklų ir informacijos saugumo. Kad šioms diskusijoms suteiktų pagrindą, praėjusį lapkritį Komisija pradėjo viešąsias konsultacijas[256] internetu, kurių analizė bus paskelbta netrukus.

Šiame komunikate numatyta veikla vykdoma pagal Europos programą dėl ypatingos svarbos infrastruktūros objektų apsaugos (EPCIP)[257] ir lygiagrečiai su ta programa. Vienas iš pagrindinių EPCIP elementų yra direktyva[258] dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems[259], kurioje nurodyta, kad pirmenybė ateityje bus teikiama informacinių ir komunikacinių technologijų sektoriui. Kitas svarbus EPCIP elementas – ypatingos svarbos infrastruktūros objektų įspėjimo informacinis tinklas (CIWIN)[260].

Komisijos pasiūlyme pertvarkyti elektroninio ryšio tinklų ir paslaugų teisinio reguliavimo sistemą[261] pateikta naujų reglamentavimo srities nuostatų dėl saugumo ir vientisumo, visų pirma, kad būtų sugriežtinti operatorių įpareigojimai užtikrinti, kad imtasi tinkamų priemonių apsisaugoti nuo nustatytų grėsmių, garantuoti nepertraukiamą paslaugos teikimą ir pranešti apie saugumo pažeidimus[262]. Toks metodas padės siekti bendrojo tikslo – padidinti ypatingos svarbos informacinės infrastruktūros objektų saugumą ir atsparumą. Šias nuostatas visapusiškai remia Europos Parlamentas ir Taryba.

Šiame komunikate pasiūlytais veiksmais papildomos šiuo metu taikomos ir numatomos policijos ir teisminio bendradarbiavimo srities priemonės, kuriomis siekiama užkirsti kelią prieš IKT infrastruktūros objektus nukreiptai nusikalstamai ir

[253] COM (2005) 229.
[254] COM (2006) 251.
[255] Reglamentas (EB) Nr. 1007/2008.
[256] http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
[257] COM (2006) 786 galutinis.
[258] 2008/114/EB.
[259] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf
[260] COM (2008) 676 galutinis.
[261] COM (2007) 697, COM (2007) 698, COM (2007) 699.
[262] Pagrindų direktyvos 13 straipsnis.

teroristinei veiklai, su ja kovoti ir už ją persekioti baudžiamąja tvarka, kaip numatyta, *inter alia*, Tarybos Pamatiniame sprendime dėl atakų prieš informacines sistemas[263] ir numatomame atnaujintame sprendime[264].

Šioje iniciatyvoje atsižvelgta į NATO veiklą bendrosios kibernetinės gynybos politikos srityje, t. y. į Kibernetinės gynybos valdymo instituciją ir į Bendros kibernetinės gynybos mokymo centrą.

Galiausiai tinkamai atsižvelgta į tarptautinius politinius įvykius, visų pirma į G8 grupės valstybių ypatingos svarbos informacinės infrastruktūros objektų apsaugos[265] principus; į Jungtinių Tautų Generalinės Asamblėjos rezoliuciją 58/199 dėl pasaulinės kibernetinio saugumo kultūros sukūrimo ir ypatingos svarbos informacinės infrastruktūros objektų apsaugos (angl. *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*) ir į neseniai paskelbtą Ekonominio bendradarbiavimo ir plėtros organizacijos rekomendaciją dėl ypatingos svarbos informacinės infrastruktūros objektų apsaugos.

3. Kuo rizikuojama?

3.1. Ypatingos svarbos informacinės infrastruktūros objektai gyvybiškai būtini ES ekonomikos ir visuomenės plėtrai

IKT sektoriaus ir IKT infrastruktūros objektų ekonominė ir visuomeninė svarba akcentuojama pastarojo meto inovacijų ir ekonomikos plėtros ataskaitose. Štai keli tokie dokumentai: Komunikatas dėl i2010 laikotarpio vidurio peržiūros[266], E. Aho grupės ataskaita[267] ir metinės Europos Sąjungos ekonomikos atskaitos[268]. Ekonominio bendradarbiavimo ir plėtros organizacija pabrėžia informacinių ir komunikacinių technologijų ir interneto svarbą siekiant gerinti ekonominės veiklos rodiklius bei didinti socialinę gerovę ir užtikrinti didesnį visuomenės pajėgumą gerinti piliečių gyvenimo kokybę visame pasaulyje[269]. Ji taip pat siūlo politiką pasitikėjimui interneto infrastruktūra stiprinti.

IKT sektorius gyvybiškai svarbus visai visuomenei. Nuo IKT sektoriaus priklauso verslo įmonių tiesioginis pardavimas ir vidaus procesų efektyvumas. Informacinės ir komunikacinės technologijos yra esminė inovacijų sudedamoji dalis, jų taikymas lemia 40 % našumo augimo[270]. Daug informacinių ir komunikacinių technologijų naudojama vyriausybių ir viešojo valdymo įstaigų darbui: visais lygiais diegiant e. valdžios paslaugas ir naują taikomąją programinę įrangą, pavyzdžiui, naujoviškus su sveikata, energetika ir dalyvavimu politikoje susijusius sprendimus, viešasis sektorius tampa vis labiau priklausomas nuo informacinių ir komunikacinių technologijų. Galiausiai nemažiau svarbu tai, kad kasdieniams darbams atlikti informacinėmis ir komunikacinėmis

[263] 2005/222/TVR.
[264] COM (2008) 712.
[265] http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf
[266] COM (2008) 199 galutinis.
[267] http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm
[268] 2007 m. ES ekonomikos apžvalga http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf
[269] http://www.oecd.org/dataoecd/1/29/40821707.pdf
[270] http://epp.eurostat.ec.europa.eu/. Mokslas ir technologijos, informacinė visuomenė.

technologijomis vis labiau pasikliauja ir naudojasi piliečiai – padidinus ypatingos svarbos informacinės infrastruktūros objektų saugumą, piliečiai labiau pasitikėtų informacinėmis ir komunikacinėmis technologijomis, pirmiausia dėl geresnės asmens duomenų ir slaptumo apsaugos.

