MYKOLO ROMERIO UNIVERSITETO
TEISĖS FAKULTETO
BAUDŽIAMOSIOS TEISĖS IR PROCESO INSTITUTAS

IRENA STELMAKOVAITĖ
BAUDŽIAMOSIOS TEISĖS IR KRIMINOLOGIJOS PROGRAMA
137227

NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE TYRIMAS: TARPTAUTINĖ IR NACIONALINĖ PRAKTIKA

Magistro baigiamasis darbas

Darbo vadovas -
Prof. dr. Vidmantas Egidijus Kurapka

Vilnius, 2015

TURINYS

ĮVADAS 3
1. Nusikaltimų elektroninėje erdvėje kriminalistinė charakteristika.....8
1.1. Nusikaltimų elektroninėje erdvėje padarymo būdas.....11
1.2. Nusikaltimą elektroninėje erdvėje padaręs asmuo 15
1.3. Nusikaltimų elektroninėje erdvėje pasikėsinimo dalykas.....17
1.4. Nusikaltimų elektroninėje erdvėje situacija.....21
2. Nusikaltimų elektroninėje erdvėje tyrimo reglamentavimas.....27
2.1. Nusikaltimų elektroninėje erdvėje tarptautinis reglamentavimas ir bendradarbiavimas....27
2.2.Tarptautinių organizacijų ir ES dokumentai dėl elektroninių nusikaltimų tyrimo.....33
2.3.Nusikaltimų elektroninėje erdvėje tyrimo reglamentavimas Lietuvoje.....38
3. Nusikaltimų elektroninėje erdvėje tyrimų tarptautinė ir nacionalinė praktika.....44
3.1. Nusikaltimų elektroninėje erdvėje prevencija ir problemos.....49
3.2. Pagrindinės nusikaltimų elektroninėje erdvėje tyrimo metodikos ir tobulinimo kryptys...56
IŠVADOS..... 64
LITERATŪROS SĄRAŠAS..... 66
ANOTACIJA.....71
ANNOTATION..... 72
SANTRAUKA 73
SUMMARY 74
PRIEDAI 75
PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ.....76

ĮVADAS

Šiuolaikinėje visuomenėje plačiai paplito informacinių technologijų naudojimas. Technologijų vystymas sąlygojo ir įvairių nusikalstamo elgesio formų atsiradimą bei plitimą.[1] Globaliame pasaulyje kompiuteris tampa ne tik teisėtos veikos įrankiu, bet kartu ir neteisėtos veikos. Elektroniniai nusikaltimai gali paveikti tiek konkretų asmenį, tiek visą visuomenę.[2] Vis dažniau tiriant nusikaltimą tenka aiškintis internetinėje erdvėje paliktus pėdsakus ir remtis jais aiškinantis padarytą nusikalstamą veiką. Nusikaltimai elektroninėje erdvėje gali pasireikšti, kaip įsilaužimas į sistemas, duomenų vagystė, draudžiamo turinio platinimas, autorinių teisių pažeidimas ir t.t. Elektroninė erdvė suteikia galimybę daryti nusikalstamas veikas, sudaro sąlygas naujiems nusikaltimo būdams atsirasti ir plisti. Todėl nusikaltėliai gali didinti nusikaltimų darymo paplitimo mastą, vienu metu gali nukentėti daug aukų skirtingose pasaulio vietose, skirtingose jurisdikcijose, kur veikia skirtingi įstatymai. Nusikaltimų elektroninėje erdvėje tyrimą apsunkina ir elektroninėje erdvėje esančių duomenų trumpalaikiškumas. Todėl nusikaltimų elektroninėje erdvėje tyrimų procesą galima apibrėžti, kaip įkalčių identifikavimą, surinkimą, išaiškinimą, analizę, bei išvadų parengimą. Tokių nusikaltimų tyrimas yra gerokai sudėtingesnis, nes jam reikia daugiau techninių, žmonių išteklių, o neretai ir tarptautinio bendradarbiavimo. Darant vieną nusikaltimą, gali dalyvauti asmenys iš skirtingų šalių, nereikia fizinio kontakto, jie palaiko ryšį ir bendrauja internete, sudaro planą, pasiskirsto vaidmenimis, vienas kuria virusą, kitas nuiminėja pinigus, kitas juos persiunčia ir tai vyksta pasauliniu mastu.

Baigiamojo darbo aktualumas. Šių dienų pasaulyje internetinė erdvė ir tarptautinė erdvė yra persipynusios tarpusavyje. Informacinė sistema apjungia kontinentus, salas, tautas, bendruomenes ir pavienius asmenis į milžinišką virtualų tinklą, tačiau nepaisant to valstybės vis tiek išlaiko savo tradicinį imunitetą. Yra sakoma, kad pasaulyje turinčiame internetą nei viena sala nėra sala.[3] Dėl vis didėjančių technologijų, ypač interneto svarbos, ankščiau tik užsienio valstybėse aktualios nusikaltimų elektroninėje erdvėje problemos atėjo ir į Lietuvą. Interneto tinklas neturi sienų, todėl tapo sunku tirti tokio pobūdžio nusikaltimus. Siekiant mažinti nusikalstamumą elektroninėje erdvėje, buvo priimta Budapešte 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų. Matydamos dideles permainas, vykstančias dėl kompiuterių tinklų skaitmeninio keitimo, susiliejimo ir nuolatinės globalizacijos, kad kompiuteriniai tinklai ir elektroninė informacija taip pat gali būti naudojami daryti nusikaltimams ir kad tokių nusikaltimų duomenys gali būti saugomi šiuose tinkluose ir jais perduodami. Taip pritardamos naujausiems poslinkiams, skatinantiems tarptautinį supratimą ir bendradarbiavimą kovojant su elektroniniais nusikaltimais,

[1] Higgins, G.E. Cybercrime: An Introduction to an Emerging Phenomen. Library of Congress Cataloging, 2010, p. 1.
[2] Brenner, S.W. Cybercrime. Criminal Threats from Cyberspace. Library of Congress Cataloging, 2010, įžangos VII
[3] McConnell International.Cyber Crime…and Punishment? Archaic Laws Threaten Global Information: Archaic Laws Threaten Global Information. December 2000, p. 8.

tarp jų Jungtinių Tautų, OECD, Europos Sąjungos ir G8 veiksmus.[4] Ši konvencija suteikia daug įgaliojimų kovoti su nusikaltimais elektroninėje erdvėje, palengvina tyrimą, sekimą, baudžiamąjį persekiojimą tarptautiniu bei nacionaliniu lygmeniu. Tačiau ši konvencija nepakankamai padeda užkirsti kelią, bei sustabdyti nuo naujų nusikaltimų darymo elektroninėje erdvėje, kadangi mažai yra pasirašiusių šalių yra šią konvenciją.

2015 m. sausio 1d. Lietuvoje įsigaliojo kibernetinio saugumo įstatymas, apibrėžiantis kibernetinio saugumo sistemos organizavimą, saugumo užtikrinimo priemones valdymą ir kontrolę, kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas. Veiklą pradėjo Nacionalinis kibernetinio saugumo centras, kurio pagrindinis dėmesys sutelktas į valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros kibernetiniam saugumui. Centras analizuoja kibernetinio saugumo aplinką, rengia reikalavimus viešojo sektoriaus informacinių išteklių ir ypatingos svarbos infrastruktūros kibernetiniam saugumui užtikrinti, kibernetinės gynybos bei grėsmių valdymo planus, koordinuoja ir prižiūri, kaip institucijų valdytojai įgyvendina kibernetinės apsaugos priemones, taip pat tiria ir reaguoja į kibernetinius incidentus. Įstatymu taip pat suteikiami įgaliojimai policijai, vykdydama kibernetinių incidentų užkardymą ir tyrimą, duoti motyvuotus nurodymus ne ilgiau kaip 48 valandoms be teismo sankcijos, ilgesniam laikui, su apylinkės teismo sankcija, apriboti viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikimą paslaugų gavėjui, kai paslaugų gavėjas ar jo naudojama informacinė ir ryšių technologijų įranga galimai dalyvauja nusikalstamoje veikoje.

2015m. kovo 3d. Vidaus reikalų ministras Sauliaus Skvernelis susitikime su verslo atstovais sakė, kad asmens teisių į privatumą ir duomenų apsaugą pastaruoju metu tampa tokia pat svarbi, kaip žmogaus gyvybės saugojimas. Įsigalėjus kibernetinio saugumo įstatymui, teisėsauga įgavo ir daugiau teisių kontroliuoti elektroninę erdvę. kibernetinio saugumo problemos mastas, remiantis naujausiais duomenimis sparčiai didėja. Šiai problemai skirtinas ypatingas dėmesys, todėl reikia verslo įsitraukimo ir pagalbos, įgyvendinat svarbius saugumo projektus.[5] Aiškinantis nusikaltimus elektroninėje erdvėje, kertasi du dalykai, duomenų apsauga ir žmogaus saugumo interesai.

Įkurta tarptautinė „Horizon2020“, didžiausia Europos Sąjungos mokslinių tyrimų ir inovacijų finansavimo programa.[6] Programos tikslas – kurti žinių ir inovacijų visuomenę, prisidėti prie „Europos 2020“ (iniciatyva „Inovacijų sąjunga“) įgyvendinimo ir Europos mokslinių tyrimų erdvės kūrimo. Kurios trukmė 2014-2020 metai. Programa „Horizontas 2020“ sprendžia visuomenės iššūkius, saugumo klausimus, padėdama įveikti atotrūkį tarp mokslinių tyrimų ir

[4] 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188.
[5] Interviu S. Skverelis. http://www.delfi.lt/news/ringas/politics/s-skvernelis-nuo-kibernetiniu-ataku-apsiginklavome-bet-truksta-specialistu.d?id=67325526 [žiūrėta 2015-03-03]
[6] Horizon 2020. http://ec.europa.eu/programmes/horizon2020/

rinkos, skatindama technologinių sprendimų pritaikymą. Norint užtikrinti piliečių saugumą tenka kovoti su nusikalstamumu, saugoti bendruomenes nuo stichinių ir žmogaus sukeltų nelaimių, terorizmu, užkirsti kelią kibernetiniams išpuoliams bei neteisėtai žmonių, narkotikų ir suklastotų prekių kontrabandai. „Horizon2020“ yra pateiktos darbo programos 2014-2015 metams dėl saugios visuomenės kūrimo. Skirtos kibernetinio nusikalstamumo, atsparumui mažinimui, kovai su terorizmu ir t.t. Moksliniai tyrimai ir inovacijos prisidės kuriant naujas technologijas, skirtas mūsų visuomenei apsaugoti, tuo pat metu nepažeidžiant piliečių privatumo ir puoselėjant jų pagrindines teises.

Baigiamojo darbo mokslinis naujumas ir tiriamos problemos ištyrimo lygis. Darbe analizuojama Lietuvos teisės moksle aktualūs klausimai, taip pat tarptautiniu bei nacionaliniu mastu. Tai nusikaltimų elektroninėje erdvėje tyrimas, problemos pagrindinės, sprendimo būdai, trūkumai. Naujumą atspindi kovos priemonės, tai konvencijos, teisės aktų įgyvendinimo klausimai. 2015 m. vasario 9 d. Europolas kovos su kibernetiniais nusikaltimais centras, kuriam vadovauja Europolas, patvirtino ES projektą skirtą kovai su mokėjimo kortelių sukčiautojais. Besiruošiant įgyvendinti projektą, pasiekta rezultatų reikšmingų, areštuoti 59 asmenys, iškeltos 32 teisminės bylos, paskelbta 17 nuosprendžių, sustabdyta penkių nusikalstamų grupuočių susijusių su elektroniniais nusikaltimais veikla. [7] Tai tik parodo, kad ieškoma aktyviai tinkamų priemonių, kovoti su nusikaltimais elektroninėje erdvėje. Didele dalį elektroninių nusikaltimų yra ištyręs teisėjas Steinas Schjolbergas. Teisėjas yra aukšto lygio tarptautinis ekspertas. [8] Jis vienas iš kompiuterinių nusikaltimų steigėjų, jis skelbė teisės aktus kovai su elektroniniais nusikaltimais. Plačiai išanalizavo elektroninius nusikaltimus ir kovas su jais. Smmit Ghosh išleistoje knygoje „Cybercrimes: A Multidisciplinary Alalysis“ paaiškina sudėtingus elektroninius nusikaltimus, analizuoja jų poveikį asmenims, visuomenei, bei tautoms. Tyrinėja kaip tinkamai reaguoti į kiekvieną nusikaltimą, kaip tradicinis mastymas ir įprasti įstatymai nepadės apsaugoti nuo nusikaltimų ir kaip paversti elektroninius nusikaltimus į technologijų ekonomikos augimą ir klestėjimą. Magistriniame baigiamajame darbe yra svarbu atskleisti tarptautines bei nacionalines organizacijas kurios kovoja su elektroniniais nusikaltimais, bei jų problematiką. JAV teisininkė, profesorė Susan W. Brennerio tyrinėja nusikaltimus elektroninėje erdvėje.[9] Brennerio nagrinėja nacionalinius ir tarptautinius nusikaltimus. Jos nuomone, dabartinė teisinė sistema pajėgi veiksmingai reaguoti į galimai didesnį kompiuterinių nusikaltimų mastą ir žalą nustatydama didesnes sankcijas, o tokių nusikaltimų sudėtingesnio tyrimo sėkmę daugiau lemia geresnis tarptautinis teisinis bendradarbiavimas. Atgrasymo funkcija taip pat kelia abejonių, nes paveikus

[7] Europolas patvirtino projektą kovai su kibernetiniais sukčiais. http://www.penki.lt/Sauga-saugos-sprendimai/Europolas-patvirtino-projekta-kovai-su-kibernetiniais-sukciautojais.im?id=349134&f=c [žiūrėta 2015-02-10]
[8] Biograpfhy of Stein Schjolberg. http://www.cybercrimelaw.net/biography.html [žiūrėta 2015-02-17]
[9] Susan W. Brenner https://www.udayton.edu/directory/law/brenner_susan.php [žiūrėta 2015-03-01]

atgrasymas yra susijęs ne tiek su kriminalizavimu ar naujomis sankcijomis, kiek su suvokimu, jog už tam tikrą veiklą bausmė yra neišvengiama. Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Steve Chon, nagrinėja įvairių tipų elektroninius nusikaltimus.

Lietuvoje nagrinėja nusikaltimus elektroninėje erdvėje Doc. Dr. D. Štitilis, Dr. R. Krikščiūnas, Prof. Dr. R. Petrauskas. Nagrinėja Lietuvos Respublikos prisijungimo prie konvencijos dėl elektroninių nusikaltimų ir jos įtakos Lietuvos nacionalinei baudžiamajai teisei.

Doc. Dr. D. Štitilis taip pat aiškinasi nusikaltimų klasifikaciją, nusikaltimų subjektus ir jų atlikimo būdus, teisinius elektroninių nusikaltimų aspektus, bei elektroninių nusikaltimų prevenciją. Teigia, kad Elektroniniai nusikaltėliai yra pelnę didesnį visuomenės palankumą negu tradiciniai nusikaltėliai ir kad elektroninis nusikaltėlis nėra mažiau pavojingas. Manoma, kad ateities grėsmė bus beveik proporcinga informacinių technologijų privalumams.[10]

Nikolaj Goranin ir Dalius Mažeika nagrinėja nusikaltimus elektroninėje erdvėje ir jų tyrimo metodikos.

Baigiamojo darbo reikšmė. Atliktas tyrimas, kuris gali suteikti naudos, tiriant nusikaltimus elektroninėje erdvėje. Ypač nusikaltimų tyrimo taktika, procesinių veiksmų ypatumų metodikos gairės, galėtų būti naudojamos tyrėjams darbe. Kai kurie teiginiai ir pasiūlymai gali būti panaudojami keliant pareigūnų kvalifikaciją, taip pat naudojami studijų procese. Gali turėti reikšmės mokslininkams, kurie galės naudotis šio tyrimo rezultatais, atlikdami tolimesnius tyrimus.

Tyrimo tikslas. Analizuoti ir atskleisti pagrindines problemas susijusias su nusikaltimais elektroninėje erdvėje, įvertinti tyrimo efektyvumą ir pateikti pasiūlymų dėl tyrimo tobulinimo.

Siekiant užsibrėžto tikslo keliami pagrindiniai ***tyrimo uždaviniai.***

1. Atskleisti nusikaltimų elektroninėje erdvėje kriminalistinę charakteristiką.
2. Išanalizuoti nusikaltimų elektroninėje erdvėje tyrimo reglamentavimo būklę ir galimas tobulinimo kryptis.
3. Atlikti lyginamąją analizę nusikaltimų tyrimo tarptautiniu ir nacionaliniu mastu, pateikti pasiūlymus ir įžvalgas dėl tyrimo metodikos plėtros krypčių.

Tyrimo metodika. Šiame darbe naudojami tokie metodai, tai dokumentų analizės, apibendrinimo, interviu ir bylų analizės.

Dokumentų analizės metodas naudojamas siekiant nagrinėti baudžiamosios teisės normas, įtvirtintuose nacionaliniuose ir tarptautiniuose teisės aktuose, užsienio šalių norminiuose aktuose.

Apibendrinimo metodas naudojamas nustatyti nacionalinius, tarptautiniuose teisės aktuose pateiktus teiginius ir iškeliant tam tikrą poziciją.

Interviu metodas naudojamas užduodant klausimus, renkama informaciją.

[10] Petrauskas, R.; Štitilis, D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p.15.

Bylų analizės metodas naudojamas siekiant nagrinėti baudžiamąsias bylas.

Tyrimo šaltiniai. Naudojausi moksline literatūra, moksliniais darbais, aktualių mokslinių žurnalų straipsniais „International Journal of Marine and Coastal Law", „International & Comparative Law Quarterly". Taip pat užsienio šalių ir Lietuvos respublikos įstatymais bei teisės aktais, konvencijomis. Tyrimo metu buvo apžvelgta Lietuvos Respublikos teismų praktika, tarptautinė teismų praktika.

Tyrimo struktūra. Magistrinis baigiamasis darbas susideda iš įvado, trijų pagrindinių dalių, iš kurių pirmojoje aptariama nusikaltimų elektroninėje erdvėje tyrimo kriminalistinė charakteristika, nusikaltimo padarymo būdas, asmuo padaręs nusikalstamą veiką, pasikėsinimo dalykas ir situacija. Antrojoje dalyje, nusikaltimų elektroninėje erdvėje tyrimo reglamentavimas, bendradarbiavimas, dokumentai, o trečioje nusikalstamų veikų tyrimas, nacionalinė ir tarptautinė praktika, prevencija, tobulinimo kryptys, taip pat pateikiamos išvados ir pasiūlymai, literatūros sąrašas, anotacija, santrauka lietuvių ir anglų kalba.