3.2. Ypatingos svarbos informacinės infrastruktūros objektams kylančios grėsmės

Dėl piktavalių antpuolių, gaivalinių nelaimių arba techninių gedimų kylanti grėsmė dažnai nėra aiškiai suprantama ir (arba) pakankamai išnagrinėjama. Todėl suinteresuotosios šalys nepakankamai informuotos, kad sukurtų veiksmingas apsaugos ir atoveikio priemones.

Kibernetiniai antpuoliai tapo kaip niekad sudėtingi. Paprasti eksperimentai perauga į sudėtingus veiksmus, vykdomus siekiant pelno arba politinių tikslų. Neseniai įvykdyti didelio masto kibernetiniai Estijos, Lietuvos ir Gruzijos antpuoliai – tai plačiausiai nušviesti bendrosios tendencijos pavyzdžiai. Kokia sunki problema, galima įsitikinti iš to, kad yra daug virusų, „kirminų“ (savaime plintančių kenksmingų kompiuterinių programų) ir kitos kenkimo programinės įrangos, kad didėja kenksmingu programiniu kodu apkrėstų kompiuterių tinklai (angl. *botnet*) ir nuolat daugėja nepageidaujamų e. pašto laiškų[271].

Atsižvelgiant į didelį priklausomumą nuo ypatingos svarbos informacinės infrastruktūros objektų, jų tarpvalstybinius sujungimus ir tarpusavio priklausomumą nuo kitos infrastruktūros objektų taip pat į jų pažeidžiamumą ir jiems kylančias grėsmes, apsisaugoti nuo gedimų ir gintis nuo antpuolių reikėtų pirmiausia sistemingai sprendžiant ypatingos svarbos informacinės infrastruktūros objektų saugumo ir atsparumo klausimus.

3.3. Ypatingos svarbos informacinės infrastruktūros objektų saugumas ir atsparumas siekiant didesnio pasitikėjimo informacine visuomene

Siekiant užtikrinti, kad IKT infrastruktūros objektai būtų kuo geriau išnaudojami ir tokiu būdu visiškai įgyvendinamos ekonominės ir socialinės informacinės visuomenės galimybės, visos suinteresuotosios šalys turi ypač pasitikėti tais infrastruktūros objektais ir jais pasikliauti. Tai priklauso nuo įvairių dalykų, iš kurių svarbiausias – užtikrinti aukštą jų saugumo ir atsparumo lygį. Pagrindiniai saugumo plėtros veiksniai – įvairovė, atvirumas, funkcinis suderinamumas, tinkamumas naudoti, skaidrumas, atsekamumas, galimybė tikrinti įvairius komponentus ir konkurencija – skatina diegti saugumą didinančius produktus, procesus ir paslaugas. Kaip pabrėžė Komisija[272], tai bendra pareiga – jokia pavienė suinteresuotoji šalis neturi priemonių, kad užtikrintų visų IKT infrastruktūros objektų saugumą bei atsparumą ir vykdytų visus susijusius įsipareigojimus.

Norint imtis šios atsakomybės reikia rizikos valdymo metodo ir kultūros, įgalinančios reaguoti į žinomus pavojus ir anksti atpažinti naujas grėsmes, nesiimant pernelyg griežtų

[271] COM (2006) 688 galutinis.
[272] COM (2006) 251 galutinis.

veiksmų ir netrukdant atsirasti naujoviškoms paslaugoms ir taikymo būdams.

3.4. Europos uždaviniai

Vykdant veiklą, susijusią su direktyvos dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems įgyvendinimu, ypač su specialių IKT sektoriaus kriterijų nustatymu, ir siekiant tą veiklą papildyti, reikia išspręsti kelis didesnius sudėtingus uždavinius, kad būtų sustiprintas ypatingos svarbos informacinės infrastruktūros objektų saugumas ir atsparumas.

3.4.1. Nevienodi ir nesuderinti nacionaliniai metodai

Nors sudėtingi uždaviniai ir problemos, su kuriomis susiduriama, turi bendrybių, valstybėse narėse skiriasi ypatingos svarbos informacinės infrastruktūros objektų saugumo ir atsparumo užtikrinimo priemonės ir tvarka, profesinė kompetencija ir parengties lygis.

Jeigu sprendimai būtų priimami nacionaliniu lygmeniu, tai Europoje gali lemti suskaidymą ir neefektyvumą. Kai nacionaliniai metodai skiriasi ir trūksta sistemingo tarpvalstybinio bendradarbiavimo, nacionalinių atoveikio priemonių efektyvumas gerokai mažesnis, *inter alia,* dėl to, kad ypatingos svarbos informacinės infrastruktūros objektai tarpusavyje sujungti, vadinasi, dėl mažai apsaugotų ir neatsparių ypatingos svarbos informacinės infrastruktūros objektų vienoje valstybėje gali padidėti pažeidžiamumas ir pavojai kitose valstybėse.

Šioms aplinkybėms įveikti reikia Europos pastangų, kad papildomos vertės nacionalinei politikai ir programoms būtų suteikta, puoselėjant sąmoningumo ugdymą ir bendrą sudėtingų uždavinių supratimą, skatinant bendrų politikos uždavinių ir prioritetų priėmimą, stiprinant valstybių narių bendradarbiavimą ir integruojant nacionalines politikos kryptis labiau europinėje ir pasaulinėje sferoje.

3.4.2. Ypatingos svarbos informacinės infrastruktūros objektams reikia Europos valdymo modelio

Didinant ypatingai svarbios informacinės infrastruktūros objektų saugumą ir atsparumą susiduriama su specifiniais sudėtingais valdymo uždaviniais. Nors už politikos krypčių, susijusių su ypatingos svarbos informacinės struktūros objektais, nustatymą visų pirma atsako valstybės narės, jų įgyvendinimas priklauso nuo privačiojo sektoriaus, kuris turi ir valdo daug ypatingos svarbos informacinės infrastruktūros objektų. Tačiau privačiajam sektoriui rinkose ne visada pakanka paskatų investuoti į ypatingos svarbos informacinės infrastruktūros objektų apsaugą tiek, kiek paprastai reikalautų valdžios institucijos.