Ginamieji teiginiai. Nusikaltimai elektroninėje erdvėje yra sudėtinga opi problema, todėl valstybės turi dėti didesnes pastangas dėl nusikaltimų elektroninėje erdvėje tyrimo harmonizavimo, ieškoti efektyvesnių tyrimo ir prevencijos būdų.

1. NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE KRIMINALISTINĖ CHARAKTERISTIKA

Literatūroje nurodoma, kad elektroninių nusikaltimų samprata iki šiol nėra suformuota vieninga. Elektroninius nusikaltimus daug kur apibūdinami kaip ir kompiuteriniai nusikaltimai. Užsienio literatūroje dažnai naudojamas terminas cybercrime. Simbolizuoja globaliai stipriai kompiuterizuotai interneto visuomenei būdingas nusikalstamas veikas.[11] 2001 metais priėmus konvenciją dėl elektroninių nusikaltimų, vis dažniau pradėta naudoti elektroninių nusikaltimų samprata. Elektroninė erdvė tai vieta, kuri suteikia galimybes atsirasti naujoms nusikalstamoms veikoms, naujiems nusikalstamų veikų padarymo būdams kilti.[12] Elektroninė erdvė naudojama plačiai, todėl ir nusikaltimai elektroninėje erdvėje sparčiai daugėja. Vartotojams perduodant tam tikrą informaciją tarpusavyje, kuri gali būti svarbi tretiesiems asmenims ir taip siekdami ją pasisavinti gali padaryti vieną ar kelias nusikalstamas veikas kurios numatytos Lietuvos Respublikos baudžiamajame kodekse ir Europos Sąjungos teisės aktuose.

Kompiuteriniai nusikaltimai buvo pavartoti jau 1960 metais. Tarptautinės teisės specialistas teigia Ulrich Sieber, kad asmeninių duomenų perdavimas, laikymas, rinkimas, saugojimas, kelia pavojų piliečių teisėms[13]. Tokiu teiginiu specialistas norėjo pasakyti, kad bet koks neatsakingas poelgis su asmeniniais duomenimis, gali sudaryti sąlygas pažeidimams atsirasti, už kuriuos yra nustatyta baudžiamoji atsakomybė. Vienas iš pirmųjų susidomėjęs šia problema JAV Donn Parker 1976, taip apibrėžė kompiuterinio nusikaltimo sąvoką: visos tyčinės veikos, vienu ar kitu būdu susijusios su kompiuteriais, kurių pasėkoje 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.[14]

2005 metais Ženevoje vykusiame WSIS (World Summit of Informatikon Society) teminiame susitikime dėl elektroninio saugumo teigta, kad elektroniniai nusikaltimai gali būti suprantami kaip atakos prieš kompiuterinių sistemų ir tinklų infrastruktūrą internete, įskaitant interneto klastotes ir sukčiavimus. Buvo pasiūlyta iš elektroninių nusikaltimų sampratos eliminuoti su turiniu susijusias (angl. – content-related) nusikalstamas veikias, nes tokios veikos, kaip autorių teisių pažeidimai, rasizmas, ksenofobija ir vaikų pornografija daugumos teisininkų nuomone nėra priskiriami prie elektroninių nusikaltimų. Autorių teisių pažeidimai pagrinde remiasi civiliniais

[11] Civilka M., Lamanauskas T., Osinaitė G. ir kt./red. D. Sauliūnas. Informacinių technologijų teisė. - Vilnius: NVO Teisės Institutas, 2004.p. 511
[12] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universitetas, 2006. p. 230
[13] Sieber U. Legal aspects of Computer-Related Crime in the Information Society. Comcrime study, prepared for European Commission, 1998 http://www.oas.org/juridico/english/COMCRIME%20Study.pdf [žiūrėta2015-04-01]
[14] Petrauskas, R.; Štitilis, D. Kompiuteriniai nusikaltimai ir jų prevencija. Vilnius: Lietuvos teisės akademija, 2000, p. 5

santykiais ir daugumoje šalių nėra traktuojamos kaip nusikalstamos veikos. Autorių teisių pažeidimai labai dažnai išsprendžiami civiliniais teisiniais gynimo būdais. Vaikų pornografija visada buvo nusikalstama veika, tai yra ir iki paplintant informacinėms technologijoms.[15] 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.[16] Teisės mokslininkai nurodo, kad universaliausia sąvoka pateikiama 2001 metų Budapešto konvencijoje dėl elektroninių nusikaltimų.[17] Pateikiami ir neteisėti veiksmai: tai neteisėta prieiga prie kompiuterinės sistemos, neteisėtas kompiuterinės informacijos perėmimas, neteisėto turinio medžiagos siuntimas, taip pat tokie veiksmai, kuriais daromas poveikis kompiuterinei sistemai bei su turiniu susiję pažeidimai.[18] Kovojant su šiais nusikaltimais pasitelkiamos ne tik teisinės, bet ir techninės bei kitos priemonės.

Prof. Dr. V. E. Kurapka ir H. Malevskis rašė, kad kiekvienos nusikaltimų rūšies tyrimo metodikos pagrindinis elementas yra kriminalistinė nusikaltimų charakteristika.[19] Kriminalistas L. A. Sergeev teigė, kad kriminalistinė nusikaltimų charakteristika suprantama kaip esminių nusikaltimo bruožų - būdo, aplinkybių, nusikaltėlio, laiko, vietos, pasikėsinimo dalyko ir atskirų nusikaltimo tyrimo momentų visuma.[20] Kriminalistinė nusikaltimų charakteristika, tai duomenys apie tam tikrą nusikaltimą, kurie padeda atkleisti nusikaltimą. Kiekvienas nusikaltimas, palieka tam tikrus pėdsakus, kurie tampa pagrindiniu kriminalistikos charakteristikos duomenų šaltiniu. Prof. Dr. S. Matulienė daktaro disertacijoje, apibūdindama kriminalistines charakteristikas, išskiria V.G. Tanasevičiaus teiginį, kad kriminalistinė nusikaltimų charakteristika – „tai tam tikrų, tarpusavyje susijusių elementų sistema, tokių kaip nusikaltimo padarymo būdas, nusikaltimo padarymo aplinka, tiesioginis nusikaltimo objektas, jo apsaugos sąlygos nuo kėsinimosi, nusikaltėlio asmenybė, maskavimas ir kt.[21] Apibendrinant kriminalistinėje literatūroje išdėstytas pozicijas, manoma, kad formuluojant kriminalistinės nusikaltimų charakteristikos sąvoką, nėra racionalu detaliai vardinti jos struktūrinius elementus, kadangi kriminalistinė nusikaltimų charakteristika yra dinamiška mokslinė kategorija. Dinamiškumas pasireiškia tuo, kad jos turinys priklauso nuo atskirų nusikaltimų grupių, rūšių ar porūšių gebėjimo keistis. Be to, tie pasikeitimai

[15] Schjølberg S. & Hubbard A.M. Harmonizing national legal approaches on cybercrime // WSIS thematic meeting on cybersecurity. Geneva, 28 June – 1 July, 2005.p.4.
[16] Kiškis, M.; Petrauskas, R.; Rotomskis, I.; Štitilis, D. Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universitetas, 2006, p. 231.
[17] Civilka M., Lamanauskas T., Osinaitė G., Sauliūnas D. ir kt. Informacinių technologijų teisė.// Vilnius, NVO Teisės Institutas, 2004, p. 513.
[18] Broderic T. R. Regulation of the Information Technology in the European Union.// London, Kluver Law International, 2000, p. 67.
[19] Kurapka, V. E., Malevski, H., Šiuolaikinė nusikaltimų tyrimo koncepcija ir jos kriminalistinis bei procesinis uţtikrinimas. Pirmieji rezultatai. Jurisprudencija, 2003. 43 (35): 81
[20] Filipov, A. G., Problemy kriminalistiki. Izbranye statji [Problems of criminology. Featured articles]. Moskva:Jurlitinform, p. 83
[21] Matulienė S. Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija: daktaro.disertacija. soc. mokslai: teisė(01S).- Vilnius, 2004, p. 20

gali būti esminiai. Kriminalistinė nusikaltimų charakteristika – tai atviras kriminalistikos teorinės bazės blokas, kuris nuolat gali ir turi būti papildytas naujomis žiniomis.[22] Kalbant apie elektroninių nusikaltimų kriminalistinę charakteristiką, pirmiausia reikia kalbėti ir atskleisti kriminalistinės charakteristikos elementus, per kuriuos turima atskleisti savybes, kurios sudaro elektroninių nusikaltimų kriminalistinės charakteristikos turinį.

Apžvelgus literatūrą, galima teigti, kad nusikaltimų kriminalistinę charakteristiką sudaro šie elementai :

1. Nusikaltimo būdas.
2. Asmuo, padaręs nusikaltimą.
3. Nusikaltimo pasikėsinimo dalykas ir (arba) – nukentėjusysis.
4. Nusikaltimo situacija.

Vadovaujantis šiais elementais siekiama atskleisti kriminalistinės nusikaltimų charakteristikos turinį. Nustačius vieną elementą, gaunama informacijos apie kitą, ar kelis kitus elementus, apie jų požymius ir šiuos požymius atitinkančias savybes. Suradus vieną tos grandinės dalį, jos pagalba mes galime nustatyti kitą dalį arba ją visą.[23] Kriminalistinės charakteristikos elementai, svarbūs tuo, kad jais pasitelkiant siekiama atskleisti kokiu būdu buvo padarytas nusikaltimas, kokios priemonės buvo naudojamos siekiant padaryti nusikalstamą veiką. Kas padarė nusikalstamą veiką, atskleidžiami bruožai asmens padariusio nusikalstamą veiką, ketinimas, motyvas. Taip pats atskleidžiamas pasikėsinimo dalykas, nukentėjusysis asmuo. Aiškinamasi kokie asmenys linkę dažniau nukentėti nuo nusikalstamų veikų, bei kokiose situacijose dažniausiai galima nukentėti, bei padaromi nusikaltimai. Atskleidus kriminalistinės charakteristikos elementus, savybes, paaiškėja kriminalistinės charakteristikos turinys[24]:

1. Duomenys apie kriminalistikai reikšmingus konkrečios nusikaltimo grupės, rūšies ar porūšio požymius.

2. Duomenys apie dėsningus ryšius tarp atskirų kriminalistinės nusikaltimo charakteristikos elementų.

3. Duomenys, tarnaujantys tyrimo versijoms iškelti ir patikrinti.

Apibendrinant nusikaltimų elektroninėje erdvėje kriminalistinė charakteristika, tai informacijos apie nusikaltimų sudėties elementus, požymius, kvalifikavimą, bei kitus ypatumus visuma. Nusikaltimų elektroninėje erdvėje kriminalistinė charakteristika apima tokius nusikaltimų sudėčių elementus ir požymius: veika ir jos padarymo būdas, subjektas, pasikėsinimo dalykas ir

[22] Matulienė S. Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija: daktaro.disertacija. soc. mokslai: teisė(01S).- Vilnius, 2004, p. 21

[23] Jablokov, N., P. Kriminalistika [Criminalistics]. Moskva: Norma. 2009, p. 305

[24] Matulienė, S., Kriminalistinė nusikaltimų charakteristika nusikaltymų tyrimo metodikoje : teorinių ir praktinių problemų šiuolaikinė interpretacija. Daktaro disertacija. Socialiniai mokslai (teisė). Vilnius: Mykolo Romerio universitetas, 2004, p 22

nusikaltimo padarymo situacija. Nusikaltimų elektroninėje erdvėje kriminalistinės charakteristikos žinojimas palengvina, efektyviau spręsi įrodinėjimo uždavinius, įrodinėjimo dalyko ir ribų klausimus, laiku atlikti tyrimą, tinkamai kvalifikuoti šiuos nusikaltimus ir parinkti tinkamą bausmę.

1.1. Nusikaltimų elektroninėje erdvėje padarymo būdas

Nusikaltimų elektroninėje erdvėje padarymo būdas, tai subjekto veiksmai ir priemonės kuriais rengiamasis padaryti nusikalstamą veiką, padaroma bei slepiama. Tai nusikaltėlio elgesys rengiantis padaryti nusikaltimą, elgesys nusikaltimo vykdymo ir slėpimo metu.

Literatūroje pateikti elektroninių nusikaltimų įvykdymo būdai:

1. Perėmimo metodai.
2. Neteisėtos prieigos metodai.
3. Manipuliacijų metodai.
4. Kompleksiniai metodai.[25]

1. Perėmimo metodai. Perėmimo metodas gali būti atliekamas panaudojant, tiek pasiklausymo priemones, tiek objekto stebėjimas per vaizdo kameras, tiek atliekant tiesioginį prisijungimą prie kompiuterio, kompiuterinės sistemos ar kompiuterinio tinklo. Gali būti ir "šiukšlių rinkimas" kai pačiame objekte ieško šiukšlių, gali būti paprastų šiukšlių paieška, tai dokumentų, raštelių, popieriaus ar kitokių skiaučių ant kurių būtų užrašyta svarbi informacija. Taip pat renkamos ir elektroninės šiukšlės, kurios ieškomos elektroninėje ir kompiuterinėje erdvėje.

2.Neteisėtos prieigos metodai. Tai neteisėta prieiga prie kompiuterinės sistemos, be savininko leidimo, kurios tikslas informacijos pasisavinimas. Konvencijoje dėl elektroninių nusikaltimų nurodyta, kad „kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jų 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."[26] Lietuvos Respublikos baudžiamame kodekse neteisėtas prisijungimas prie informacinės sistemos kriminalizuota 198-1 straipsnyje. Kad kiltų baudžiamoji atsakomybė turi būti neteisėtai prisijungta prie informacinės sistemos ir taip pažeisdamas informacinės sistemos apsaugos priemones.

[26] Konvencija dėl elektroninių nusikaltimų.
http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2 [žiūrėta 2015-03-26]

Neteisėta prieiga prie informacinės sistemos dažniausiai pasireiškia: Įsilaužimas į informacinę sistemą ar kompiuterį, nusikaltėlio apsimetimas teisėtu kompiuterio vartotoju ir kita.

3. Manipuliacijų metodai. Tai elektroninių duomenų pasisavinimas, platinimas, paskelbimas, pakeitimas kitais duomenimis, panaudojimas. Prisideda sukčiavimas, kompiuteriniai virusai.

4. Kompleksiniai metodai. Pasireiškia dažniausiai įsibrovimu į informacinę sistemą, nusikalstamą veiką darantis asmuo dažniausiai apeina sistemos slaptažodžius pasinaudodamas saugumo spragomis. Šnipinėjimas vykdomas, tai programa, kuri be asmens žinios renka informaciją ir ją kaupia nurodytame pašte. Nukenčia elektronine bankininkystę besinaudojantys klientai kai bandoma gauti jų slaptažodžius siuntinėjant žinutes ar netikrus prisijungimo prie sistemos puslapius.

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys atlieka tyrimus, kai yra įvykdyta ar vis dar vykdoma:

Elektroninės paslaugos trikdymo ataka - tai veiksmas kuriuo metu trikdomas viešojo ryšių tinklo ir ar informacinės sistemos darbas arba viršuoju ryšių tinklu teikiamų paslaugų teikimas.

Informacinės sistemos užvaldymas – tai neteisėtas informacinės sistemos išteklių naudojimas arba neteisėtas prisijungimas prie informacinės sistemos.

Manipuliacijas elektroniniais duomenimis- elektroninių duomenų pasisavinimas, platinimas, paskelbimas, pakeitimas kitais elektroniniais duomenimis, elektroninių duomenų iškraipymas ar kitoks neteisėtas jų naudojimas.

Kenkėjiška programinė įranga - programinė įranga ar jos dalis, sukurta neteisėtai prisijungti ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar viešojo ryšių tinklo, sutrikdyti ar pakeisti (taip pat perimti valdymą) informacinės sistemos ar viešojo ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims.[27]

Vientisumo pažeidimas – viešojo ryšių tinklo ar jo dalies pažeidimas, sutrikdęs šiuo tinklu teikiamų viešųjų elektroninių ryšių paslaugų nepertraukiamą teikimą.[28]

Lietuvos Respublikos ryšių reguliavimo tarnybos tinklų ir informacijos saugumo departamento incidentų tyrimo skyrius 2014 metų veiklos ataskaitoje yra apibendrinti rezultatai. 2014 metai ištyrė 36 iš 136 incidentus pagal pranešimus gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos

[27] LR ryšių reguliavimo tarnybos direktoriaus įsakymas, dėl nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinio veiklos nuostatai. 2009 m. kovo 20 d. įsakymu Nr. 1V-348 2.8. p.

[28] Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys https://www.cert.lt/tipai.html [žiūrėta 2015-03-30]

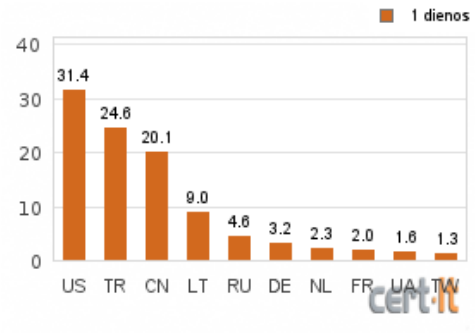
interneto naudotojų. Palyginti su 2013 metais (25 337 pranešimai), pranešimų buvo gauta 43 proc daugiau.

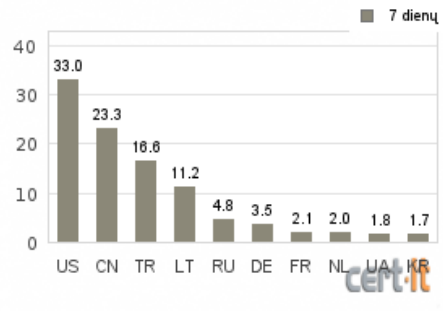
Prenešimų pobūdis **Apie kenkimo programinę įrangą**	
2014 metų laikotarpis	**Iš viso**
Apie kenkimo programinę įrangą	11276
Apie informacinių sistemų užvaldymą	4853
Apie elektroninės paslaugos trikdymo atakas	165
Apie elektroninių duomenų klastojimą	630
Apie vientisumo pažeidimus	35
Apie įrenginių saugumo spragas	13 827
Apie manipuliaciją elektroniniais duomenimis	32
Kita	5318

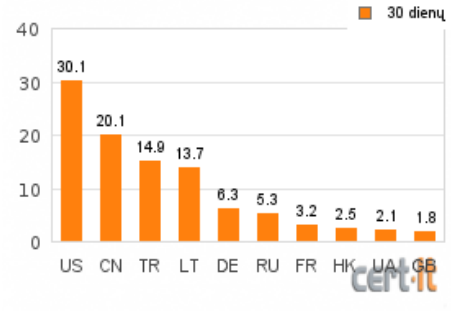
1.1. lentelė. CERT-LT 2014 m. nagrinėti pranešimai pagal jų tipus.

Iš pateiktos statistikos matyti, kad Lietuvoje didelė yra problema su elektroniniais nusikaltimais. Per 2015 m. CERT-LT siekia sustiprinti kovą su įrenginių saugumo spragomis: planuojama dar aktyviau bendradarbiauti su interneto paslaugų teikėjais, plėsti šviečiamąją veiklą raginant vartotojus pasirūpinti turimų tinklo įrenginių saugumu. Pranešimai apie įrenginių saugumo spragas, kurie priklauso asmenims kurie turi saugumo spragų. 2014 m. užfiksuota daug incidentų, susijusių su kenkimo programine įranga. CERT-LT ištyrė 11 276 kenkimo programinės įrangos panaudojimo atvejus. Kompiuterinės sistemos savininkas gali nežinoti apie informacinės sistemos pažeidimus. Antivirusinės programos turi vadinamuosius euristinius analizatorius (kurių veikimo tikslas – aptikti žalingą kodą net jei jo nėra antivirusinės programos duomenų bazėje, analizuojant kodo „elgesį“, jei jis būtų vykdomas). Neretai būna taip, kad pavojingą kodą antivirusinės programos atpažįsta tik po kelių dienų (pvz., taip buvo su „Geodo“ ir „Feodo“ virusu). Manoma,

kad 2015 metais virusų kūrėjai ir programišiai dar aktyviau kurs žalingus kodus išmaniesiems telefonams ir planšetiniams kompiuteriams.



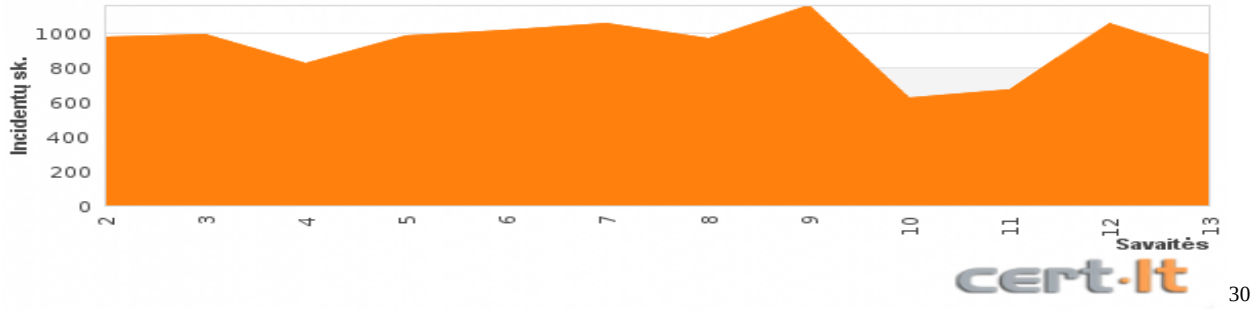




[29]

1.2 lentelė. Atakų šaltinio šalys (1 dienos, 7 dienų, 30 dienų intervale) [%]. Užfiksuotų kibernetinių atakų iš šalių procentinė dalis nuo visų užfiksuotų atakų.

Iš pateiktų statistikų matome, kad užfiksuotų kibernetinių atakų iš šalių Lietuva sudaro nemažą procentą ir yra ketvirtoje vietoje, o daugiausiai kibernetinių atakų atliekama Jungtinėse Amerikos Valstijose.



[30]

1.3. Lentelė. CERT-LT išspręstų incidentų skaičius per savaitę.

CERT-LT tiria elektroninių ryšių paslaugų teikėjų, užsienio tarnybų atliekančių tarptautinius incidentų tyrimus, taip atlieka tyrimus ir iš interneto vartotojų gautus pranešimus apie nusikaltimus

[29] Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, atakų šaltinio šalys. https://www.cert.lt/ataku_statistika.html [žiūrėta 2015-03-30]
[30] Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, išspręstų incidentų skaičius per savaitę. https://www.cert.lt/cert_lt_incidentu_statistika.html [žiūrėta 2015-03-30]

elektroninėje erdvėje. Apžvelgus nusikaltimų elektroninėje erdvėje padarymo būdus, galima daryti išvadą, kad tai opi problema, asmenys darantys nusikaltimą imasi neteisėtų būdų, kad apeitų sistemas, pasinaudoja spragomis, kuria virusus, pažeidžia asmenine erdve ir daro tai dėl asmeninės naudos.

Nusikaltimo būdo turinį sudaro nusikaltimo įrankiai, priemonės, nusikaltimo padarymo lygis, veiksmai prieš padarant nusikalstamą veiką, veiksmai nusikaltimo darymo metu, bei veiksmai po nusikaltimo padarymo - tai slėpimas, vengimas. Visi šie elementai leidžia užkirsti kelią nusikaltimo darymui, kurie gali būti įvykdomi žinomu ar numatomu būdu.

1.2. Nusikaltimą elektroninėje erdvėje padaręs asmuo

Nusikaltimą elektroninėje erdvėje padaręs asmuo, kaip ir bet kuris kitas asmuo padaręs nusikaltimą, tai pakaltinamas įstatymo nustatyto amžiaus sulaukęs asmuo, kaltas dėl pavojingos visuomenei ir priešingos teisei veiklos. Šių požymių visuma sudaro nusikaltimo subjekto turinį. Atsižvelgiant į elektroninių nusikaltimų paplitimą ir mastą, galima nusikaltimą padariusius asmenis išskirti pagal tam tikrus požymius. Elektroninius nusikaltimus vis dažniau daro jauni žmonės, studentai, moksleiviai, programuotojai mėgėjai, teroristai, nusikalstamų grupuočių nariai. Elektroniniai nusikaltėliai yra atliekami įvairiais būdais ir priemonėmis. Knygoje ‚Computer crime'[31] nusikaltimą padarius asmenis elektroninėje erdvėje skirsto:

1. Hakerius;
2. Tipinius nusikaltėlius;
3. Vandalus;

Hakeris – Tai įsilaužėlis į kompiuterines sistemas. „Vienas iš žymiausių įsilaužėlių tai 2006 metais hakeris, pasivadinęs „Iskorpitx" slapyvardžiu, sugebėjo sėkmingai pakeisti 38 549 svetainių turinius vienu metu. Manoma, kad „Iskorpitx" savo kontroversišką veiklą pradėjo 2003-siais metais, pasirodęs kaip pirmasis hakeris iš Turkijos. Toks jo nesustabdomas siautulys kibernetinėje erdvėje priartės prie 117 000 „nulaužtų" svetainių, tarp kurių yra ir jo šalies vyriausybinės svetainės. Pastaruosius mėnesius iš „Iskorpitx" imti pavyzdį stengiasi kuo daugiau jaunų Turkijos „hakerių" ir prisidėti prie jo „žygdarbių", taip stengiamasi tapti viena iš didžiausių svetainių gadintojų karalysčių pasaulyje ir pralenkti kol kas pirmaujančią Braziliją".[32] Hakeriai dažniausiai būna vis jaunesni asmenys ir moksleiviai, studentai, kurie gerai išmano programavimą, moka pasinaudoti spragomis ir taip nulaužti sistemas.

[31] Icove, D. *Computer Crime: a Crimefighter`s Handbook*. O'Reilly Media, 2005, 62 p.
[32] Hakeris http://lt.wikipedia.org/wiki/Hakeris [žiūrėta2015-03-30]

Vienas iš pavyzdžių, tai 2013 metais Lietuvoje prie Radviliškio V.Kudirkos pagrindinės mokyklos elektroninio dienyno neteisėtai prisijungę ‚programišiai' dviejų klasių moksleiviams prirašė neigiamų pažymių bei išsiuntinėjo pranešimus, kuriuose gausu necenzūrinių žodžių ir išsireiškimų, buvo sukurta necenzūrinių žodžių kupina apklausa, tokie pranešimai išsiuntinėti mokiniams ir jų tėvams. Už tokius mėgėjus programinius yra daug pavojingesni hakeriai profesionalai, kurie savo sugebėjimais daro žalą, kad gautų naudos. Jų kėsinimosi objektai elektroninės bankininkystės, įmonės.

Tipinis nusikaltėlis – Šie nusikaltėliai yra dažniausiai suaugę, pakaltinami. Užsiima šnipinėjimu, sukčiavimu bei piktnaudžiavimu.

Šnipinėjimas – Tai pagrobimas, rinkimas informacijos negavus tam leidimo. Taip pat vykdant kitos valstybės užduotį, pagrobiant informaciją ir ją perduodant kitai valstybei.

Sukčiavimas ir piktnaudžiavimas - Dažniausiai yra vidutinio amžiaus. Pasaulinio audito, mokesčių ir konsultacijų įmonių tinklo KPMG tyrimas „Profiles of a Fraudster" parodė, kad dažniausiai versle sukčiauja įmonių darbuotojai, kurie neretai turi pagalbininkų pačioje įmonėje ar už jos ribų. Tipinis sukčius dažniausiai yra vidutinio amžiaus darbuotojas (70 proc. atvejų sukčiaus amžius yra nuo 36 iki 55 m.), dirbantis aukščiausioje vadovų grandyje, administracijoje, rinkodaros ar pardavimų skyriuje. 54 proc. atvejų tai užimantis vadovaujančią poziciją asmuo.[33] Sukčiai vis labiau domisi galimybėmis sukčiauti elektroninėje erdvėje, nelegalių verslo sandorių sudaryme ir įvykdime. Tai patvirtina, kad dviem iš trijų sukčiavimo elektroninėje erdvėje atvejų veikė informacinių technologijų specialistai, kuriuos pati įmonė ir pasamdė. Įsitraukia dažnai nusikalstamos, organizuotos grupuotės, kurių tikslas pasisavinti neteisėtas pajamas elektroninėje erdvėje, vykdant kompiuterinį sukčiavimą, bei piktnaudžiavimą.

Lietuvos Aukščiausiojo Teismo Baudžiamojoje byloje 2K – 345/2014[34] pilietis V.M. kaltinamas, kad pagal LR BK 198 str 1d. kad būdamas valstybės tarnautoju Panevėžio apskrities vyriausiojo policijos komisariato Kelių policijos biuro viršininku, piktnaudžiaudamas tarnybine padėtimi, neteisėtai įgijo ir paskleidė neviešus elektroninius duomenis. Kelių policijos biuro viršininkas, piktnaudžiaudamas tarnybine padėtimi, neteisėtai įgijo ir paskleidė neviešus elektroninius duomenis, t. y. 2011 m. vasario 14 d. neteisėtai peržiūrėjo, atsispausdino duomenis apie R. J. Teistumą ir juos paskleidė tretiesiems asmenims.

Vandalai – Tai asmenys kurie elektroninius nusikaltimus įvykdo iš keršto, kad padaryti kuo daugiau žalos.

[33] KPMG tyrimas http://www.kpmg.com/LT/lt/IssuesAndInsights/ArticlesPublications/Puslapiai/profiles_of_a_fraudster.aspx [žiūrėta 2015-03-30]

[34] Lietuvos Aukščiausiojo Teismo Baudžiamoji byla 2K – 345/2014

Nusikaltimus elektroninėje erdvėje atlieka subjektai, kurie gerai išmano programavimą, turi gerus įgūdžius įsilaužti į kompiuterius, nulaužti ar apeiti saugos priemones, prisijungimo kodus, slaptažodžius. Subjektai gali būti tiek profesionalai, tiek mėgėjai, eiliniai naudotojai bei vartotojai, taip pat organizuotos grupuotės, įstaigos darbuotojai turintys galimybę prieiti prie informacinės sistemos.

1.3. Nusikaltimų elektroninėje erdvėje pasikėsinimo dalykas

Dauguma žmonių kiekvieną dieną naudojasi informacinėm technologijom. Tai naršo internete, keičiasi failais, naudojasi elektroniniu paštu, bendrauja ir susirašinėja socialiniuose tinkluose, prisijungia prie bankų sistemų ir atlieka finansines operacijas. Nukentėjusiuoju dėl elektroninių nusikaltimų gali tapti, tiek fiziniai tiek juridiniai asmenys.

Aukos nukentėjusios nuo elektroninių nusikaltimų gali būti tiesioginė ir netiesioginės.

1. Tiesioginės aukos, tai aukos kurios tiesiogiai susiduria su nusikalstama veika ir jos pasekmėmis.
2. Netiesioginė aukos, tai aukos, kurios netiesiogiai susiduria su nusikalstama veika ir jos pasekmėmis. Tai pavyzdžiui aukų artimieji, kurie taip pat pergyvena kartu su aukomis. Nusikaltimus elektroninėje erdvėje iššaukia, nepakankama duomenų apsauga. Prie nusikaltimo gali prisidėti ir pati auka, neapdairiai paviešinti asmeninius duomenis elektroninėje erdvėje, nepagalvodama apie galimas pasekmes.

Aukos pagal įsitraukimą į nusikaltimą gali būti skirstamos:

1. Aukos, visiškai neprisidėjusios prie nusikaltimo;
2. Aukos, pasielgusios nerūpestingai;
3. Aukos, išprovokavusios nusikaltimą.

Federalinis tyrimų biuras Nacionalinės kompiuterinių nusikaltimų tyrimų grupė teigia, kad 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.[35]

Nusikaltimų elektroninėje erdvėje latentiškumą didelį lemia:

1. Vartotojai nepastebi arba nesuvokia, kad buvo padaryta nusikalstama veika.
2. Nepranešimas atitinkamos įstaigoms, siekdami nesugadinti savo reputacijos, nenorėdami viešinti informacijos dėl spragų informacinėse sistemose bei informacinių sistemų apsaugos priemonėse.

[35] Kiškis, M.; Petrauskas, R.; Rootmskis, I.; Štitilis, D. Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universitetas, 2006, p. 240.

Jauno ir vidutinio amžiaus žmonės vis dažniau nukenčia nuo elektroninių nusikaltimų, kadangi šie žmonės vis dažniau naudojasi elektroninėmis paslaugomis, neabejingi naujovėmis. Nieko blogo neįtardami ir nenorėdami atsilikti nuo visuomenės vis dažniau viešina asmeninio gyvenimo detales. Tokiems žmonėms padidėja rizika tapti elektroninio nusikaltėlio aukomis. Ir tai patvirtina naujausias atliktas „Eurobarometro“ tyrimas 2014 m. spalio mėn.

Rezultatai rodo, kad 85 proc. interneto vartotojų Europos Sąjungoje mano, jog rizika tapti elektroninių nusikaltimų aukomis didėja, (taip manančių europiečių yra 9 proc. daugiau palyginus su 2013 metais), Lietuvoje tokios pozicijos laikosi 81 proc. gyventojų (6 proc. mažiau negu 2013 m.). 57 proc. Lietuvos gyventojų jaučiasi gerai informuoti apie elektroninių nusikaltimų pavojus. 74 proc. gyventojų nurodė, jog jiems kelia nerimą, kad internetinė asmeninė informacija nėra apsaugota interneto svetainių, o 69 proc. atsakė manantys, jog jų asmeninė informacija nėra apsaugota valdžios institucijų. 87 proc. lietuvių vengia atskleisti savo asmeninę informaciją internetu. 41 proc. lietuvių nurodė, kad, jiems atliekant sandorius internetu, labiausiai nerimą kelia, jog kažkas gali netinkamai panaudoti asmens duomenis, o 40 proc. atsakė nerimaujantys dėl mokėjimų internetu saugumo. 69 proc. lietuvių mano, jog jie patys gali pakankamai apsisaugoti nuo elektroninių nusikaltimų, pavyzdžiui, naudodami antivirusinę programinę įrangą; visoje Europos Sąjungoje taip manančių yra 74 proc. 62 proc. respondentų Lietuvoje nurodė turintys įdiegtą antivirusinę programą. 56 proc. Lietuvos gyventojų internetu naudojasi kasdien, 89 proc. internete skaito naujienas, 83 proc. naudojasi el. paštu, o 73 proc. - internetine bankininkyste.[36]

Pagrindinės situacijos kai patiriama arba tampama aukomis:

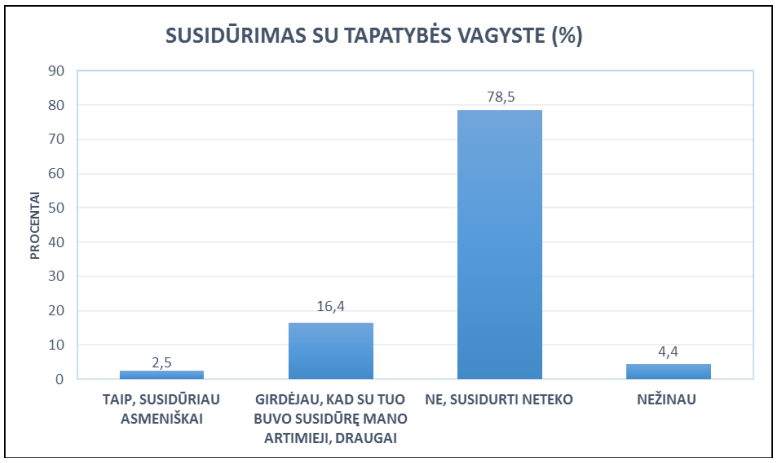
1. Kompiuteryje aptikta kenkėjiška programinė įranga;
2. Gauti apgavikiški elektroniniai laiškai, prašančio prieigos prie kompiuterio;
3. Negalėjimas pasinaudoti banko paslaugomis, dėl kibernetinių išpuolių;
4. Įsibrovimas į elektroninę pašto paskyrą;
5. Internetinė apgaulė, kai įsigytos prekės nebuvo pristatytos, suklastotos, arba ne tokios kokių buvo reikalaujama.
6. Prašymas susimokėti už tai, kad būtų gražintas įrenginio valdymas.
7. Asmens tapatybės vagyste pvz. apsiperka aukos vardu.
8. Atsitiktinis susidūrimas su vaikų pornografija internete.

Tarptautinio tyrimo „EU Kids Online“ 2013 m. duomenys. Net 76 proc. 9-16 metų Lietuvos vaikų turi savo asmeninį profilį socialinių tinklų svetainėse. Šis skaičius kur kas didesnis už Europos vidurkį – profilius turi 59 proc. vaikų. Daugiau nei trečdalis apklaustųjų teigia, kad savo

[36] Lietuvos Respublikos seimo Europos informacijos biuras http://www.eic.lrs.lt/index.php?18458626,[žiūrėta 2015-03-31]

profilyje skelbia tokius duomenis, kaip telefono numeris ar namų adresas, o 26 proc. prisipažįsta, kad visa jų skelbiama informacija yra prieinama viešai.[37] Pateikta informacija socialiniuose tinkluose suteikia sąlygas nusikalstamą veiką darantiems asmenims laisvai naudotis į socialinius tinklus įkeltomis nuotraukomis ir pateikta vieša informacija. Pateikti rezultatai rodo, kad vaikams trūksta žinių apie internete tykančius pavojus, todėl viešina savo asmeninę informaciją nenutokdami apie galima pasekmes.