Nacionaliniu lygmeniu, kaip bazinis modelis, sudaryta viešojo ir privataus sektorių partnerystė šiai valdymo problemai spręsti. Nors ir sutariama, kad viešojo ir privataus sektorių partnerystė būtų naudinga ir Europos lygmeniu, tokia Europos masto partnerystė dar nesukurta. Privatųjį sektorių dalyvauti nustatant viešosios politikos tikslus bei veiklos prioritetus ir priemones būtų galima paskatinti Europos masto daugelio suinteresuotųjų

šalių dalyvavimu grindžiama valdymo sistema, kurioje gali būti numatytas aktyvesnis ENISA vaidmuo. Tokia sistema leistų panaikinti atotrūkį tarp nacionalinės politikos formavimo ir praktinės veiklos tikrovės.

3.4.3. Ribotos Europos ankstyvojo atpažinimo ir reagavimo į incidentus išgalės

Valdymo mechanizmai bus tikrai veiksmingi tik tada, kai visi dalyviai veiks remdamiesi patikima informacija. Tai ypač svarbu toms valdžios įstaigoms, kurios pirmiausiai atsakingos už piliečių saugumo ir gerovės užtikrinimą.

Tačiau tinklo saugumo incidentų kontrolės ir pranešimo apie juos procesai ir veikla įvairiose valstybėse narėse gerokai skiriasi. Kai kuriose iš jų pamatinės organizacijos kontrolei atlikti nėra. Negana to, valstybių narių bendradarbiavimas ir dalijimasis patikimais saugumo incidentų duomenimis, kuriais remiantis galima imtis veiksmų, nepakankamai išplėtotas – jis arba neoficialus, arba apsiriboja dvišaliais ar nedaugelio šalių duomenų mainais. Be to, norint padidinti ypatingos svarbos informacinės infrastruktūros objektų saugumą ir atsparumą, labai svarbu modeliuoti incidentus ir rengti pratybas reagavimo išgalėms išbandyti, visų pirma dėmesį skiriant lanksčioms strategijoms ir procesams, kad būtų atsižvelgiama į tai, jog galimos krizės yra nenuspėjamos. Europos Sąjungoje kibernetinio saugumo pratybos vis dar pradiniame etape. Labai mažai vykdoma tarpvalstybinių pratybų. Atsižvelgiant į patirtį, susijusią su pastarojo meto įvykiais[273], abipusė pagalba yra ypač svarbi norint tinkamai reaguoti į didelio masto grėsmes ir ypatingos svarbos informacinės infrastruktūros objektų antpuolius.

Europoje išgalės anksti atpažinti pavojus ir reaguoti į incidentus turi būti pagrįstos sklandžiai dirbančiomis nacionalinėmis (valstybinėmis) kompiuterinių incidentų tyrimo grupėmis (angl. *National/Governmental Computer Emergency Response Teams*, CERT), t. y. turi turėti bendras pagrindines išgales. Šios įstaigos valstybėse turi skatinti suinteresuotųjų šalių susidomėjimą ir gebėjimą vykdyti viešosios politikos veiklą (įskaitant veiklą, susijusią su piliečius ir mažąsias ir vidutines įmones apimančiomis informacijos mainų ir įspėjimo sistemomis) ir užsiimti efektyviu tarpvalstybiniu bendradarbiavimu bei informacijos mainais, galbūt maksimaliai naudodamosi esamomis organizacijomis, pavyzdžiui, Europos vyriausybinių CERT grupe (angl. *European Governmental CERTs Group*, EGC)[274].

3.4.4. Tarptautinis bendradarbiavimas

Internetas tapo pagrindine ypatingos svarbos informacine infrastruktūra, todėl ypatingą dėmesį reikia skirti jo atsparumui ir stabilumui. Įsitikinta, kad dėl savo paskirstytos dubliuotosios sandaros internetas yra labai tvirta infrastruktūra. Tačiau dėl neregėto augimo nuolat didėja fizinis ir loginis sudėtingumas bei atsiranda naujos paslaugos ir naudojimo būdai; pagrįstai kyla klausimų, ar internetas gali atlaikyti didėjantį gedimų ir kibernetinių antpuolių skaičių.

[273] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/
[274] http://www.egc-group.org/

Požiūris į interneto elementų svarbą skiriasi, todėl suprantama, kodėl tarptautiniuose forumuose valdžios institucijų pateikiamos pozicijos yra tokios skirtingos, o šio klausimo svarba dažnai suvokiama prieštaringai. Dėl to gali būti sunku užkirsti kelią internetui kylančioms grėsmėms, pasirengti jas atremti ir likviduoti jų padarinius. Pavyzdžiui, perėjimo nuo IPv4 prie IPv6 pasekmes taip pat reikėtų įvertinti atsižvelgiant į ypatingos svarbos informacinės infrastruktūros objektų saugumą.

Internetas – pasaulinis labai plačiai paskirstytas tinklų tinklas, kurio valdymo centrai veiklą dažnai vykdo neatsižvelgdami į nacionalines sienas. Norinti užtikrinti interneto atsparumą bei stabilumą, būtinas specialus tikslinis metodas, pagrįstas dviem viena kitą papildančiomis priemonėmis. Pirma, būtina susitarti, kokie interneto atsparumo ir stabilumo Europos prioritetai, atsižvelgiant į viešąją politiką ir praktinį diegimą. Antra, remiantis mūsų strateginiu dialogu ir bendradarbiavimu su trečiosiomis šalimis ir tarptautinėmis organizacijomis, būtina drauge su pasauline bendruomene ir laikantis pagrindinių Europos vertybių nustatyti interneto atsparumo ir stabilumo principus. Ši veikla būtų pagrįsta Pasaulio aukščiausiojo lygio susitikimo informacinės visuomenės klausimais[275] pripažinimu, kad interneto stabilumas yra svarbiausia.

4. Tolesnės veiklos kryptis. Geresnis koordinavimas ir bendradarbiavimas ES lygmeniu

Kadangi problema svarbi ne tik Bendrijos, ir bet tarptautiniu lygmeniu, integruotas ES metodas ypatingos svarbos informacinės infrastruktūros objektų saugumui ir atsparumui padidinti papildytų ir suteiktų papildomos vertės nacionalinėms programoms ir veikiančioms dvišalėms ir daugiašalėms valstybių narių bendradarbiavimo sistemoms.