2014 metais buvo atliktas sociologinis visuomenės nuomonės tyrimas, dėl elektroninėje ir neelektroninėje erdvėje vykdomų asmens duomenų vagysčių bei pavogtų asmens duomenų panaudojimo nusikalstamais tikslais. Tyrimo metu buvo apklausti 1005 respondentai iš įvairių Lietuvos regionų nuo 18 iki 75 metų amžiaus.



1.4. Lentelė. Susidūrimas su tapatybės vagyste.

Tyrimo metu buvo siekiama išsiaiškinti, jei asmenys yra susidūrę su tapatybės vagystėmis, tai kokios pasekmės jiems dėl to dažniausiai kildavo:

28 proc. – paimtas greitasis kreditas;

28 proc. – pavogti asmens dokumentai;

24 proc. – apgaulės būdu (telefonu, el. paštu) buvo išvilioti asmens duomenys;

20 proc. – kita;

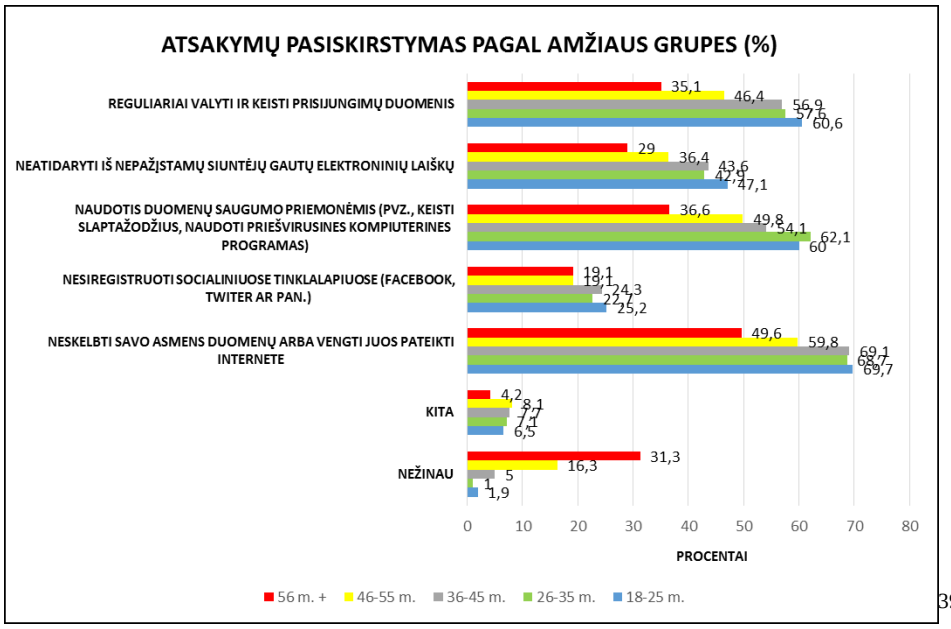
16 proc. – jūsų vardu pirktos prekės ir (ar) paslaugos internete;

8 proc. – iš banko sąskaitos dingo pinigai[38]

[37] Tyrimas EU Kids http://www.draugiskasinternetas.lt/repository/dokumentai/ataskaitos/2014/zero_to_eight_19aug.pdf [žiūrėta201503-31]

[38] 2014 m. Sociologinis visuomenės nuomonės tyrimas, dėl elektroninėje ir neelektroninėje erdvėje vykdomų asmens duomenų vagysčių bei pavogtų asmens duomenų panaudojimo nusikalstamais tikslais. file:///D:/My%20Documents/Downloads/apklausos%20analize_galutinis%20(1).pdf [žiūrėta2015-03-30]

Iš pateiktų atsakymų galima teigti, kad elektroniniai nusikaltėliai siekia pasisavinti svetimą turtą ir taip siekti asmeninės naudos, praturtėti. Siekia apeiti kaip įmanoma geriau saugos priemones, nulaužti sistemas, išvilioti asmenų duomenis, taip paimti prekių ir greitųjų kreditų. Nukentėjusiųjų nuo elektroninių nusikaltimų procentas taip pat didėja, tai kelia dideles problemas ir susirūpinimą.



[39]

1.5. Lentelė. Atsakymų pasiskirstymas pagal amžiaus grupes.

Kad nukentėjusiųjų asmenų nuo elektroninių nusikaltimų taptų vis mažiau, asmenys turėtų atsakingiau elgtis elektroninėje erdvėje ir laikytis saugumo priemonių:

1. Kompiuteryje turėti įdiegtas geras antivirusines programas ir atnaujinti operacinę sistemą;
2. Neatidarinėti elektroninių laiškų iš nežinomų ar įtartinų asmenų;
3. Mažiau teikti asmeninės informacijos elektroninėje erdvėje;
4. Lankytis tik tokiose internetinėse svetainėse kurios yra patikimos ir žinomos;
5. Skirtingose internetinėse svetainėse patartina naudoti skirtingus slaptažodžius.

Apibendrindami pasikėsinimo dalyko sampratą, bei turinį, galime konstatuoti, kad nukentėjusysis tai fizinis ar juridinis asmuo, kuriam yra padaryta žala, fizinė, turtinė ar moralinė. Pasikėsinimo dalykas gali turėti įtakos nusikaltimo padarymui, tai neatsakingas elgesys socialiniuose tinkluose, privačios informacijos viešinimas, neatsakingas elgesys su nežinomais laiškais iš įtartinų asmenų.

[39] 2014 m. Sociologinis visuomenės nuomonės tyrimas, dėl elektroninėje ir neelektroninėje erdvėje vykdomų asmens duomenų vagysčių bei pavogtų asmens duomenų panaudojimo nusikalstamais tikslais. file:///D:/My%20Documents/Downloads/apklausos%20analize_galutinis%20(1).pdf [žiūrėta2015-03-30]

1.4. Nusikaltimų elektroninėje erdvėje situacija

Elektroninė erdvė sudaro galimybes ne tik palengvinti bendravimą, sudaro galimybę naudotis tam tikromis paslaugomis, plėtoti verslą, bet taip pat sukelia ir daug rizikos.

Atsižvelgiant į šiandieninę situaciją, dėl nuolat kintančių elektroninių nusikaltimų pasireiškimo būdų, padidėjusio masto, elektroninius nusikaltimams galima priskirti šiuos bruožus:

1. Didelės elektroninių nusikaltimų atakos prieš informacines sistemas.

2.Užkrėstų ir valdomų kompiuterių atakos. Asmenys rengiantys šias atakas, sieja pastovūs tarpusavio ryšiai ir pasiskirstymas vaidmenimis ar užduotimis. Šios atakos susijusios su organizuotu nusikalstamumu.

3.Nusikalstamos veikos padaromos, panaudojant kompiuterio virusus su tikslu užkrėsti kompiuterius.

Nusikaltimai vykdomi elektroninėje erdvėje:

1. Nelegali prekyba;
2. Neapykantos skatinimas ar kurstymas;
3. Šmeižtas;
4. Sukčiavimas internete;
5. Asmens duomenų vagystės ir su tuo susiję nusikaltimai;
6. Vaikų seksualinis išnaudojimas;
7. Įsilaužimai į sistemas;
8. Draudžiamo turinio platinimas;
9. Autorinių teisių pažeidimai ir kt.

Elektroninė erdvė taip pat yra laikoma, kaip nusikaltėliams priemonė veikti:

1. Informacijos apie žudymo įrankiu paieškai;
2. Informacijos mainai tarp teroristinių grupuočių;
3. Nusikaltimų planavimas;
4. Prekyba uždraustais, padirbtais vaistais, narkotinėm bei psichotropinėm medžiagom.

Užkrėtus kompiuterius pavojinga programine įranga, siekiama:

1. Finansinės naudos gauti. Tai sukčiavimas, turto prievartavimas, pinigų vagystės iš internetinės bankininkystės sąskaitų.

2. Komercinį šnipinėjimą atlikti. Siekimas sužlugdyti konkurentus, kompromituojančios informacijos rinkimas.

3. Politinį šnipinėjimą atlikti. Tai siekimas perimti neviešą informaciją, valstybės paslaptis.

4. Informacinį karą ir kibernetinę ataką atlikti. Pavyzdžiui Estijoje ataka įvyko 2007 metais. Buvo paralyžiuotas pagalbos skambučių centro darbas ir neveikė dviejų pagrindinių šalies bankų internetinės bankininkystės sistemos, labai didelės žalos nei užpultoms privataus verslo, nei vyriausybės svetainėms nepadaryta. Estijos institucijos ir įmonės buvo puolamos iš kompiuterių, esančių 173 valstybėse visame pasaulyje. Tikėtina, kad daugelis šių kompiuterių savininkų net nežinojo, kad jų kompiuteriu buvo pasinaudota atakai.[40] Tyrimo metu specialistai nustatė, kad kompiuterinės atakos prieš Estiją nebuvo viena suderinta tęstinė ataka, bet nepaisant to, tai buvo spontaniškas pykčio iššauktas veiksmas, kurį atliko keli skirtingose lokacinėse vietose buvę asmenys. Techniniai duomenys parodė, kad kompiuterinių atakų šaltiniai buvo išsiskirstę po visą pasaulį, o ne susitelkę keliose vietose. Kompiuterinis kodas, kuris sukėlė DDoS atakas buvo paviešintas ir platinamas daugelyje rusiškų pokalbių kambariuose, kur sovietinių memorialų perkėlimo tema buvo labai aktyviai diskutuojama. Analitikai taip pat teigia, kad nepaisant prieigos prie Estijos vyriausybinių įstaigų užblokavimo pasitelkus kenksmingą kodą, nebuvo aišku, ar atakų tikslas tikrai nebuvo tik interneto prieigos sutrikdymas.[41]

2013 m. Šiaurės Korėjos atakos prieš pietų Korėjos informacinių technologijų infrastruktūrą. Buvo pavogta daug duomenų, susijusių su nacionaline infrastruktūrą, įskaitant cheminių medžiagų saugyklas, taip pat informaciją, susijusią su asmenų finansiniais reikalais.[42]

5. Asmens duomenų vagystėms atlikti. Tai prisijungimo duomenys, slaptažodžiai, kurie panaudojami prisijungti prie socialinių tinklų, elektroninių parduotuvių.

Lietuvos Respublikos prokuratūros 2014 metų veiklos ataskaitoje yra pateikti duomenys apie nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumą.

„2014 m. užregistruotos 1089 nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui. Tai beveik dvigubai arba 43 proc. daugiau nei 2013 m. (622 veikos) ir net septynis kartus daugiau nei 2012 m. (154 veikos). 2014 m. daugiausia nusikalstamų veikų (820) registruota dėl neteisėtų prisijungimų prie informacinių sistemų (BK 1981 str.), 235 nusikalstamos veikos – dėl neteisėto elektroninių duomenų perėmimo ir panaudojimo (BK 198 str.). 2014 m. pradėti 192 ikiteisminiai tyrimai dėl šios kategorijos nusikalstamų veikų, t. y. du kartus daugiau nei 2013 m. (92) ir net tris kartus daugiau nei 2012 m. (63).

Statistinių duomenų analizė rodo, kad (kaip ir 2013 m.) daugiausia ikiteisminių tyrimų (121) buvo pradėta ir atliekama pagal BK 1981 str. dėl neteisėtų prisijungimų prie informacinių sistemų (2013 m. – 55, 2012 m. – 11), taip pat pagal BK 198 str. dėl neteisėto elektroninių duomenų perėmimo ir panaudojimo – 52 (2013 m. – 38, 2012 m. – 41).

---

[40] http://www.delfi.lt/news/daily/world/pirmaji-kibernetini-kara-laimes-estija.d?id=59952503 [2015-03-31]

[41] Wilson C. Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 3. January 29, 2008. https://www.fas.org/sgp/crs/terror/RL32114.pdf [žiūrėta2015-03-31]

[42] http://www.technologijos.lt/n/technologijos/it/S-36520 [žiūrėta2015-03-31]

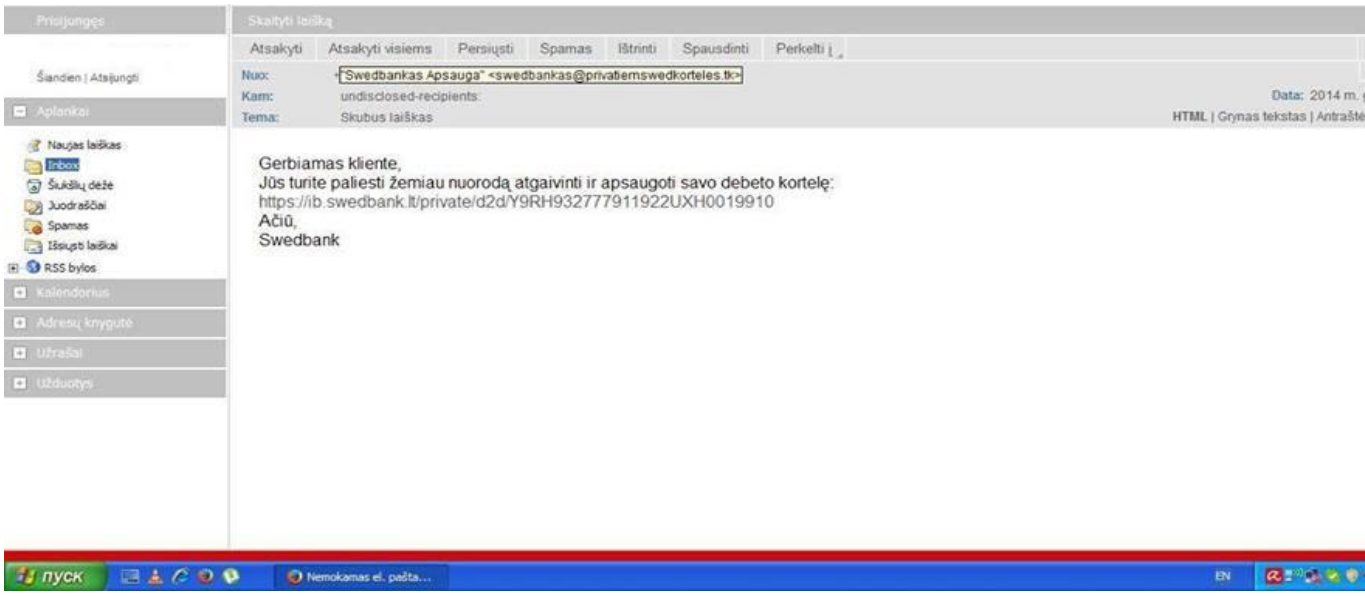
2014 m. iš viso ištirtos 994 nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui. Tai beveik du kartus daugiau nei 2013 m. ir beveik dešimt kartų daugiau nei 2012 m.“ [43]

Dalis nusikaltimų atliekama juokais dėl socialinių politinių pažiūrų, o kiti profesionalų veiksmai, kaip siekimas pasipelnyti ir tai jų verslas. Ši ataskaita parodo nusikaltimų tyrimo rezultatus ir spartų šių nusikaltimų augimą. Dažniausiai neteisėtai įgyjami svetimų elektroninių mokėjimo priemonių duomenys, skirti prisijungti informacinių sistemų ir atliekamos neteisėtos finansinės operacijos. Taip vienu metu padaromos kelios ir daugiau nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui.

Nusikalstamos veikos, atliekamos elektroninėje erdvėje, pasižymi ypač dideliu įvairiapusiškumu. Siekiant atskleisti jų pavojingumą, pateikiami nusikaltimų elektroninėje erdvėje situacijos:

Nusikaltimu elektroninėje erdvėje, sukčiavimas ir vagystė.

2014 metais vasario 27d. Swedbank Lietuvoje pateikė informaciją, kad platinami elektroniniai laiškai su nuoroda į suklastotą Swedbank internetinį puslapį, kuriame prašoma pateikti prisijungimo duomenis - PIN generatoriaus kodus. Pranešama, kad tokiuose puslapiuose savo duomenų nesuvedinėti.



1.6. Lentelė. Elektroninio laiško pavyzdys.

Kevin Mitnick – žymiausias pasaulio hakeris, kuris buvo nuteistas. Jis buvo suimtas FTB 1995 m. vasario 15 d., Mitnikas buvo suimtas už sukčiavimą ir įsilaužimą į „Fujitsu“, „Motorola“, „Nokia“, „Sun Microsystems“ kompiuterių sistemas. [44]Jis kalėjime sedėjo 5 metus, buvo paleistas 2000 m. sausio 21d. Per prižiūrimą paleidimą, kuris baigėsi 2003 m. sausio 21d.

[43] 2014 m. Lietuvos respublikos prokuratūros veiklos ataskaita file:///D:/My%20Documents/Downloads/ataskaita-2014%20(1).pdf [žiūrėta 2014-03-31]
[44] Kevin Mitnick http://lt.wikipedia.org/wiki/Kevin_Mitnick [žiūrėta 2015-03-31]

Mitnikas padarė daugiau kaip 100 milijonų JAV dolerių nuostolių vien per 1982 – 1990 metus. Tai tik parodo, kokie pavojingi nusikaltimai elektroninėje erdvėje, sunku tokius nusikaltimus greitai sustabdyti, todėl padaroma didelė žala. Sukčiavimo būdu gautų lėšų skaičius didėja, taip pat pasikėsinimai į bankus, identifikavimo duomenis

Elektroninių nusikaltimo sąmokslo pavyzdys tai L. Levino kuriam padėjo daug bendrininkų. kurie įsilaužė į „Citibank“ banko kompiuterius ir elektroniniu būdu iš banko klientų sąskaitų pasisavino apie 10 milijonų JAV dolerių. Klientų sąskaitos buvo „Citibank“ banko filialuose JAV Kalifornijos valstijoje, Suomijoje, Vokietijoje, Olandijoje, Šveicarijoje ir Izraelyje. V.Levinas 1995 metais buvo sulaikytas Londone ir išduotas JAV. 1998 m. vasario 24 dieną jis buvo nuteistas trejų metų laisvės atėmimo bausme ir įpareigotas sumokėti „Citibank“ bankui 240 tūkstančių JAV dolerių.[45] Kaltininko veiksmų neteisėtumas pasireiškia tuo, kad jis, norėdamas prisijungti prie elektroninės bankininkystės sistemos, neteisėtai naudoja kitiems asmenims priklausančius prisijungimo kodus ir identifikavimo duomenis. Dėl to banko tarnybinėje stotyje įdiegta sistema automatiniu režimu šiuos duomenis įvedusį asmenį identifikuoja kaip teisėtą elektroninės bankininkystės sistemos vartotoją ir leidžia atlikti norimas finansines operacijas. Tokiais veiksmais pažeidžiamos elektroninės bankininkystės sistemos apsaugos priemonės, kurios yra skirtos užtikrinti, kad prie šių sistemų paskyrų galėtų prisijungti tik banko klientai, sudarę su banku elektroninės bankininkystės sutartis.