Sprendžiant iš viešosios politikos aptarimo po įvykių Estijoje, panašių išpuolių poveikį galima riboti prevencijos priemonėmis ir suderintais veiksmais ištikus krizei. Labiau struktūriškai apibrėžti informacijos ir gerosios patirties mainai visoje Europos Sąjungoje galėtų gerokai palengvinti kovą su tarptautinėmis grėsmėmis.

Būtina sustiprinti esamas bendradarbiavimo priemones, įskaitant ENISA, ir prireikus sukurti naujų. Ypač svarbus kelis lygmenis apimantis daugelio suinteresuotųjų šalių metodas, kuris Europos lygmeniu taikomas visapusiškai atsižvelgiant į nacionalines pareigas ir jas papildant.

Būtina visiškai suprasti aplinką ir egzistuojančius suvaržymus. Pavyzdžiui, susirūpinimą kelia paskirstytoji interneto struktūra, kurioje galinių mazgų antpuoliai gali būti vykdomi, pavyzdžiui, kenksmingu programiniu kodu apkrėstų kompiuterių tinklais (angl. *botnet*). Tačiau ši paskirstytoji struktūra yra vienas iš svarbiausių stabilumo ir atsparumo komponentų, dėl jos veikla gali būti atkurta sparčiau nei paprastai, kai laikomasi pernelyg reglamentuotų hierarchinių procedūrų. Dėl šios priežasties reikia apgalvotai išnagrinėti kiekvieną atvejį ir nustatyti veiklos procedūras.

Svarbu ir numatomas laikotarpis. Akivaizdu, kad reikia veikti nedelsiant ir skubiai nustatyti būtinus elementus, kad būtų sukurta sistema, kuria naudodamiesi galėtume

275 Tuniso informacinės visuomenės darbotvarkė http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

spręsti dabartinius sudėtingus uždavinius ir kuri būtų naudinga būsimai tinklų ir informacijos saugumo strategijai.

Siūlomi tokie penki šių sudėtingų uždavinių sprendimo ramsčiai:

(1) parengtis ir prevencija: užtikrinti parengtį visais lygmenimis;

(2) atpažinimas ir reagavimas: numatyti tinkamus ankstyvojo atpažinimo mechanizmus;

(3) padarinių mažinimas ir veiklos atkūrimas: sustiprinti ES ypatingos svarbos informacinės infrastruktūros objektų gynybos mechanizmus;

(4) tarptautinis bendradarbiavimas: ES prioritetus propaguoti tarptautiniu lygiu;

(5) IKT sektoriaus kriterijai: remti direktyvos dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems[276] įgyvendinimą.

5. Veiksmų planas

5.1. Parengtis ir prevencija

Išgalių ir paslaugų bazė bendradarbiauti Europos mastu. Valstybes nares ir susijusias suinteresuotąsias šalis Komisija ragina:

- su Europos tinklų ir informacijos apsaugos agentūros pagalba nustatyti minimalų nacionalinių (valstybinių) kompiuterinių incidentų tyrimo grupių išgalių ir paslaugų lygmenį ir reagavimo į incidentus veiklą, vykdomą Europos masto bendradarbiavimui paremti;

- užtikrinti, kad nacionalinės (valstybinės) kompiuterinių incidentų tyrimo grupės veiktų kaip parengties, informacijos mainų, koordinavimo ir reagavimo išgalių pagrindinė sudedamoji dalis.

Užduotis: iki 2010 m. pabaigos suderinti minimalius standartus; iki 2011 m. pabaigos visose valstybėse narėse įsteigti gerai veikiančias nacionalines (valstybines) kompiuterinių incidentų tyrimo grupes.

Europos viešojo ir privačiojo sektoriaus partnerystė (EP3R) atsparumui užtikrinti. Komisija:

- skatins viešojo ir privačiojo sektoriaus bendradarbiavimą tokiais klausimais: saugumo ir atsparumo tikslai, baziniai reikalavimai, geroji politikos patirtis ir priemonės; EP3R pirmiausia dėmesį sutelktų Europos aspektui strateginiu (pavyzdžiui, politikos gerosios patirties) ir taktiniu (veiklos) (pavyzdžiui, diegimo pramonėje) požiūriu. EP3R turėtų remtis esamomis nacionalinėmis iniciatyvomis ir ENISA darbine veikla bei jas papildyti.

Užduotis: iki 2009 m. pabaigos parengti EP3R strateginį planą ir planą; iki 2010 m. įsteigti EP3R; iki 2010 m. pabaigos EP3R gauna pirmuosius rezultatus.

[276] Tarybos direktyva 2008/114/EB.

Valstybių narių informacijos mainų Europos forumas. Komisija:

- įsteigs valstybių narių Europos forumą, kuriame bus keičiamasi ypatingos svarbos informacinės infrastruktūros objektų saugumo ir atsparumo informacija ir gerąja politikos patirtimi. Tam būtų naudingi kitų organizacijų, ypač ENISA, veiklos rezultatai.

Užduotis: iki 2009 m. pradėti forumo veiklą, iki 2010 m. pabaigos pateikti pirmuosius rezultatus.

5.2. Atpažinimas ir reagavimas

Europos informacijos mainų ir įspėjimo sistema (EISAS). Komisija pritaria tam, kad

būtų sukurta ir įdiegta nacionalinėmis ir privačiojo sektoriaus informacijos mainų ir įspėjimo sistemomis pagrįsta EISAS, kurioje dalyvautų piliečiai ir mažosios ir vidutinės įmonės. Komisija lėšomis remia du papildomuosius prototipų kūrimo projektus[277]. ENISA raginama kritiškai įvertinti šių projektų ir kitų nacionalinių iniciatyvų rezultatus ir parengti strateginį tolesnio EISAS kūrimo ir diegimo planą.

Užduotis: iki 2010 m. pabaigos baigti prototipų kūrimo projektus; iki 2010 m. pateikti strateginį Europos sistemos kūrimo planą.