Taip pat pavojinga nusikalstama veika yra vagystės elektroninėje erdvėje.

Pavyzdžiui, 2015 metais vasario 15d.,spaudoje pasirodė pranešimas, kad Bendra Interpolo, Europolo ir apsaugos sistemų kūrėjos „Kaspersky Lab“ operacija, kuri truko dvejus metus, atskleidė nusikaltimą, kurio metu užpuolikai pasisavino apie milijardą JAV dolerių. Nuo kenkėjiškos veiklos nukentėjo apie 100 bankų visame pasaulyje. Nusikalstamą grupuotę „Carbanak“ sudaro nusikaltėliai iš Rusijos, Ukrainos, Kinijos ir kai kurių Europos šalių. Ji naudojama tikslinėms atakoms būdingus metodus, tačiau skirtingai nuo daugelio ankstesnių incidentų šis apiplėšimas pasiekė aukštesnį lygį: nusikaltėliai gali pavogti pinigus tiesiogiai iš bankų, o ne iš vartotojų. pat rasta duomenų vagystės įkalčių.Hakeriai siuntė elektroninius laiškus su kenkėjiška programa pavadinimu „Carbanak“ šimtams banko darbuotojų, tikėdamiesi užkrėsti administratoriaus kompiuterį. Po vieno iš banko darbuotojų kompiuterio užkrėtimo užpuolikas gaudavo prieigą prie vidinio tinklo, surasdavo piniginių operacijų administratoriaus kompiuterį ir pradėdavo jo ekrano vaizdo stebėjimą. Tokiu būdu gauja žinojo kiekvieną banko personalo darbo detalę ir galėjo imituoti įprastus veiksmus, pervedant pinigus į sukčių sąskaitas. Atėjus laikui pasiimti pinigus, nusikaltėliai panaudodavo internetinę bankininkystę arba mokėjimo sistemas

[45] Cyber attacks: Removing reodblocks to invetigation and informatikon sharing.http://www.gpo.gov/fdsys/pkg/CHRG-106shrg69358/html/CHRG-106shrg69358.htm [žiūrėta2015-03-31]

pinigų pervedimui iš banko sąskaitos į savo. Nusikaltėlių sąskaitos buvo atidarytos Kinijos ir Jungtinių Amerikos Valstijų bankuose, tačiau ekspertai neatmeta galimybės, kad nusikaltėliai taip pat gali laikyti pavogtus pinigus ir kitose šalyse.[46] Minėtas atvejis tik parodo, kad sukčiavimas ir vagystė naudojant kompiuterines sistemas tampa vis pavojingesni.

2015-04-10 dieną spaudoje pasirodė pranešimas, kad Japonijoje per 82 tūkst. asmeninių kompiuterių buvo užkrėsti nauju virusu, pranešė Tokijo policijos valdybos kibernetinio saugumo padalinys. Kenkėjiška programa, vartotojams atliekant banko operacijas internetu, automatiškai perkelia jų lėšas į svetimas sąskaitas. Užkrėstų kompiuterių nustatyta Japonijoje, kiti – Europos ir Azijos šalyse. Patirta žala siekia 2,9 mlrd. Jenų. Vasario pradžioje Tokijo apygardos teismas nuteisė aštuoneriems metams kalėti kibernetinių atakų teroristą Yusuke Katayama, kuris platino teroristinius grasinimus per interneto forumus. Nusikaltėlis šiuo tikslu sukūrė specialius virusus, leidžiančius per nuotolį naudotis svetimais kompiuteriais nepageidaujamiems laiškams siuntinėti.[47]

Taip pat didelė problema yra, netinkamas elgesys internete, tyčiniai veiksmai, kurie nukreipti pažeminti, šmeižti, įbauginti, kontroliuoti, manipuliuoti, įžeisti, melagingai diskredituoti asmenį. Tai veiksmai, kuriais siekiama kitaip pakenkti arba varžyti kitą asmenį ir interneto turinys, kuris yra žalingas piliečiams, įskaitant vaikus.

Pavyzdžiui, vieno dienraščio internetiniame portale komentarą apie iš darbo Kauno Vytauto Didžiojo universitete atleistą homoseksualų dėstytoją A.Z. parašęs 63 metų Šilutės rajono gyventojas A. G. užsidirbo teistumą – teismas konstatavo, kad neįgalus vyras viešai ragino smurtauti, fiziškai susidoroti su homoseksualios orientacijos asmenimis.[48] Socialiniai tinklai taip pat yra priemonė ir didelė problema, kurią nusikaltėliai naudoja seksualiai išnaudojamiems vaikams surasti, pokalbiams su vaikais „nevaikiškomis“ temomis, rinkti medžiagą, kuri vėliau panaudojama patyčioms ir įbauginimui, sudaryti galimybę kontroliuoti vaiką.

Vienas pirmųjų tyrimų, siekiant išsiaiškinti vaikų seksualinio išnaudojimo mastus, pusę milijono gyventojų turinčiame Didžiosios Britanijos mieste Edinburge buvo atliktas 2008 metais. Paaiškėjo, kad vien šiame mieste 700 kompiuterių naudojosi privačiu interneto tinklu (P2P), kuriame keičiamasi pornografinio turinio informacija ir vaizdais. 2010–1012 metais penki Didžiosios Britanijos policijos padaliniai konfiskavo apie 26 mln. vaikų pornografijos vaizdų. Tai padarė tik penki padaliniai. Remiantis skaičiavimais, visoje šalyje tuo metu cirkuliavo apie 300 mln. vaikų pornografijos vaizdų. Apie 50–60 tūkst. žmonių keičiasi tokia medžiaga. 2004 metais buvo

[46] Hakeriai pavogė milijardą dolerių. http://topcom.lt/hakeriai-pavoge-milijarda-doleriu/ [žiūrėta2015-03-31]

[47] Siaučia vienu pavojingiausių virusų. http://www.delfi.lt/mokslas/technologijos/siaucia-pinigus-vagiantis-kompiuteriu-virusas-zala-skaiciuojama-milijardais.d?id=67667720 [žiūrėta2015-04-10]

[48] Lietuvoje nuteistas komentatorius. http://www.technologijos.lt/n/technologijos/it/S-21755/straipsnis/Lietuvoje-nuteistas-dar-vienas-interneto-komentatorius?l=2&p=1 [201503-31]

sulaikyta tik apie 2,5 tūkst. tokių nusikaltėlių.[49] Tai tik keletas neteisėtų veikų pavyzdžių kurių gausu elektroninėje erdvėje. Apibendrinant galima teigti, kad elektroninėje erdvėje gausu būdų nusikaltimams atlikti. Elektroninėje erdvėje gausu nusikaltimų tai sukčiavimų, vagysčių, pornografijos, neapykantos nusikaltimų, autorių teisių pažeidimų, neteisėta prieiga, neteisėtas naršymas ir kita. Neteisėtos veikos elektroninių ryšių sektoriuje išsiskiria dideliu įvairumu ir pavojingumu, o jų pasekmės asmens privatumo pažeidimas, materialiniai nuostoliai, tarptautiniai konfliktai.

Šnipinėjimo atvejai Lietuvos Respublikoje:

2014 m. gruodžio 29 d. slaptos operacijos metu, kurioje dalyvavo LR generalinės prokuratūros, Lietuvos kriminalinės policijos biuro ir AOTD pareigūnai, sulaikyti du šnipinėjimu prieš Lietuvos interesus įtariami asmenys – Lietuvos kariuomenės Karinių oro pajėgų karininkas ir Rusijos Federacijos bei LR pilietybes turintis asmuo, kuriam, kaip įtariama, Lietuvos kariuomenės karininkas slapta teikė žvalgybinę informaciją. Asmuo, kuriam, kaip įtariama, Lietuvos karininkas teikė informaciją, daug metų tarnavo Sovietų Sąjungos kariuomenėje, turėjo pulkininko karinį laipsnį, yra tarnavęs Sovietų Sąjungos kariuomenės dalinyje, kuris buvo dislokuotas Lietuvoje. Įtariamasis žvalgybinės operacijos prieš Lietuvą laikotarpiu periodiškai lankydavosi Lietuvoje, kur turėjo kilnojamojo ir nekilnojamojo turto, palaikė senus ir mezgė naujus draugystės ryšius su LR piliečiais bei turėjo kitų sąsajų su Lietuva.

Aktyvius žmogiškosios žvalgybos veiksmus prieš Lietuvos gynybinius interesus 2014 m. taip pat vykdė GRU atstovai po diplomatine priedanga. Naudodamiesi diplomatiniu statusu GRU atstovai įvairiais žvalgybiniais metodais rinko Rusijos kariniam planavimui reikalingą informaciją. Informacija buvo renkama lankantis įvairaus pobūdžio renginiuose, konferencijose ir diplomatiniuose priėmimuose. Šių renginių metu buvo siekiama išgauti kuo naudingesnės informacijos iš asmenų, kurie dažniausiai net neįtarė, kad prieš juos buvo vykdomos žvalgybinės apklausos.

Šiandieninė situacija, dėl elektroninių incidentų nukreiptų prieš Lietuvos Respubliką:

Didžiąją dalį elektroninių incidentų, nukreiptų prieš Lietuvos valstybės duomenų apdorojimo ADA sistemas ir tinklus, 2014 metais vykdė užsienio valstybių žvalgybos ir saugumo tarnybos kontroliuojami ir remiami elektroniniai įsibrovėliai. Rusijos žvalgybos ir saugumo

[49] Vaikų pornografija. http://www.15min.lt/naujiena/aktualu/lietuva/britu-ekspertas-johnas-carras-vaiku-pornografijos-naudotojams-ir-platintojams-neuztektu-visu-pasaulio-kalejimu-56-388174 [žiūrėta2015-03-31]

tarnybos, ypač FSB bei Gynybos ministerijos struktūriniai padaliniai ir su šiais padaliniais susiję subjektai, turi didžiausius kibernetinius pajėgumus, nukreiptus rinkti informaciją, trikdyti Lietuvos ADA sistemų ir tinklų funkcionavimą, juos užvaldyti, tikrinti Lietuvos atsakingų institucijų gebėjimą gintis.[50] Rusija, naudodama kibernetinius pajėgumus, užvaldydama kompiuterinę įrangą, telekomunikacijų įrenginius, ADA tinklus ir sistemas, mobiliuosius įrenginius, siekia įgyti pranašumo gynybos, politikos, ekonomikos, technologijų ir kitose srityse.

AOTD pateiktoje 2013 m. AOTD grėsmių nacionaliniam saugumui vertinimo ataskaitoje, teigia, kad vykdydamos kibernetinį šnipinėjimą Rusijos tarnybos, su jomis susiję ar šių tarnybų kontroliuojami bei remiami kibernetiniai įsibrovėliai siekė apkrėsti kompiuterius, ADA sistemas ir tinklus šnipinėjimui skirtomis programomis arba kenksmingais kodais. Šnipinėjimo programų veikla arba šių programų pėdsakai buvo aptikti daugelio Lietuvos valstybės institucijų ADA sistemose, tinkluose. 2014 m. aktyviai veikė su Rusija siejama „Sofacy“ grupuotė, kurios vykdomos kibernetinės atakos buvo nukreiptos prieš NATO, atskirai JAV ir jos sąjungininkių karines institucijas, ambasadas, gynybos sektoriaus įmones, Rusijos opozicijos politikus ir disidentus, tarptautinę žiniasklaidą. Šios grupuotės veikla buvo pastebėta ir Baltijos valstybėse.[51]

Pateikti pavyzdžiai tik patvirtina, kad grėsmių sulaukiama nemažai ir turima ieškoti priemonių kaip tas grėsmes laiku sustabdyti ir užkirsti joms kelią toliau plisti. Šios grėsmės kelia pavojų ne tik nacionaliniam, bet ir tarptautiniam saugumui.

2. NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE TYRIMO REGLAMENTAVIMAS

2.1. Nusikaltimų elektroninėje erdvėje tarptautinis reglamentavimas ir bendradarbiavimas

Nusikaltimus vykdantys asmenys ir nusikaltimo aukos gali būti bet kurioje, nebūtinai toje pačioje valstybėje, todėl tarptautinis teisėsaugos institucijų bendradarbiavimas yra būtinas, siekiant kovoti su nusikaltimais tarptautiniu mastu.[52] Tarptautinė kova su elektroniniais nusikaltimais priklauso nuo patikimų bendradarbiavimo priemonių ir vieningai suderintų valstybinių įstatymų. Remiantis bendru dvigubo baudžiamumo principu, efektyviam tarptautiniam bendradarbiavimui yra būtinas baudžiamosios teisės nuostatų suderinimas, su tikslu išvengti saugaus prieglobsčio bet kurioje valstybėje sukūrimu.[53] Tarptautinis reglamentavimas, tai

[50] AOTD prie KAM 2015 m. veiklos ataskaita. file:///D:/My%20Documents/Downloads/aotd%202014%20viesoji%20ataskaita.pdf [žiūrėta2015-04-07]
[51] AOTD prie KAM Gresmių Nacionaliniam saugumui vertinimas 2013m file:///D:/My%20Documents/Downloads/aotd%202013%20gr%C4%97smi%C5%B3%20nacionaliniam%20saugumui%20vertinimas%20(ns)%20(1).pdf [žiūrėta2015-04-07]
[52] Sofaer A.D., Goodman S.E. Cyber Crime and Security The Transnational Dimensijon http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf [žiūrėta 2015-03-31]
[53] WSIS Thematic Meeting on Cybersecurity. Geneva, June 28 - July 1, 2005. http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf [žiūrėta 2015-03-31]

tarptautinių organizacijų kurios kovoja su elektroniniais nusikaltimais veiklos sritis. Be to, viena iš pagrindinių problemų, su tinkamai apibrėžti elektroniniais nusikaltimais yra konkrečių statistinių duomenų trūkumas. Nusikaltimų elektroninėje erdvėje ataskaitos yra savanoriškos, tai užregistruoti nusikaltimai. Šie skaičiai yra tikrai daug mažesni nei faktinis padarytų nusikaltimų skaičius. Teksaso baudžiamajame kodekse kompiuterinių nusikaltimų skyriuje, apibrėžia tik vieną nusikalstamą veiką – kompiuterių saugumo pažeidimas. Kalifornijos Baudžiamasis kodeksas, apibrėžia aštuonias veikas susijusias su kompiuteriniais nusikaltimais, žalojimas, įsibrovimas, keitimas, sukčiavimas, apgavimas, neteisėtai kontroliuoti ir pasisavinti pinigus, arba duomenų naudojimas be leidimo, sutrikdant kompiuterines paslaugas. Japonijos įstatymai vis dar reikalauja, kad materialaus turto paėmimas negali būti taikomas, jei duomenys yra prieinami per telekomunikacijų įrenginių. Jungtinėse Amerikos Valstijose nusikaltimus elektroninėje erdvėje nagrinėja apie 40 įstatymų. Svarbiausi iš jų šie: kompiuterinio sukčiavimo ir piktnaudžiavimo įstatymas, nacionalinės informacijos infrastruktūros įstatymas, ryšių padorumo įstatymas, autorinių teisių įstatymas, telekomunikacijų įstatymas, vaikų pornografijos prevencijos įstatymas ir kt. Visuose šiuose įstatymuose labai smulkiai išdėstytos veikos, paaiškinta dauguma terminų, galinčių sukelti teisminius ginčus. Tačiau dauguma jų yra skirtingi negu kitose valstybėse. Anglijoje 1990 metais buvo priimtas "Kompiuterio piktnaudžiavimo įstatymas" kuriuo buvo reglamentuoti elektroniniai nusikaltimai, buvo išspręsti ekstradicijos klausimai ir neaiškumai. Lenkijoje 1995 metais buvo priimtas baudžiamasis kodeksas, kurio atskiras skirsnis taip pat skirtas elektroniniams nusikaltimams. Rusijoje, kuri pastaraisiais metas paliko nemenką pėdsaką elektroninių nusikaltimų žemėlapyje, taip pat yra atskirų įstatymų reglamentuojančių kompiuterinius nusikaltimus, o taip pat šios šalies baudžiamasis kodeksas turi ir atskirą skirsnį kriminalizuojantį šios kategorijos nusikaltimus.

1981 metais Interpolas su tikslu nustatyti trūkumus esančius teisiniame reglamentavime ir jį suvienodinti apžvelgė valstybių narių baudžiamosios teisės normas. 2005 metais Interpolas su Afrikos regionine darbo grupe susitarė dėl šių tikslų:[54]

1. Kūrimas ir žinių kaip kovos su elektroniniais nusikaltimais regione ir tarp regionų.
2. Plėtoti ir stiprinti partnerystę su organizacijomis kurios dirba su elektroniniais nusikaltimais.
3. Sukurti, koordinuoti ir skatinti naudoti geriausią praktiką vykdant tyrimą ir prevenciją su elektroniniais nusikaltimai .
4. Padidinti informacijos srautą apie elektroninius nusikaltimus.
5. naudoti standartizuotas tyrimo procedūras.

[54]Afrikos regionine darbo grupė. http://itlaw.wikia.com/wiki/African_Regional_Working_Party_on_Information_Technology_Crime [žiūrėta2015-04-05]

Europos Sąjungos sprendimu 2002 metais valstybėms narėms buvo suteikta atsakomybė kriminalizuojant neteisėtą prieigą ir neteisėtą kišimąsi į informacines sistemas. Amerikos valstybių organizacija paskatino valstybes kriminalizuoti kibernetinius nusikaltimus ir harmonizuoti valstybių narių teisės normas, taip pat apsvarstyti galimybę prisijungti prie konvencijos dėl elektroninių nusikaltimų. Didžiojo aštuoneto šalys, Paryžiaus konferencijoje aptarė bendradarbiavimo galimybę, kuriant tarptautinį baudžiamąjį kodeksą skirtą kovoti su kompiuteriniais nusikaltimais.

Interpolo Europos informacinių nusikaltimų darbo grupė parengė kompiuterinių nusikaltimų vadovą, kuriame pateiktos techninės gairės, kurių turėtų būti laikomasi įgyvendinant teisės normas; siekiama užtikrinti, kad priimtos teisės normos būtų efektyvios ir veikiančios, skatinamas bendradarbiavimas. 2001 m. Amerikos teisingumo ir vidaus reikalų ministro įkurta elektroninių nusikaltimų ekspertų grupė dirbo siekdami atrasti bendradarbiavimo Amerikoje sistemą, kovojant su elektroniniais nusikaltimais. Didžiojo aštuoneto grupė taip pat peržiūrėjo egzistuojančius bendradarbiavimo mechanizmus, atrado spragas ir dėjo pastangas joms užpildyti. Valstybės narės buvo skatinamos padidinti kriminalizavimą, persekiojimą, tyrimą ir tarptautinį bendradarbiavimą. Iš pateiktos informacijos matyti, kad teisinio reglamentavimo harmonizavimo srityje yra siekiama kurti tarptautinius teisės aktus, tarptautines sutartis, kurių pagalba būtų užtikrinamas teisės normų skirtų kovoti su elektroniniais nusikaltimais vienodumas tarptautiniu mastu. Kovojant su elektroniniais nusikaltimais tarptautinės organizacijos taip pat imasi priemonių skirtų tiesiogiai užkirsti kelią šiems nusikaltimams. Prie šių priemonių priskiriamos dvi kategorijos: tai elektroninių nusikaltimų prevencijos ir elektroninių nusikaltimų tyrimo priemonės. Tiesioginės tarptautinės kovos su elektroniniais nusikaltimais apima du svarbius aspektus: elektroniniai nusikaltimai ir jų prevencijos ir kovos su elektroniniu nusikalstamumu tyrimas. Įvairios organizacijos ėmėsi atskirų priemonių kovoti su tam tikromis nusikalstamomis veikomis. Pavyzdžiui, Interpolas tiesiogiai bendradarbiauja su bankais, kovojant su sukčiavimu mokėjimo metu. EBPO gairės vartotojų apsaugos elektroninės komercijos kontekste 1999 apibrėžė vartotojų apsaugą elektroninėje komercijoje ir tradicinėje prekyboje. Rekomendacijos dėl informacinių sistemų ir tinklų saugumui 2002 paragino valstybes skirti daugiau dėmesio saugumui informacinėms sistemoms ir tinklų priemonėmis.

Lietuvos Respublikoje yra priimtas elektroninių ryšių įstatymas 2004 metais, kurio nuostatos yra labiau pritaikytos telefonijai, tačiau jis dabar taikomas ir internetui. „Šio įstatymo paskirtis, tikslai ir taikymas reglamentuoja visuomeninius santykius, susijusius su elektroninių ryšių paslaugomis, tinklais ir su jais susijusiomis priemonėmis bei paslaugomis, elektroninių ryšių išteklių naudojimu,

taip pat visuomeninius santykius, susijusius su radijo įrenginiais, galiniais įrenginiais ir elektromagnetiniu suderinamumu.“[55]

Pateikiu bendradarbiavimo pavyzdžių, Tore TVEDT byla, dėl rasistinių ir antisemitinių propagandų elektroninėje erdvėje. Savo interneto svetainėje, skelbė neonacizmą, rasinę neapykantą ir religiją, teigdamas, garbinti Odin ir kitų senovės skandinavų dievus. Tikslas buvo atkreipti vaikus ir jaunimą į antisemitinius ir rasistinius įsitikinimus. TVEDT Norvegijoje pripažino atsakinga už savo pagrindiniame puslapyje turinį, nors ji buvo paskelbtas serveryje, kuris buvo įsikūrusi Jungtinėse Amerikos Valstijose ir iš Norvegijos jurisdikcijos.[56]

JAV 2010 rugpjūčio mėn. buvo atliktas tarptautinis tyrimas operacija Delego , veikianti prižiūrint Krašto saugumo departamento , uždarė tarptautinį pedofilų svetaine Dreamboard. Svetainė buvo maždaug 600 narių, ir galėjo platinamas iki 123 terabaitų vaikų pornografija. Iki šiol tai yra viena didžiausių JAV prokuratūra tarptautinio vaikų pornografija, buvo pateikti 52 areštai buvo visame pasaulyje.[57] Operacijoje „Delego“ vyko didelis tarptautinis bendradarbiavimas, siekiant nustatyti ir sulaikyti pedofilus prisijungusius svetainėje Dreamboard. Tyrime dalyvavo ir koordinavimo ICE, Teisingumo departamentas; Eurojustas, Europos Sąjungos teisinio bendradarbiavimo institucija; ir dešimtys visame pasaulyje teisėsaugos agentūrų, 19 Dreamboard nariai buvo prisijungę penkiuose žemynuose ir 13 šalyse. Šios šalys yra Kanada, Danija, Ekvadoras, Prancūzija, Vokietija, Vengrija, Kenija, Nyderlanduose, Filipinai, Kataras, Serbija, Švedija ir Šveicarija. Dauguma tyrimų susijusią su operacija „Delego“ dar tebevyksta. Ši operacija yra geras pavystys, kad bendradarbiavimas gali atnešti realių rezultatų.

Tarptautinio bendradarbiavimo pavyzdžiai Lietuvoje:

Lietuvos kriminalinės policijos biuras, užkardant bei tiriant nusikaltimus, plėtoja tiek tarpžemyninį tiek tarptautinį bendradarbiavimą su Europos Sąjungos ir su kitų valstybių teisėsaugos institucijomis. Perimama užsienio šalių praktika, taip pat perduodama sava praktika, žinios apie naujus darbo metodus, priemones, atliekami bendri tyrimai, operacijos. Dalyvaujama tarptautinių organizacijų veikloje, tai Interpolas, Europolas, Šengeno erdvė, dalyvavimas Baltijos jūros regiono valstybių kovos su organizuotu nusikalstamumu projekte, prisiimami tarptautiniai įsipareigojimai.[58] Lietuvos kriminalinės policijos biuro bendradarbiavimas su Europos Sąjunga ir kitomis šalimis

[55] Lietuvos Respublikoje elektroninių ryšių įstatymas. Valstybės žinios, 2004-04-30, Nr. 69-2382 1 str.
[56] Norwegian jailed for Web racism http://edition.cnn.com/2002/WORLD/europe/04/23/norway.web/ [žiūrėta2015-03-03]
[57] Vaikų seksualinis išnaudojimas. http://www.dhs.gov/news/2011/08/03/secretary-napolitano-and-attorney-general-holder-announce-largest-us-prosecution [žiūrėta2015-04-05]
[58] Lietuvos kriminalinės policijos biuras. http://lkpb.policija.lt/index.php?option=com_content&view=category&layout=blog&id=56&Itemid=50 [žiūrėta-2015-04-10]

padeda greičiau atskleisti, užkirsti kelią ir ištirti nusikaltimus elektroninėje erdvėje, naudotis naujausia praktika ir efektyviais tyrimo metodais.

Pavyzdžiai iš sėkmingo bendradarbiavimo: 2014m. spalį tarptautinės operacijos metu, užkirstas kelias sukčiavimui internete. Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo valdybos pareigūnai, kartu su Vokietijos Žemutinės Saksonijos Osnabriuko prokuratūros Kovos su nusikaltimais elektroninėje erdvėje centrinės žinybos pareigūnais dalyvavo tarptautinėje operacijoje. Jos metu atliktos pas tarptautinės organizuotos grupės narius, susijusius su kompiuterinių virusų skirtų sukčiauti ir prievartauti turtą, kūrimu ir platinimu. Kratos atliktos ir sulaikymai Lietuvoje, Vokietijoje, Belgijoje ir Ukrainoje. [59]

2014 m. gruodį tarptautinėmis policijos pajėgomis sutriuškinta narkotikų kontrabandą vykdė organizuota nusikalstama grupuotė. Pastaroji sukūrė narkotinių ir psichotropinių medžiagų platinimo tinklą ir organizavo jų kontrabandą dideliais kiekiais iš Nyderlandų Karalystės į Suomijos Respubliką. Grupuotės veikloje dalyvavo ir Lietuvos Respublikos piliečiai. Tyrimas buvo vykdomas bendradarbiaujant Amsterdamo policijai ir Suomijos Nacionaliniam tyrimų biurui. Taip pat operacijoje dalyvavo Lietuvos, Lenkijos, Belgijos ir Prancūzijos policijos pareigūnai. Europole ir Eurojuste bendrų policijos veiksmų planavimui bei koordinavimui buvo įkurtas operacijos koordinacinis centras. Bendros operacijos metu buvo aptikti labai dideli kiekiai narkotinių ir psichotropinių medžiagų. Byloje daugiau nei trisdešimt įtariamųjų iš daugiau nei dešimties šalių: Suomijos, Prancūzijos, Belgijos, Nyderlandų, Estijos, Lietuvos, Somalio, Egipto, Irako ir Irano.[60]

2014 m. lapkritį Lietuvos kriminalinės policijos biuro ir Lietuvos Respublikos generalinės prokuratūros pareigūnai, kartu su teisėsaugos ir prokuratūros institucijomis iš viso pasaulio dalyvavo jungtinėje tarptautinėje operacijoje, kurios tikslas – anoniminiame TOR tinkle veikiančių tinklalapių, pardavinėjančių uždraustas prekes ir paslaugas, uždarymas. 16 Europos Sąjungos valstybių narių (Airija, Bulgarija, Čekijos Respublika, Suomija, Prancūzija, Vokietija, Vengrija, Latvija, Lietuva, Liuksemburgas, Nyderlandų Karalystė, Rumunija, Ispanija, Švedija, Šveicarija, Jungtinė Karalystė) kartu su kolegomis iš Jungtinių Amerikos Valstijų, sudavė stiprų smūgį TOR tinkle veikusiems internetinės prekybos tinklalapiams. Tarptautinei operacijai, iš operacijų koordinavimo centro Hagoje vadovavo Europolas. Jungtiniais teisėsaugos institucijų veiksmais siekta sustabdyti uždraustų prekių ir daiktų, tokių kaip ginklai ir narkotikai, pardavimą, platinimą ir reklamą, vykdomą anoniminiose tinklalapiuose. Operacijos metu sulaikyta 17 asmenų – prekiautojų bei administratorių – organizavusių prekybos tinklalapių veiklą, uždaryta 410 TOR

[59] Ten pat.
[60] Ten pat.

tinklalapių. Konfiskuota apie 1 mln. JAV dolerių vertės "Bitcoin" valiutos ir 180 000 eurų grynųjų pinigų, narkotikų, aukso ir sidabro.[61]

2014 m. rugsėjį didžiulio masto teisėsaugos operacijoje „Archimedes" suduotas smūgis organizuoto nusikalstamumo tinklams visoje Europoje. 34 valstybių teisėsaugos institucijos ir tarptautinės organizacijos, koordinuojamos ir padedamos Europolo, sujungė savo pajėgas didžiausioje kada nors surengtoje slaptoje tarptautinėje operacijoje „Archimedes", nusitaikydami į organizuotų nusikalstamų grupuočių veiklą bei jų infrastruktūras visoje Europos Sąjungos teritorijoje. „Operacija „Archimedes" yra sėkmingo teisėsaugos bendruomenės darbo rezultatas. Analogų neturintys operacijos mastai, baigęsi daugiau nei 1000 asmenų suėmimu visoje Europoje, kad tarptautinė teisėsaugos bendruomenė yra pasiryžusi kovoti su neteisėta jų veikla.[62]

2014 m. gegužę Lietuvos kriminalinės policijos biuras, bendradarbiaudamas su JAV Federalinių tyrimų biuru bei JAV ambasada Vilniuje, surengė kibernetinio saugumo mokymus, kuriuos vedė JAV Federalinių tyrimų biuro instruktoriai. Kibernetinio saugumo užtikrinimo problema yra aktuali ir kitoms organizacijoms, todėl į Lietuvos kriminalinės policijos biure vykusius mokymus buvo pakviesti atstovai iš Lietuvos Respublikos krašto apsaugos ministerijos, Specialiųjų tyrimų tarnybos bei Ryšių reguliavimo tarnybos Tinklų ir Informacijos saugumo departamento Saugumo incidentų tyrimų skyriaus (CERT-LT). Vykdant Lietuvos kriminalinės policijos reformą, nuo 2014 m. rugsėjo 1 d. šalies apskričių policijos komisariatuose bus įsteigti nusikaltimus elektroninėje erdvėje tiriantys padaliniai. Todėl į mokymus buvo pakviesti tyrėjai ir specialistai iš 5 didžiausių šalies miestų apskričių vyriausiųjų policijos komisariatų. Mokymų metu dalyviai buvo supažindinti su JAV Federalinių tyrimų biuro naudojamais kibernetinio saugumo incidentų, kenkimo programinės įrangos tyrimo metodais bei tam naudojama įranga, dalyviai vykdė praktines užduotis.[63] Mokymų metu gautos žinios bei programinė įranga padės efektyviau užtikrinti kibernetinio saugumo užtikrinimo bei nusikaltimų elektroninėje erdvėje tyrimo funkcijas. Visi šitie pavyzdžiai tik patvirtina, kad glaudus valstybių bendradarbiavimas, palengvina nusikalstamų veikų išaiškinimą ir tyrimą.

Apibendrinant nusikaltimų elektroninėje erdvėje tarptautinį reglamentavimą ir bendradarbiavimą, galima teigti, kad tai yra valstybėms svarbu ir naudinga. Tik glaudžiai valstybėms bendradarbiaujant, ieškant kovos priemonių su nusikaltimais elektroninėje erdvėje,

[61] Ten pat.
[62] Lietuvos kriminalinės policijos biuras. http://lkpb.policija.lt/index.php?option=com_content&view=category&layout=blog&id=56&Itemid=50 [žiūrėta-2015-04-10]

[63] Lietuvos kriminalinės policijos biuras. http://lkpb.policija.lt/index.php?option=com_content&view=category&layout=blog&id=56&Itemid=50 [žiūrėta-2015-04-10]

galima pasiekti gerų rezultatų. Europos Sąjungos valstybės narių ir kitų šalių teisėsaugos institucijoms yra pakankamai sukurta teisinių priemonių, suteikiančių galimybę bendradarbiauti tiriant nusikaltimus elektroninėje erdvėje.

2.2. Tarptautinių organizacijų ir ES dokumentai dėl elektroninių nusikaltimų tyrimo

Nusikaltimus elektroninėje erdvėje tarptautiniu mastu organizacijos koordinuoja ir derina valstybių veiksmus, siekiant kovoti su elektroniniais nusikaltimais, užkirsti kelią jiems plisti. Pagrindinės organizacijos, tai Jungtinės Tautos, Europos Taryba, Europos Sąjunga, Europos ekonominio bendradarbiavimo ir plėtros organizacija, Interpolas, didžiojo aštuoneto šalys. Kartais nacionaliniai teisės aktai ir juose įtvirtintos teisinės priemonės būna neveiksmingos ir reikia pasikliauti tarptautinių organizacijų siūlomomis priemonėmis. Nes tarptautinės organizacijos nuolat stebi nusikalstamų veikų pokyčius, steigia darbo grupes, kuria strategijas, skirtas kovoti su šio pobūdžio nusikaltimais ir leidžia organizacinius aktus su įtvirtintomis nuostatomis dėl kovos su elektroniniais nusikaltimais tarptautiniu mastu.

Jungtinės Tautos. Vienas svarbiausių dokumentų tai, Tarptautinė nusikaltimų politikos apžvalga – rekomendacija dėl su kompiuteriais susijusių nusikaltimų užkardymo ir kontrolės.[64] Atskiri įstatymai, tiek ir tarptautinis bendradarbiavimas vystėsi daug lėčiau nei naujosios technologijos. Visuomenės priklausomybė nuo kompiuterinių sistemų, turi didelį aspektą. Greita tarptautinė plėtra, didelės apimties kompiuteriniai tinklai ir galimybė prieiti prie sistemų, telefono linijų padidina šių sistemų pažeidžiamumą ir būtinybę piktnaudžiavimo ar nusikalstamos veiklos galimybę. Kompiuterinio nusikaltimo pasekmės gali turėti rimtų ekonominių sąnaudų, taip pat rimtų išlaidų saugumui. Rekomendacijoje apibūdintos visos neteisėtos veikos, susijusios su kompiuterių panaudojimu, pateikta kompiuterinio nusikaltimo samprata, tarptautinio bendradarbiavimo sąlygos, baudžiamoji atsakomybė nenagrinėjama.

1948 metais įsteigė Jungtinių Tautų Organizaciją kovoti su tarptautiniu nusikalstamumu. Vadovaujantis EBPO pateikta ataskaita, JTO sušaukė aštuntą Jungtinių Tautų kongresą dėl nusikaltimų prevencijos ir elgesio su nusikaltimais, siekiant spręsti tarptautinius teisinius iššūkius kylančius iš elektroninių nusikaltimų. Kongresas sukūrė rezoliuciją, raginančią visas JTO valstybes nares dėti daugiau pastangų kovojant su elektroniniais nusikaltimais ir modernizuoti savo nacionalinius baudžiamuosius įstatymus, prireikus pagerinti kompiuterių saugumo ir prevencijos priemones, skatinti baudžiamąjį persekiojimą, konfiskavimą ir restituciją

[64] International review of criminal policy „United Nations Manual on the prevention and control of computer-related crime.

neteisėtai įgytam turtui, iš kompiuterinių nusikaltimų veiklos.[65] 1995 metais, JTO paskelbė vadovą „Prevencija ir kontrolė su kompiuteriais susijusiems nusikaltimams".[66] Reglamentuoja kompiuterinius nusikaltimus, teisės aktus saugančius duomenų ir informacijos savininkus, privatumą, procesinę teisę ir tarptautinį bendradarbiavimą. 2000 metais Vienoje, Jungtinės Tautos savo dešimtąjį kongresą skyrė prevencijai ir elgesiui su nusikaltėliais, susijusiais su kompiuteriniai tinklais. Kongreso metu vyko techninis seminaras skirtas kompiuterinių nusikaltimų prevencijai. Tačiau šio kongreso metu pasiūlytos kovos ir prevencijos priemonės, kaip ir kitos JTO kuriamos priemonės į priekį judėjo labai lėtai. Dažnai tarptautinių sutarčių, tokių kaip konvencija kūrimas ir ratifikavimas užtrunka dešimtmečius, todėl jų kaip priemonių efektyvumas yra menkas. S. Ghosh nuomone, Jungtinių Tautų kova su elektroniniais nusikaltimais tarptautiniu mastu yra itin svarbi siekiant sveikos civilizacijos.[67]

Jungtinių Tautų konvencija prieš tarptautinį organizuotą nusikalstamumą (TOC) buvo patvirtinta 2000 metų lapkričio 15 dieną, Generalinės Asamblėjos rezoliucija 55/25.[68] Tai tarptautinė sutartis, kurios tikslas kovoti su organizuotu nusikalstamumu elektroninėje erdvėje tarptautiniu mastu.