5.3. Padarinių mažinimas ir veiklos atkūrimas

Nacionalinis nepaprastųjų situacijų planavimas ir pratybos. Valstybes nares Komisija ragina:

- siekiant glaudesnio koordinavimo visoje Europoje, sudaryti nacionalinius nepaprastųjų situacijų planus ir reguliariai organizuoti reagavimo į didelio masto tinklų saugumo incidentus ir veiklos atkūrimo pratybas. Nacionalinėms (valstybinėms) kompiuterinių incidentų tyrimo grupėms (reagavimo į kompiuterinius saugumo incidentus tarnyboms) gali būti duota užduotis vadovauti nacionalinei nepaprastųjų situacijų planavimo veiklai ir bandymams, dalyvaujant privačiojo ir viešojo sektoriaus suinteresuotosioms šalims. ENISA raginama valstybėms narėms padėti keistis gerąja patirtimi.

Užduotis: iki 2010 m. pabaigos kiekvienoje valstybėje narėje surengti mažiausiai vienerias nacionalines pratybas.

Didelių tinklo saugumo incidentų Europos masto pratybos. Komisija:

- finansiškai parems dideles interneto saugumo[278] pratybas, kurios taip pat galėtų būti platforma Europos mastu dalyvauti tarptautinėse tinklo saugumo incidentų pratybose, panašiose į JAV organizuotas pratybas *CyberStorm*.

[277] Pagal specialiąją ES programą „Terorizmo ir kitos su saugumu susijusios rizikos prevencija, parengtis ir padarinių valdymas“ http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm.
[278] *Supra* 27.

Užduotis: iki 2010 m. parengti ir atlikti pirmąsias Europos masto pratybas; iki 2010 m. pabaigos pasirengti Europos mastu dalyvauti tarptautinėse pratybose.

Aktyvesnis nacionalinių (valstybinių) kompiuterinių incidentų tyrimo grupių bendradarbiavimas. Valstybes nares Komisija ragina:

- stiprinti nacionalinių (valstybinių) kompiuterinių incidentų tyrimo grupių bendradarbiavimą, be kita ko maksimaliai išnaudojant ir plėtojant esamus bendradarbiavimo mechanizmus, pavyzdžiui EGC[279]. ENISA raginama aktyviai veikti, kad paskatintų ir paremtų Europos masto nacionalinių (valstybinių) kompiuterinių incidentų tyrimo grupių bendradarbiavimą, kurį vykdant turėtų būti pagerinta parengtis ir sustiprintos Europos pajėgos reaguoti ir atsakyti į incidentus, bei pradėtos Europos masto (ir (arba) regioninės) pratybos.

Užduotis: iki 2010 m. pabaigos užtikrinti, kad Europos valstybinių CERT grupėje dalyvautų dvigubai daugiau nacionalinių įstaigų; iki 2010 m. pabaigos ENISA turėtų parengti pagalbinę bendradarbiavimo Europos mastu informacinę medžiagą.

5.4. Tarptautinis bendradarbiavimas

Interneto atsparumas ir stabilumas. Numatytos trys papildomosios veiklos kryptys.

- Europos ilgalaikiai interneto atsparumo ir stabilumo prioritetai. Komisija vadovaus visų susijusių viešojo ir privačiojo sektorių suinteresuotųjų šalių diskusijai, kad būtų nustatyti Europos ilgalaikiai interneto atsparumo ir stabilumo prioritetai.

Užduotis: iki 2010 m. pabaigos nustatyti ES ypatingos svarbos interneto komponentų prioritetus ir problemas.

- Interneto atsparumo ir stabilumo principai ir gairės (Europos lygmens). Komisija ir valstybės narės sieks nustatyti interneto atsparumo ir stabilumo gaires, dėmesį sutelkdamos, *inter alia*, į pasekmių šalinimo veiksmus, savitarpio pagalbos susitarimus, suderintas veiklos atkūrimo ir tęstinumo strategijas, geografinį ypatingos svarbos interneto išteklių paskirstymą, technologines apsaugos priemones interneto infrastruktūroje ir protokoluose, paslaugų ir duomenų dubliavimą. Komisija jau finansuoja sričių vardų sistemos (angl. *Domain name system*, DNS) atsparumo darbo grupę, kuri drauge su kitais susijusiais projektais padės pasiekti sutarimą[280].

Užduotis: iki 2009 m. pabaigos parengti strateginį Europos planą, kaip nustatyti interneto atsparumo ir stabilumo principus bei gaires; iki 2010 m. suderinti tokių principų ir gairių pirmą projektą.

- Interneto atsparumo ir stabilumo principai ir gairės (pasaulio lygmens). Komisija ir valstybės narės parengs strateginį planą, kaip principus ir gaires

[279] *Supra* 24.
[280] *Supra* 27.

propaguoti pasaulio lygmeniu. Siekiant pasaulinio susitarimo bus plėtojamas strateginis bendradarbiavimas su trečiosiomis šalimis, ypač informacinės visuomenės dialogas[281].

Užduotis: 2010 m. pradžioje sudaryti tarptautinio bendradarbiavimo saugumo ir atsparumo principų ir gairių klausimais strateginį planą; iki 2010 m. pabaigos parengti pirmą pasaulyje pripažintų principų ir gairių redakciją, kuri bus aptarta su trečiosiomis šalimis ir susijusiuose forumuose, įskaitant Interneto valdymo forumą.

Veiklos atkūrimo ir pasekmių mažinimo po didelio masto interneto incidentų pasaulinės pratybos. Suinteresuotąsias šalis Komisija ragina:

- apsvarstyti, kaip pratybas, vykdomas pagal padarinių mažinimo ir veiklos atkūrimo ramstį, plėtoti pasaulio lygmeniu, remiantis regioniniais nepaprastųjų situacijų planais ir išgalėmis.

Užduotis: iki 2010 m. pabaigos Komisija turėtų pasiūlyti sistemą ir strateginį planą, kaip paremti Europos dalyvavimą pasaulinėse veiklos atkūrimo ir pasekmių mažinimo po didelio masto interneto incidentų pratybose.

5.5. Europos ypatingos svarbos infrastruktūros objektų IKT sektoriuje kriterijai

Specialūs IKT sektoriaus kriterijai. Remdamasi pradine 2008 m. vykdyta veikla, Komisija:

- drauge su valstybėmis narėmis ir visomis susijusiomis suinteresuotomis šalimis toliau kurs kriterijus, kaip nustatyti IKT sektoriaus Europos ypatingos svarbos infrastruktūros objektus. Tam reikalinga informacija bus paimta iš specialaus šiuo metu pradedamo tyrimo[282].

Užduotis: per pirmąjį 2010 m. pusmetį Komisija turėtų nustatyti IKT sektoriaus Europos ypatingos svarbos infrastruktūros objektų kriterijus.

6. Išvados

Ypatingos svarbos informacinės infrastruktūros objektų saugumas ir atsparumas – pirmoji priemonė apsisaugoti nuo gedimų ir gintis nuo antpuolių. Saugumą ir atsparumą visoje Europos Sąjungoje būtina stiprinti, kad būtų pasinaudota visais įmanomais informacinės visuomenės privalumais. Šiam plataus užmojo tikslui pasiekti siūlomas veiksmų planas, kad Europos lygiu būtų sustiprintas taktinis ir veiklos bendradarbiavimas. Šių veiksmų sėkmė priklauso nuo to, kaip efektyviai juos galima pagrįsti viešojo ir privačiojo sektorių veikla ir kiek jie naudingi tai veiklai, taip pat nuo valstybių narių, Europos institucijų ir suinteresuotųjų šalių pasiryžimo ir visapusiško dalyvavimo.

2009 m. balandžio 27–28 d. įvyks ministrų konferencija, kurioje su valstybėmis narėmis bus aptartos pasiūlytos iniciatyvos ir įvertintas jų pasiryžimas aptarti atnaujintą ir sustiprintą tinklų bei informacijos saugumo politiką Europoje.

[281] COM (2008) 588 galutinis.
[282] *Supra* 27.

Galiausiai ypatingos svarbos informacinių struktūrų saugumo ir atsparumo stiprinimas yra ilgalaikis tikslas, kurio strategiją ir priemones reikia reguliariai vertinti. Kadangi šis tikslas dera su bendrąja diskusija dėl būsimos tinklų ir informacijos saugumo politikos Europos Sąjungoje po 2012 m., 2010 m. pabaigoje Komisija, siekdama įvertinti pirmojo etapo veiksmus ir prireikus nustatyti bei pasiūlyti tolesnes priemones, pradės rezultatų apžvalgą.

Priedas Nr. 3

Ištrauka iš Lietuvos Respublikos baudžiamojo kodekso

2011-06-30 versija

PATVIRTINTAS
2000 m. rugsėjo 26 d.
įstatymu Nr. VIII-1968

LIETUVOS RESPUBLIKOS

BAUDŽIAMASIS KODEKSAS

BENDROJI DALIS

I SKYRIUS

BENDROSIOS NUOSTATOS

<...>

XXIV SKYRIUS

NUSIKALTIMAI ASMENS PRIVATAUS GYVENIMO NELIEČIAMUMUI

165 straipsnis. Neteisėtas asmens būsto neliečiamumo pažeidimas

1. Tas, kas neteisėtai slapta ar atvirai, panaudodamas apgaulę ar smurtą arba kitokiu būdu prieš savininko ar jo įgaliotų asmenų valią įsibrovė į kito žmogaus gyvenamąjį namą, butą ar kitą gyvenamąją patalpą arba jos priklausinius, įskaitant saugomą būsto teritoriją,

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

2. Už šiame straipsnyje numatytą veiką asmuo atsako tik tuo atveju, kai yra nukentėjusio asmens skundas ar jo teisėto atstovo pareiškimas, ar prokuroro reikalavimas.

166 straipsnis. Asmens susižinojimo neliečiamumo pažeidimas

1. Tas, kas neteisėtai perėmė paštu ar per pasiuntinių paslaugos teikėją siunčiamą siuntą ar siuntinį arba neteisėtai perėmė, fiksavo ar stebėjo asmens elektroninių ryšių tinklais siunčiamus pranešimus, arba neteisėtai fiksavo, klausėsi ar stebėjo asmens pokalbius elektroninių ryšių tinklais, arba kitaip pažeidė asmens susižinojimo neliečiamumą,

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

2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

167 straipsnis. Neteisėtas informacijos apie privatų asmens gyvenimą rinkimas

1. Tas, kas neteisėtai rinko informaciją apie privatų asmens gyvenimą,

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

2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

168 straipsnis. Neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas

1. Tas, kas be asmens sutikimo viešai paskelbė, pasinaudojo ar kitų asmenų labui panaudojo informaciją apie kito žmogaus privatų gyvenimą, jeigu tą informaciją jis sužinojo dėl savo tarnybos ar profesijos arba atlikdamas laikiną užduotį, arba ją surinko darydamas šio kodekso 165–167 straipsniuose numatytą veiką,

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

2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.
3. Už šiame straipsnyje numatytą veiką asmuo atsako tik tuo atveju, kai yra nukentėjusio asmens skundas ar jo teisėto atstovo pareiškimas, ar prokuroro reikalavimas.

<...>

XXVIII SKYRIUS

NUSIKALTIMAI IR BAUDŽIAMIEJI NUSIŽENGIMAI NUOSAVYBEI, TURTINĖMS TEISĖMS IR TURTINIAMS INTERESAMS

<...>

182 straipsnis. Sukčiavimas

1. Tas, kas apgaule savo ar kitų naudai įgijo svetimą turtą ar turtinę teisę, išvengė turtinės prievolės arba ją panaikino,

   baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.
2. Tas, kas apgaule savo ar kitų naudai įgijo didelės vertės svetimą turtą ar turtinę teisę arba didelės mokslinės, istorinės ar kultūrinės reikšmės turinčias vertybes arba išvengė didelės vertės turtinės prievolės, arba ją panaikino, arba sukčiavo dalyvaudamas organizuotoje grupėje,

   baudžiamas laisvės atėmimu iki aštuonerių metų.
3. Tas, kas apgaule savo ar kitų naudai įgijo nedidelės vertės svetimą turtą ar turtinę teisę, išvengė nedidelės vertės turtinės prievolės arba ją panaikino, padarė baudžiamąjį nusižengimą ir

   baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu.
4. Už šio straipsnio 1 ir 3 dalyse numatytas veikas asmuo atsako tik tuo atveju, kai yra nukentėjusio asmens skundas ar jo teisėto atstovo pareiškimas, ar prokuroro reikalavimas.
5. Už šio straipsnio 1 ir 2 dalyse numatytas veikas atsako ir juridiniai asmenys.