Europos Taryba. 1989 metais Europos Tarybos pateikė rekomendaciją R 89(9) apie nusikaltimus, susijusius su kompiuterine sistema.[69] Europos Tarybos narėms pateikti pasiūlymai peržiūrėti ar kuriant įstatymus, yra vadovaujamasi Europos komiteto pranešimu, dėl nusikaltimų susijusių su kompiuteriais nusikaltimus. Šiame dokumente nustatyti bendri principai Europos Tarybų narių įstatymų leidžiamajai valdžiai. Nustatyta piktnaudžiavimo atvejai susiję su kompiuterių naudojimu. Rekomendacijoje aprašoma samprata, aštuoni nusikalstamų veikų punktai ir pasirinktinis keturių punktų kriminalizavimo veikų sąrašas.

Rekomendacijoj pasiūlytas minimalus su kompiuteriais susijusių nusikaltimų sąrašas:

1. Sukčiavimas susijęs su kompiuteriais.
2. Klastojimas naudojant kompiuterį.
3. Kompiuterinių duomenų ar programų sunaikinimas arba sugadinimas.
4. Sabotažas naudojant kompiuterį.
5. Neteisėta prieiga prie kompiuterių sistemos.
6. Neteisėtas informacijos perėmimas kompiuterinėje sistemoje.

---

[65] Eight united nations congress on the prevention of crime ant the treatment of offenders. http://www.asc41.com/UN_congress/8th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/026%20ACONF.144.28.Rev.1%20Eighth%20United%20Nations%20Congress%20on%20the%20Prevention%20of%20Crime%20and%20the%20Treatment%20of%20Offenders.pdf [žiūrėta 2015-03-25]

[66] International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime. http://www.uncjin.org/Documents/EighthCongress.html [žiūrėta 2015-03-25]

[67] Ghosh S, Turrini E. Cybercrimes: A Multidisciplinary Analysis.// Springer, 2010, p. 328.

[68] Jungtinių Tautų konvencija prieš tarptautinį organizuotą nusikalstamumą. Valstybės žinios. 2002-05-22, Nr. 51-1933.

[69] Recommendations no. R (89)9 on Computer-related crime // http://cm.coe.int/ta/rec/1989/89r9.htm

7. Neteisėtas apsaugotų kompiuterio programų dauginimas ir platinimas.

8. Neteisėtas kompiuterių lustų topografijų dauginimas ir platinimas.

Europos Taryba parengė 2001 metais „Nusikaltimų elektroninėje erdvėje konvenciją“ baimindamasis, kad elektroniniai nusikaltimai gali peraugti į baudžiamuosius nusikaltimus ir suprasdama, kad turi būti tarptautinis bendradarbiavimas siekiant užkirsti kelią naujoms nusikalstamoms veikoms daryti, bei joms plisti. Pagrindinis konvencijos tikslas yra suvienodinti baudžiamąją politiką, siekiant apsaugoti visuomenę nuo elektroninių nusikaltimų, priimant tinkamus teisės aktus ir skatinant tarptautinį bendradarbiavimą. Konvencija buvo siekiama suderinti baudžiamosios materialinės teisės susijusios su elektroniniais nusikaltimais elementus. Konvencijoje numatyti vidaus baudžiamajam persekiojimui reikalingi įgaliojimai, tiriant ir persekiojant asmenis padariusius elektroninę nusikalstamą veiką. Tuo yra siekiama sukurti greitą ir veiksmingą tarptautinio bendradarbiavimo tvarką. Konvencijoje numatytų kovos priemonių, nes tik esant jam valstybės galėtų tinkamai reaguoti į teisėsaugos problemas, kylančias kovojant su elektroniniais nusikaltimais. Be to šis tinklas tūrėtų papildyti tarpvalstybinį bendradarbiavimą, nes kiekvienas toks centras atliktų ne tik technines funkcijas, tai yra duomenų išsaugojimą, rinkimą, bet ir teisines konsultacijas.

Siekiant paskirti atsakomybę už veikas, susijusias su rasinės ir tautinės neapykantos kurstymu pasitelkiant kompiuterines sistemas, 2002 m. lapkričio 7 d. buvo priimtas Europos Tarybos nusikaltimų elektroninėje erdvėje konvencijos papildomas protokolas (2002)24[70] Už bet kokią rašytinę medžiagą, vizualinis, minčių ar teorijų, skatinančias diskriminaciją ar smurtą prieš individą ar jų grupes, išsiskiriančias dėl savo rasės, tikėjimo, politinių pažiūrų. Europos Taryba apima beveik visas nusikalstamas veikas padarytas elektroninėje erdvėje, kurios įvardintos Nusikaltimų elektroninėje erdvėje konvencijoje.

2005 konferencijoje dėl elektroninių nusikaltimų, Europos Vadovų Taryba pareiškė susirūpinimą dėl sparčiai didėjančių grėsmių ir rimtų socialinių ir ekonominių rezultatų elektroninių nusikaltimų, įskaitant teroristinės veiklos internete, pažymėdami, kad dauguma elektroniniai nusikaltimai yra tarptautinio pobūdžio nusikaltimai. Pripažino, kad bendradarbiavimas kovojant su elektroniniais nusikaltimais, duos geresnių rezultatų.

Europos Sąjunga. 1995, Europos Parlamentas ir Taryba patvirtino Direktyvą 95/46 / EB, 24 spalis 1995 dėl asmenų apsaugos ryšium su asmens duomenų tvarkymu ir dėl laisvo tokių duomenų judėjimo.1997, Europos Parlamentas ir Taryba patvirtino Direktyvą 1997/66 / EB 15 gruodžio 97 asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje.

[70] 2002 m. lapkričio 7 d. Europos Tarybos nusikaltimų elektroninėje erdvėje konvencijos papildomas protokolas (2002)24http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm [žiūrėta2015-03-25]

1989 metais Europos Taryba priėmė Rekomendaciją Nr. R(89)9, kuria Europos Tarybos valstybės narės kviečiamos atsižvelgti į ekspertų komiteto paruoštą ataskaitą kuriant įstatymus, susijusius su kompiuteriniais nusikaltimais. 1995 metų rugsėjį buvo priimta Rekomendacija Nr. R(95)13, kuria siekiama įtvirtinti naujus baudžiamojo proceso veiksmus, kurie būtų taikomi tiriant būtent elektroninius nusikaltimu.[71] Nurodyti procesiniai principai: krata ir poėmis, telekomunikacijų kontrolė, pareiga bendradarbiauti, elektroninė duomenų forma, šifravimo kūrimas ir panaudojimas, profesiniai mokymai ir tarpvalstybinis bendradarbiavimas. Priimtas Europos Parlamento ir Tarybos 1999 m. sausio 25 d. sprendimas Nr.276/1999/EB, kuriuo patvirtintas ilgalaikis Bendrijos veiksmų planas, siekiama skatinti palankią aplinką interneto pramonės plėtrai, skatinti saugų naudojimąsi internetu ir kovos su neteisėtu žalingu turiniu. Programa yra pagrysta trimis veiklos kryptimis:

1. Sukuriant saugesnę aplinką, sukuriant Europos specialių telefono linijų tinklą, skatinant savireguliaciją.
2. Plėtoti filtravimo priemones.
3. Didinti informatyvumą.

2001 metų sausio 26 dienos komunikatas – Saugesnės informacinės visuomenės kūrimas, gerinant informacinių infrastruktūrų saugą ir kovą su nusikaltimais, susijusiais su kompiuteriais. KOM (2000)890.[72] Nurodytos priemonėmis, kuriomis turima kovoti su elektroniniais nusikaltimais. Tai nacionalinės baudžiamosios teisės harmonizavimas, procesinės teisės suvienodinimas.

2002 metais ES lygiu dėl elektroninių ryšių sektoriaus buvo priimta direktyvų, kuriose teigiama, kad lengvai prieinamos interneto paslaugos atveria naujas galimybes, bet sukelia naują grėsmę privatumui ir saugumui. Europos Sąjungos praktika reglamentavime su elektroniniais nusikaltimais yra nepakankamas, kadangi direktyvose neteisėtos veikos elektroninių ryšių sektoriuje nenagrinėjamos, nesprendžiami ir baudžiamosios atsakomybės klausimai.

2013 metų rugpjūčio 12 dieną priima Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas. [73] Direktyva pakeičia 2005 metų Europos Taryba priimtą pamatinį sprendimą, dėl atakų prieš informacines sistemas Nr. 2005/222/JHA. Direktyvos tikslas, suderinti valstybių narių baudžiamosios teisės normas dėl atakų informacinių sistemų srityje, nustatant taisykles, susijusias su nusikalstamų veikų apibrėžtimi, ir atitinkamas sankcijas. Taip pat pagerinti valstybių narių atsakingų institucijų, policijos ir kitų teisėsaugos institucijų, Eurojusto, Europolo ir Europos kovos su elektroniniais nusikaltimais centro bei Europos tinklų ir informacijos apsaugos agentūros bendradarbiavimą.

Europos ekonominio bendradarbiavimo ir plėtros organizacija. Tai pirmoji organizacija 1983 kai Europos ekonominio bendradarbiavimo ir plėtros organizacija kompiuterinių

[71] Council of Europe Recommendation No. R(95) 13
[72] Commission of the European Communities COM (2000) 890
[73] Europos Parlamento ir Tarybos direktyva 2013/40/ES

nusikaltimų komitetas išleido ataskaitą „Su kompiuteriais susiję nusikaltimai: teisinės politinės analizės“ ir rekomendavo šios organizacijos narėms, kriminalizuoti veikas susijusias su kompiuteriniais nusikaltimais.1992 metais paruošė kitą rekomendaciją „Dėl informacinių sistemų apsaugos gairių“ kurioje suformuoti reikalavimai internetiniai saugai užtikrinti. Pradėjo išsamų tyrimą dėl baudžiamosios teisės problemų, taikant elektroniniams nusikaltimams tarptautiniu mastu. Atlikus tyrimą, buvo pateiktas minimalus pavojingų veikų, susijusių su kompiuteriais ir telekomunikacijomis, sąrašas. Daugiausia dėmesio skiria elektroniniam saugumui ir skatina pasaulinę politiką, grindžiamą tarpusavio pasitikėjimu.

Interpolas. Nuo 1990, Tarptautinė kriminalinės policijos organizacija. Yra didžiausia pasaulyje tarptautinė organizacija, turinti prisijungusiųjų 190 pasaulio valstybių. Interpolas tarnauja valstybių teisėsaugos institucijoms. Jis atlieka žvalgybos funkcijas ir teikia paramą valstybių vykdomiems tyrimams dėl įvykdytų ar vykdomų tęstinio pobūdžio nusikalstamų veikų, nepriklausomai nuo valstybių sienų.[74] Taip pat 1990 metais Interpolas sukūrė pirmąją darbo grupę elektroninių nusikaltimų klausimais, pavadintą Europos darbo grupė su informacinių technologijų nusikaltimais. Kiekvienas Interpolo regionuose įsikūręs centrinis biuras yra atsakingas už jiems pateiktus pagalbos prašymus, suteikti reikiamą pagalbą dėl vienokios ar kitokios elektroninės nusikalstamos veikos. Atsižvelgiant į viso pasaulio dėmesį skiriamą šiai organizacijai, Interpolas buvo priverstas žengti koja kojon su visais elektroniniais nusikaltimais, nepriklausomai nuo jų sudėtingumo masto ar geografinės vietos. Dėl šių priežasčių Interpolas dabar turi saugią sistemą, pritaikytą rinkti, saugoti, analizuoti, keistis prašoma ir pateikiama informacija.

Apibendrinant Interpolo veiklą, galima teigti, kad bendradarbiavimas valstybių tik parodo norą kovoti su kintančiais elektroniniais nusikaltimais.

Didžiojo aštuoneto šalys. Nuo 1990-ųjų vidurio, Aštuoneto grupės (G8) sukūrė darbo grupes ir išdavė komunikatuose lyderių ir veiksmų planus. Didysis aštuonetas arba G-8, susideda iš didžiausių pasaulio pramonės šalių: Didžiosios Britanijos, Prancūzijos, Vokietijos, Italijos, Kanados, JAV, Japonijos ir Rusijos. 1996 metais metiniame viršūnių susitikime valstybių vadovai priėmė rekomendaciją skirtą kovoti su tarptautiniu nusikalstamumu. 1997 buvo sukurta didžiojo septyneto grupė, skirta kovoti su modernių technologijų nusikaltimais. 1998 metais, kai prisijungė Rusija, pavadino didžiojo aštuoneto grupe. [75] 1997, G8 išleido ministrų komunikatą, kuris apima veiksmų planą ir principus, siekdama kovoti su elektroniniais nusikaltimais ir apsaugoti duomenis ir sistemas nuo neteisėtos sutrikusi. G8 pat įgalioja, kad visos teisėsaugos darbuotojai turi būti apmokyti ir pasirengę spręsti su elektroniniais nusikaltimais, ir nurodo visas šalis nares turėti

[74] Interpol http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [žiūrėta2015-03-25]
[75] History of the G8 http://www.g8.co.uk/history-of-the-g8/ [žiūrėta2015-03-25]

sąlyčio tašką 24 valandas per parą / 7 dienas per savaitę.[76] Aštuoneto grupės susitarė dėl principų ir metodų privatumo apsaugos, laisvos informacijos srauto, ir dėl sandorių saugumo.

2.3. Nusikaltimų elektroninėje erdvėje tyrimo reglamentavimas Lietuvoje

Elektroninius nusikaltimus tiria, Lietuvos kriminalinės policijos biuro nusikaltimų elektroninėje erdvėje tyrimo valdyba kuri įkurta 2001 metais. Vykdo ikiteisminius tyrimus susijusius su elektroniniais nusikaltimais. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų įsteigtas Lietuvos Respublikos vidaus reikalų ministerijos 1994 m.

2009 metais Informatikos ir ryšių departamentas, panaikinus Vidaus reikalų ministerijos Informacinės politikos departamentą, perėmė dalį šio Vidaus reikalų ministerijos struktūrinio padalinio funkcijų. Vykdo virš 30 viešojo administravimo funkcijų, viešojo saugumo bei elektroninės informacijos valdymo srityse. Informatikos ir ryšių departamento veikla vykdoma trimis lygiais: vidaus reikalų sistemos, šalies ir tarptautiniu mastu. Siekdamas efektyvaus ir patikimo vidaus reikalų srities valstybės informacinių sistemų, registrų bei tinklų veikimo, Informatikos ir ryšių departamentas kuria ir diegia saugias informacines ir ryšių technologijas, nuosekliai inicijuoja ir įgyvendina projektus, susijusius su IRT plėtra bei sauga, bendradarbiauja su Europos Sąjungos, Šiaurės Atlanto sutarties organizacijos (NATO) valstybių atsakingomis institucijomis bei Jungtinių Tautų Narkotikų kontrolės ir nusikalstamumo prevencijos biuru (UNODC), nuolat dalyvauja informacinių technologijų ir kibernetinio saugumo srities tarptautiniuose renginiuose.[77] 2007 m. pabaigoje prisijungus prie Šengeno informacinės sistemos. Informatikos ir ryšių departamentas dalyvauja įgyvendinant Elektroninės informacijos saugos plėtros 2011–2019 m. programos nuostatas. Taip pat nusikaltimus elektroninėje erdvėje tiria antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, kuris vykdo žvalgybą ir kontržvalgybą. 2015 m. sausio 1d. Lietuvoje įsigaliojo kibernetinio saugumo įstatymas, apibrėžiantis kibernetinio saugumo sistemos organizavimą, saugumo užtikrinimo priemones valdymą ir kontrolę, kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas. Veiklą pradėjo Nacionalinis kibernetinio saugumo centras, kurio pagrindinis dėmesys sutelktas į valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros kibernetiniam saugumui. Taip pat kiekvienas vyriausiasis policijos komisariatas pradėjo dirbti su elektroniniais nusikaltimais.

[76]International cybercrime http://en.wikipedia.org/wiki/International_cybercrime [žiūrėta 2015-03-25]

[77] Informatikos ir ryšių departamentas prie LR VRM veikla. http://www.ird.lt/veikla-2/ [žiūrėta2015-04-02]

Lietuvoje Elektroniniam saugumui labai svarbu yra, tinkamas teisinis reglamentavimas. Lietuvoje nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui reglamentavimas prasidėjo 1991 metais. Baudžiamasis kodeksas buvo priimtas Lietuvos Respublikos Seimo 2000 m. rugsėjo 26 d. įstatymu (Nr. VIII-1968); tuo pačiu įstatymu patvirtinti ir Baudžiamojo proceso kodeksas bei Bausmių vykdymo kodeksas. Naujasis baudžiamasis sąvadas įsigaliojo suderintas kartu su su Europos Sąjungos teisės aktų nuostatomis, taip pat su naujaisiais Lietuvos BPK ir BVK 2003 m. gegužės 1 d. baudžiamoji atsakomybė už nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui numatyta LR BK XXX skyriuje:[78]

1. *Neteisėtas poveikis elektroniniams duomenims (196 str.)* Straipsnyje nurodyta baudžiamoji atsakomybė už elektroninių duomenų ar techninės įrangos neteisėtą sunaikinimą, sugadinimą ar pakeitimą, jei dėl to buvo padaryta didelė žala;

2. Neteisėtas poveikis informacinei sistemai (197 str.) Straipsnyje nurodyta baudžiamoji atsakomybė už elektroninių duomenų neteisėtą sutrikdymą ar nutraukimą darbo, jei dėl to padaryta didelė žala.

3. Neteisėtas elektroninių duomenų perėmimas ir panaudojimas (198 str.) Straipsnio 1-oje dalyje nurodyta baudžiamoji atsakomybė už neteisėtą stebėjimą, fiksavimą, perėmimą, įgijimą, laikymą, pasisavinimą, paskleidimą ar kitokį panaudojimą neviešus elektroninius duomenis. 2 –oje dalyje nurodyta baudžiamoji atsakomybė už neteisėtą stebėjimą, fiksavimą, perėmimą, įgijimą, laikymą, pasisavinimą, paskleidimą ar kitokį panaudojimą strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis.

4. Neteisėtas prisijungimas prie informacinės sistemos (198$^{(1)}$ str.) Straipsnio 1-oje dalyje nurodyta baudžiamoji atsakomybė už neteisėtą prisijungimą prie informacinės sistemos pažeidžiant informacinės sistemos apsaugos priemones. Straipsnio 2 – oje dalyje nurodyta baudžiamoji atsakomybė už neteisėtą prisijungimą prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos. Straipsnio 3 – oje dalyje nurodyta baudžiamoji atsakomybė ir juridiniams asmenims.