Straipsnio pakeitimai:

Nr. IX-2314, 2004-07-05, Žin., 2004, Nr. 108-4030 (2004-07-13)

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

<...>

XXIX SKYRIUS

NUSIKALTIMAI INTELEKTINEI IR PRAMONINEI NUOSAVYBEI

191 straipsnis. Autorystės pasisavinimas

1. Tas, kas savo vardu išleido arba viešai paskelbė svetimą literatūros, mokslo ar meno kūrinį (įskaitant kompiuterių programas ir duomenų bazes) arba jo dalį,

   baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų.
2. Tas, kas pasinaudodamas tarnybos padėtimi arba panaudodamas psichinę prievartą privertė literatūros, mokslo ar meno kūrinio (įskaitant kompiuterių programas ir duomenų bazes) arba jo dalies autorių pripažinti kitą asmenį bendraautoriumi ar autoriaus teisių perėmėju arba atsisakyti autorystės teisės,

   baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.
3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. IX-1992, 2004-01-29, Žin., 2004, Nr. 25-760 (2004-02-14)

Nr. XI-330, 2009-07-09, Žin., 2009, Nr. 87-3663 (2009-07-23)

Straipsnio pavadinimo pakeitimai:

Nr. XI-330, 2009-07-09, Žin., 2009, Nr. 87-3663 (2009-07-23)

192 straipsnis. Literatūros, mokslo, meno kūrinio ar gretutinių teisių objekto neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas

1. Tas, kas neteisėtai atgamino literatūros, mokslo ar meno kūrinį (įskaitant kompiuterių programas ir duomenų bazes) ar gretutinių teisių objektą arba jų dalį komercijos tikslais arba platino, gabeno ar laikė komercijos tikslais neteisėtas jų kopijas, jeigu kopijų bendra vertė pagal teisėtų kopijų, o kai jų nėra, pagal atgamintų kūrinių originalų kainas viršijo 100 MGL dydžio sumą,

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

*2. Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką, jeigu neteisėtų kopijų bendra vertė pagal teisėtų kopijų, o kai jų nėra, pagal atgamintų kūrinių originalų kainas viršijo 250 MGL dydžio sumą,

baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.

3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. XI-330, 2009-07-09, Žin., 2009, Nr. 87-3663 (2009-07-23)

Pastaba: **1 dalis, straipsnis papildytas nauja 2 dalimi, buvusią 2 dalį laikyti 3 dalimi*

193 straipsnis. Informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas

1. Tas, kas be autorių teisių ar gretutinių teisių subjekto leidimo komercijos tikslais sunaikino arba pakeitė informaciją apie autorių teisių ar gretutinių teisių valdymą, jeigu pagal tą informaciją identifikuojamas kūrinys, kūrinio autorius, kitas autorių teisių subjektas arba atlikėjas, kūrinio atlikimas, fonograma, fonogramos gamintojas, kitas gretutinių teisių subjektas, taip pat informaciją apie kūrinio, jo atlikimo ar fonogramos naudojimo sąlygas ir tvarką, įskaitant visus skaičius ar kodus, perteikiančius kūrinio, atlikimo įrašo ar fonogramos egzemplioriuose pažymėtą arba jų viešo paskelbimo metu pateikiamą informaciją,

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

2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.

194 straipsnis. Neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas

1. Tas, kas neteisėtai pašalino bet kokias technines apsaugos priemones, kurias autorių teisių ar gretutinių teisių subjektai naudoja savo teisėms įgyvendinti ar apsaugoti, arba komercijos tikslais gamino, importavo, eksportavo, laikė, gabeno ar platino galimybę pašalinti tas technines apsaugos priemones suteikiančius prietaisus (dekoderius, dekodavimo korteles ar kitokius prietaisus) arba programinę įrangą, slaptažodžius, kodus ar kitokius panašius duomenis,

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

2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. IX-2314, 2004-07-05, Žin., 2004, Nr. 108-4030 (2004-07-13)

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

<...>

XXX SKYRIUS

NUSIKALTIMAI ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI

196 straipsnis. Neteisėtas poveikis elektroniniams duomenims

1. Tas, kas neteisėtai sunaikino, sugadino, pašalino ar pakeitė elektroninius duomenis arba techninę įranga, programinę įranga ar kitais būdais apribojo naudojimąsi tokiais duomenimis padarydamas didelės žalos,

   baudžiamas viešaisiais darbais arba bauda, arba laisvės atėmimu iki ketverių metų.
2. Tas, kas šio straipsnio 1 dalyje numatytą veiką padarė strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniams duomenims,

   baudžiamas bauda arba areštu, arba laisvės atėmimu iki šešerių metų.
3. Tas, kas padarė šiame straipsnyje numatytą veiką padarydamas nedidelės žalos, padarė baudžiamąjį nusižengimą ir

   baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu.
4. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. IX-1992, 2004-01-29, Žin., 2004, Nr. 25-760 (2004-02-14)

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

197 straipsnis. Neteisėtas poveikis informacinei sistemai

1. Tas, kas neteisėtai sutrikdė ar nutraukė informacinės sistemos darbą padarydamas didelės žalos,

   baudžiamas bauda arba areštu, arba laisvės atėmimu iki ketverių metų.
2. Tas, kas šio straipsnio 1 dalyje numatytą veiką padarė strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiai informacinei sistemai,

   baudžiamas bauda arba areštu, arba laisvės atėmimu iki šešerių metų.
3. Tas, kas padarė šiame straipsnyje numatytą veiką padarydamas nedidelės žalos, padarė baudžiamąjį nusižengimą ir

baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu.

4. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. IX-1992, 2004-01-29, Žin., 2004, Nr. 25-760 (2004-02-14)

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

198 straipsnis. Neteisėtas elektroninių duomenų perėmimas ir panaudojimas

1. Tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis,

   baudžiamas bauda arba laisvės atėmimu iki ketverių metų.

2. Tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis,

   baudžiamas laisvės atėmimu iki šešerių metų.

3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

198(1) straipsnis. Neteisėtas prisijungimas prie informacinės sistemos

1. Tas, kas neteisėtai prisijungė prie informacinės sistemos pažeisdamas informacinės sistemos apsaugos priemones,

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

2. Tas, kas neteisėtai prisijungė prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos,

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

3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

Kodeksas papildytas straipsniu:

Nr. IX-1992, 2004-01-29, Žin., 2004, Nr. 25-760 (2004-02-14)

Straipsnio pakeitimai:

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

198(2) straipsnis. Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis

1. Tas, kas neteisėtai gamino, gabeno, pardavė ar kitaip platino įrenginius ar programinę įrangą, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis, tiesiogiai skirtus daryti nusikalstamas veikas, arba tuo pačiu tikslu juos įgijo ar laikė,

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

2. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

Kodeksas papildytas straipsniu:

Nr. IX-1992, 2004-01-29, Žin., 2004, Nr. 25-760 (2004-02-14)

Straipsnio pakeitimai:

Nr. X-1233, 2007-06-28, Žin., 2007, Nr. 81-3309 (2007-07-21)

<...>

XLIII SKYRIUS

NUSIKALTIMAI IR BAUDŽIAMIEJI NUSIŽENGIMAI VALDYMO TVARKAI, SUSIJĘ SU DOKUMENTŲ AR MATAVIMO PRIEMONIŲ KLASTOJIMU

300 straipsnis. Dokumento suklastojimas ar disponavimas suklastotu dokumentu

1. Tas, kas pagamino netikrą dokumentą, suklastojo tikrą dokumentą arba žinomai netikrą ar žinomai suklastotą tikrą dokumentą laikė, gabeno, siuntė, panaudojo ar realizavo,

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

2. Tas, kas pagamino netikrą asmens tapatybės kortelę, pasą, vairuotojo pažymėjimą ar valstybinio socialinio draudimo pažymėjimą arba suklastojo tikrą asmens tapatybės kortelę, pasą, vairuotojo pažymėjimą ar valstybinio socialinio draudimo pažymėjimą, arba žinomai netikrą ar žinomai suklastotą tikrą asmens tapatybės kortelę, pasą, vairuotojo pažymėjimą ar valstybinio socialinio draudimo pažymėjimą laikė, gabeno, siuntė, panaudojo ar realizavo,

   baudžiamas areštu arba laisvės atėmimu iki ketverių metų.

3. Tas, kas padarė šio straipsnio 1 ar 2 dalyje numatytas veikas, jeigu dėl to buvo padaryta didelės žalos, arba pagamino didelį kiekį netikrų asmens tapatybės

kortelių, pasų, vairuotojo pažymėjimų ar valstybinio socialinio draudimo pažymėjimų, arba suklastojo didelį kiekį tikrų asmens tapatybės kortelių, pasų, vairuotojo pažymėjimų ar valstybinio socialinio draudimo pažymėjimų, arba žinomai netikrų ar žinomai suklastotų tikrų didelį kiekį asmens tapatybės kortelių, pasų, vairuotojo pažymėjimų ar valstybinio socialinio draudimo pažymėjimų laikė, gabeno, siuntė, panaudojo ar realizavo,

baudžiamas laisvės atėmimu iki šešerių metų.

4. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. X-511, 2006-01-20, Žin., 2006, Nr. 17-605 (2006-02-11)

<...>

XLIV SKYRIUS
NUSIKALTIMAI IR BAUDŽIAMIEJI NUSIŽENGIMAI DOROVEI

<...>

309 straipsnis. Disponavimas pornografinio turinio dalykais

1. Tas, kas turėdamas tikslą platinti pagamino ar įsigijo arba platino pornografinio turinio dalykus,

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

2. Tas, kas pagamino, įsigijo, laikė, demonstravo, reklamavo arba platino pornografinio turinio dalykus, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas,

   baudžiamas bauda arba laisvės atėmimu iki dvejų metų.

3. Tas, kas turėdamas tikslą platinti pagamino ar įsigijo arba platino didelį kiekį pornografinio turinio dalykų, kuriuose vaizduojamas mažametis vaikas,

   baudžiamas laisvės atėmimu iki penkerių metų.

4. Tas, kas demonstravo ar reklamavo pornografinio turinio dalykus, padarė baudžiamąjį nusižengimą ir

   baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu.

5. Už šio straipsnio 1, 2 ir 3 dalyse numatytas veikas atsako ir juridinis asmuo.

Straipsnio pakeitimai:

Nr. IX-1992, 2004-01-29, Žin., 2004, Nr. 25-760 (2004-02-14)

Nr. X-711, 2006-06-22, Žin., 2006, Nr. 77-2961 (2006-07-14)

Štitilis, Darius
Elektroniniai nusikaltimai. Metodinė priemonė / Doc. dr. Darius Štitilis. — Vilnius: Mykolo Romerio universitetas, 2011. 158 psl.
ISBN 978-9955-19-329-6

Metodinė priemonė yra skirta specialistams, kuriems svarbu išmanyti vieną didžiausių elektroninėje erdvėje slypinčių pavojų – elektroninius nusikaltimus. Pasitelkus Lietuvos mokslininkų darbus, teisės precedentus ir aktus, taip pat internetinius šaltinius, knygelėje pateikta informacija apie elektroninį nusikalstamumą, elektroninių nusikaltimų klasifikaciją, nusikaltimų subjektus ir jų atlikimo būdus, teisinius elektroninių nusikaltimų aspektus bei elektroninių nusikaltimų prevenciją, – tai yra svarbiausi dalykai, sudarantys Teisės pažeidimų elektroninėje erdvėje dalyko, dėstomo Mykolo Romerio universiteto Naujų technologijų teisės studentams, pagrindą.

Doc. dr. Darius Štitilis

ELEKTRONINIAI NUSIKALTIMAI

Metodinė priemonė

Redagavo Aistė Koženiauskienė
Maketavo Vilija Stankienė

Tiražas 50 egz.

Išleido Mykolo Romerio universitetas, Ateities g. 20, LT-08303 Vilnius
Tel. (8 5) 271 4625, faks. (8 5) 267 6000,
el. p. roffce@mruni.eu, www.mruni.eu

Spaudė UAB „Smaltijos“ leidykla, Kapsų g. 82, LT-44144 Kaunas
Tel. (37) 425402, faks. (37) 208992,
el. p. office@smaltija.lt, interneto svetainė http://www.smaltija.lt/