5. *Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis (198$^{(2)}$ str.)* Straipsnyje nurodyta baudžiamoji atsakomybė už elektroninių duomenų neteisėtą gaminimą, gabenimą, pardavinėjimą ar kitokį platinimą įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodus ar kitokius panašius duomenis, tiesiogiai skirtus daryti nusikalstamas veikas, arba tuo pačiu tikslu juos įgijo ar laikė. Taip pat atsako ir juridinis asmuo.

[78] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 [žiūrėta2015-04-02]

Šiuos pažeidimus būtų įmanoma nustatyti, kai elektroninėje erdvėje padaromos nusikalstamos veikos ir kai nusikalstamų veikų padarymui yra pasitelkiamos informacinės technologijos bei elektroninė erdvė.

1. *Asmens susižinojimo neliečiamumo pažeidimas (166 str.*) Straipsnyje numatyta baudžiamoji atsakomybė „už neteisėtai perimtą 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. Atsako ir juridinis asmuo“[79]
2. *Neteisėtas naudojimasis energija ir ryšių paslaugomis (179 str.)* Straipsnyje numatyta baudžiamoji atsakomybė „už neteisėtai prisijungęs prie energijos tiekimo arba ryšių tinklo ar saugyklos, iškraipydamas skaitiklių rodmenis arba kitais neteisėtais būdais naudojosi elektros ar šilumos energija, dujomis, vandeniu, telekomunikacijomis ar kitais ekonominę vertę turinčiais dalykais ir dėl to kitam asmeniui padarė turtinės žalos“[80]. Pavyzdžiui 1983 metais devyniolikmetis UCLA studentas panaudojo savo kompiuterį įsilaužti į gynybos departamento tarptautinių ryšių sistemą.

LR BK XXIX skyriuje „Nusikaltimai intelektinei ir pramoninei nuosavybei“ .

1. Literatūros, mokslo, meno kūrinio ar gretutinių teisių objekto neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas (192 str.) Straipsnyje numatyta baudžiamoji atsakomybė „už 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“[81] Nusikalstama veika turi būti atlieka internetinėje erdvėje, pavyzdžiui platinant internete.

LR BK 191, 193, 194 ir 195 straipsniuose taip pat nustatyta baudžiamoji atsakomybė ir už kitus intelektinės ir pramonės nuosavybės teisių pažeidimus, kurie atliekami naudojantis elektroniniais ryšiais, pavyzdžiui platinimas internete.

Melagingas pranešimas apie visuomenei gresiantį pavojų ar ištikusią nelaimę (285 str.) Straipsnyje nurodyta baudžiamoji atsakomybė už tai, kad melagingai pranešė ar paskleidė žinią apie visuomenei gresiantį pavojų ar ištikusią nelaimę, dėl to kilo visuomenės sumaištis ir jei buvo padaryta didelės turtinės žalos, arba dėl to buvo iškviestos specialios tarnybos. Melagingu

[79] [79] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 166 str.
[80] [80] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 179 str.
[81] [81] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 192 str.

pranešimu laikytina. Melaginga pranešimas perduodamas elektroniniais ryšiais, parašant elektroninį laišką, perduodant telefonu informaciją. Melagingu pranešimu laikytina, pavyzdžiui pranešimas, kad padėtas sprogmuo tam tikrame objekte ir viskas susprogs.

Viešai neskelbtinos informacijos platinimas:

1. Vieši raginimai smurtu pažeisti Lietuvos Respublikos suverenitetą (122 str.); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad , „viešai ragino smurtu pažeisti Lietuvos Respublikos suverenitetą – pakeisti jos konstitucinę santvarką, nuversti teisėtą valdžią, kėsintis į jos nepriklausomybę arba pažeisti teritorijos vientisumą, šiems tikslams kurti ginkluotas grupes arba daryti kitus šiame skyriuje numatytus nusikaltimus, kuriais kėsinamasi į Lietuvos valstybę“[82]

2. Valstybės paslapties atskleidimas (125 str.); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad atskleidė informaciją, kuri yra Lietuvos Respublikos valstybės paslaptis, jeigu jam ta informacija buvo patikėta arba jis ją sužinojo dėl savo tarnybos, darbo ar atlikdamas viešąsias funkcijas, bet nebuvo šnipinėjimo požymių.

3. Neteisėtas disponavimas informacija, kuri yra valstybės paslaptis (124 str.) Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad neteisėtai įgijo ar perleido informaciją, kuri yra Lietuvos Respublikos valstybės paslaptis, arba neteisėtai laikė materialius objektus, kurių turinys ar informacija apie juos yra Lietuvos Respublikos valstybės paslaptis, jeigu nebuvo šnipinėjimo požymių.

4. Valstybės paslapties praradimas (126 str.); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad sunaikino, sugadino ar prarado dėl tarnybos, darbo ar viešųjų funkcijų atlikimo jam patikėtą dokumentą, daiktą ar kitą materialų objektą, kurio turinys ar informacija apie jį yra Lietuvos Respublikos valstybės paslaptis.

5. Neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ir panaudojimas (168 str.); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad be asmens sutikimo viešai skelbė informaciją apie kito žmogaus privatų gyvenimą. Ir tą informaciją sužinojo dėl savo tarnybinės veiklos, profesijos, ar atlikdamas užduotį. Arba surinko informaciją darydamas šio kodekso 165–167 straipsniuose numatytą veiką. Atsako ir juridinis asmuo.

6. Kurstymas prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę (170 str.) Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad 1 – oje dalyje kas turėdamas tikslą platinti gamino, įsigijo, siuntė, gabeno, laikė dalykus, kuriuose tyčiojamasi, niekinama, skatinama neapykanta ar kurstoma diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų arba kurstoma smurtauti, fiziškai susidoroti su tokia žmonių grupe ar jai

[82] [82] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 122 str.

priklausančiu asmeniu, arba juos platino. 2 – ojoje dalyje kas viešai tyčiojosi, niekino, skatino neapykantą, kurstė diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų. 3-ojoje dalyje kas viešai kurstė smurtauti, fiziškai susidoroti su žmonių grupe ar asmeniu dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų arba finansavo ar kitaip materialiai rėmė tokią veiklą. Atsako ir juridinis asmuo. Nusikaltimais laikytini padaryti elektroninių ryšių sektoriuje, kai padaromi naudojantis elektroninėmis priemonėmis. Pavyzdžiui kompiuteriu sukuriant pranešimus, kuriais viešai raginama internete, skatinti smurtu pažeisti Lietuvos respublikos suverenitetą.

Vieni iš dažniausiai pasitaikančių nusikaltimų naudojant informacines technologijas yra:

1. Šmeižimas (LR BK 154 str. 2d.); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad šmeižė asmenį, neva šis padarė sunkų ar labai sunkų nusikaltimą, arba per visuomenės informavimo priemonę ar spaudinyje.

2. Įžeidimas (LR BK 155 str. 1d.) turinio komentarų ar informacijos talpinimas; Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad viešai veiksmu, žodžiu ar raštu užgauliai pažemino žmogų. Šis straipsnis taikomas prie elektroninių nusikaltimų, kadangi elektroninė erdvė yra laikoma vieša vieta.

3. Neapykantos skatinimas ar kurstymas diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl. lyties, seksualinės orientacijos, rasės, tautybės (LR BK 170 str.) paviešinant informaciją internete; Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad 1- ojoje dalyje turėdamas tikslą platinti gamino, įsigijo, siuntė, gabeno, laikė dalykus, kuriuose tyčiojamasi, niekinama, skatinama neapykanta ar kurstoma diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų arba kurstoma smurtauti, fiziškai susidoroti su tokia žmonių grupe ar jai priklausančiu asmeniu, arba juos platino. 2 – ojoje dalyje viešai tyčiojosi, niekino, skatino neapykantą ar kurstė diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų. 3 – ojoje dalyje viešai kurstė smurtauti, fiziškai susidoroti su žmonių grupe ar jai priklausančiu asmeniu dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų arba finansavo ar kitaip materialiai rėmė tokią veiklą. Taip pat atsako ir juridinis asmuo.

4. Vaiko išnaudojimas pornografijai (LR BK 162 str.); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad verbavo, vertė arba įtraukė vaiką dalyvauti pornografinio pobūdžio renginiuose, arba išnaudojo vaiką tokiems tikslams, arba išnaudojo vaiką pornografinei produkcijai

gaminti, arba pelnėsi iš tokios vaiko veiklos arba dalyvavo pornografinio pobūdžio renginyje, į kurį buvo įtrauktas vaikas. Taip pat atsako juridinis asmuo.

5. Disponavimas pornografinio turinio dalykais (LR BK str. 309 straipsnis); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad 1 –oje dalyje platino, pagamino ar įsigijo arba platino pornografinio turinio dalykus. 2 – oje dalyje pagamino, įgijo, laikė, demonstravo, reklamavo, siūlė arba platino pornografinio turinio dalykus, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas, arba pasinaudodamas informacinėmis ir ryšių technologijomis ar kitomis priemonėmis įgijo ar suteikė prieigą prie pornografinio turinio dalykų, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas,. 3 – oje dalyje kas turėdamas tikslą platinti pagamino ar įsigijo arba platino didelį kiekį pornografinio turinio dalykų, kuriuose vaizduojamas mažametis vaikas. 4 –oje dalyje , kas demonstravo ar reklamavo pornografinio turinio dalykus.

6. Sukčiavimas (LR BK 182 straipsnis); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad 1 –ojoje dalyje apgaule savo ar kitų naudai įgijo svetimą turtą ar turtinę teisę, išvengė turtinės prievolės arba ją panaikino.

2 –ojoje dalyje 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. 3 –ojoje dalyje apgaule savo ar kitų naudai įgijo nedidelės vertės svetimą turtą ar turtinę teisę, išvengė nedidelės vertės turtinės prievolės arba ją panaikino[83].

7. Disponavimas elektronine mokėjimo priemone arba jos duomenimis (LR BK 214 straipsnis); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad „gamino vieną ar daugiau netikrų elektroninių mokėjimo priemonių ar jų dalių ar suklastojo vieną ar daugiau tikrų elektroninių mokėjimo priemonių arba neteisėtai įgijo, laikė, perdavė ar realizavo vieną ar daugiau svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių, arba neteisėtai įgijo, laikė, perdavė ar realizavo vienos ar daugiau svetimų elektroninių mokėjimo priemonių ar jų naudotojo tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti, arba gamino, įgijo, laikė, perdavė ar realizavo techninę įrangą, programinę įrangą ar kitokias priemones, tiesiogiai skirtas ar pritaikytas netikroms elektroninėms mokėjimo priemonėms ar jų dalims gaminti ar tikroms elektroninėms mokėjimo priemonėms klastoti. Atsako ir juridinis asmuo“[84].

8. Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas (LR BK 215 straipsnis); Straipsnyje numatyta baudžiamoji atsakomybė taikoma už tai, kad neteisėtai inicijavo ar atliko finansinių operacijų viena ar daugiau svetimų, netikrų ar suklastotų elektroninių mokėjimo

---

[83] [83] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 182 str.

[84] [84] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 214 str.

priemonių arba neteisėtai panaudodamas vieną ar daugiau svetimų elektroninių mokėjimo priemonių ar jų naudotojo tapatybės patvirtinimo priemonių duomenis, arba panaudodamas žinomai netikrus vienos ar daugiau tapatybės patvirtinimo priemonių duomenis, arba žinomai neteisėtą vienos ar daugiau svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių panaudojimą pripažino teisėtu. Atsako ir juridinis asmuo.[85]

3. NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE TYRIMŲ TARPTAUTINĖ IR NACIONALINĖ PRAKTIKA

Tarptautinė kova su elektroniniais nusikaltimais priklauso nuo patikimų bendradarbiavimo priemonių ir vieningai suderintų valstybinių įstatymų. Remiantis bendru dvigubo baudžiamumo principu, efektyviam tarptautiniam bendradarbiavimui yra būtinas baudžiamosios teisės nuostatų suderinimas, su tikslu išvengti saugaus prieglobsčio bet kurioje valstybėje sukūrimu.[86] Svarbu suderinti tyrimo priemones, kad visos valstybės, dalyvaujančios tyrime turėtų būtinas priemones efektyviam tyrimui užtikrinti ir vadovautųsi naujausia teismų praktika.

Vadovaujantis informacinių technologijų pateikta statistika 2014 metų, elektroninių nusikaltimų žala siekė 110 milijonų JAV dolerių, daugiau nei 2013 metais 100 milijonų JAV dolerių. Nukentėjusiųjų nuo šio tipo nusikaltimų yra 550 milijonų. 33% saugumo pažeidimų buvo padaryta ir nuolatinės prieigos.[87] Daugiausiai elektroninių nusikaltimų buvo atliekama Irane, Vietname, Rusijoje. Vyriausybės atstovai, atsakantys už informacinių technologijų plėtrą, teigia, kad biudžetas, skiriamas apsaugoti valstybę nuo elektroninių nusikaltimų bei kibernetinių įsilaužimų, kiekvienais metais yra vis didesnis.

Per 2013 m. JAV užfiksuota,143211 įsilaužimų į mobiliojo ryšio išmaniąją įrangą:

- 33,5% su tikslu pavogti pinigus (kenkėjiškų programų pobūdis - siųsti SMS žinutes, numeriais, kuriais tokios paslaugos yra brangiai apmokamos, įsiminti elektroninės bankininkystės prisijungimo duomenis, elektroninių piniginių ištuštinimas (pvz QIWI), Bitcoin valiutos vagystės).
- 20,6% su tikslu pavogti ar neteisėtai pasisavinti duomenis (kenkėjiškų programų pobūdis – internetinių paskyrų pasisavinimas, SMS ir elektroninio pašto laiškų skaitymas, nuotraukų ir įrenginyje esančių kitų duomenų pasisavinimas).
- 19,4% su tikslu uždirbti pinigų (kenkėjiškų programų pobūdis – prijungia įrenginį prie programos, kuri pradeda valdyti įrenginį t. y. Siųsti elektroninius laiškus ir sms padidintu

[85] [85] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 2015 str.
[86] WSIS Thematic Meeting on Cybersecurity. Geneva, June 28 - July 1, 2005. http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf [žiūrėta 2015-03-30]
[87] 15new cybercrime infographics from april 2014 http://www.hacksurfer.com/posts/15-new-cybercrime-infographics-from-april-2014 [žiūrėta2015-04-13]

kiekiu, vykdyti operacinės sistemos atakas, naudojantis interneto ryšiu, automatiškai parenka nuorodas, kurių paspaudimas kainuoja).

- 26,5% su tikslu sekti mobiliojo įrenginio naudotoją (kenkėjiškų programų pobūdis – nustatyti įrenginio buvimo vietą, mikrofono ir vaizdo kameros automatinis valdymas, skambučių istorijos analizė.

Nusikaltimų elektroninėje erdvėje tyrimas ir sudėtingumas:

Dažnai pasitaiko, kad nusikalstama veika padaroma iš kitos valstybės, dažniausiai JAV, Airijoj, Didžiojoj Britanijoj ar Norvegijos teritorijoje esančio kompiuterio ir ten gyvenančio jo naudotojo. Nustačius kurioje valstybėje yra padaryta nusikalstama veika, yra siunčiamas teisinės pagalbos prašymas kitai valstybei, dėl duomenų pateikimo. Toks susirašinėjimas yra ilgas ir ne visada duodantis teigiamų rezultatų. Kai kuriose šalyse net ir nustačius IP adreso vartotoją, baudžiamasis persekiojimas tampa neįmanomas, nes toje šalyje pagal galiojančius įstatymus ši veika yra nebaudžiama ir duomenys nepateikiami. Generalinės prokuratūros 2009-12-23 Metodinės rekomendacijos Nr. 12.14-40 „Dėl nusikalstamų veikų, padarytų rasiniais, nacionalistiniais, ksenofobiniais, homofobiniais ar kitais diskriminacinio pobūdžio motyvais, ikiteisminio tyrimo organizavimo, vadovavimo jam ir atlikimo ypatumų“ numato, kad tokiais atvejais ikiteisminio tyrimo pareigūnas turėtų teisės aktuose nustatyta tvarka raštu reikalauti iš ikiteisminio tyrimo įstaigos ar prokuratūros analogiškos nusikalstamos veikos ikiteisminio tyrimo atveju gautų dokumentų, kurie supaprastintų ikiteisminio tyrimo atlikimą. Kitais atvejais šalys duomenų pateikti negali, nes praeina laikas, numatytas informacijai apie IP naudotoją saugoti. Nusikalstamas veikas darantys asmenys išnaudoja technologinę pažangą savo kėslams, kuriamos vis sudėtingesnės programos, virusai, kuriais būtų galimą padaryti didesnės žalos, nuslėpti nusikalstamas veikas, sunaikinti šių veikų pėdsakus, tyrimui reikšmingus daiktus, dokumentus, duomenis ir taip apsunkinti tyrimą, bei likti nenubaustiems. Tyrimai nusikaltimų elektroninėje erdvėje sėkmingi, kai tinkamai pirminių neatidėliotinų tyrimo veiksmai parenkami ir atlikimas bei glaudus bendradarbiavimas su specialistais, laiku ir operatyviai nustatytas IP adresai.

Tyrimo procesą apsunkina:

- Tarptautinis Interneto pobūdis; problemos gaunant duomenis iš užsienio šalių Interneto paslaugų tiekėjų.

- Galimybės likti anonimiškam.

- Duomenų rinkimas ir fiksavimas

- Duomenų trumpalaikiškumas; kai duomenys, IP adresai pas interneto paslaugų tiekėjus saugomi 6 mėnesius, greitai galima pašalinti duomenis, reikšmingą informaciją.

- Slaptažodžių ir informacijos, susijusios su įtariamaisiais, paieška Internete.

- Debesų kompiuterija; paties vartotojo kompiuteris turi tik minimalų programinės įrangos kiekį – operacinę sistemą ir interneto naršyklę. Visi kiti ištekliai gaunami iš interneto linijomis. Tokiu atveju, jei nusikaltimui įvykdyti būtų panaudoti tik interneto linijomis, nebūtų galimybės išimti kompiuterių tyrimui, kadangi vartotojo kompiuteris yra tik prieiga prie jo resursų, o interneto linijos tik paslaugų teikėjo skaičiavimo centre saugomi duomenys daugybės, tarpusavyje nesusijusių, vartotojų. Debesų kompiuterijos atakos vadinamos „DDoS“, kurios yra užsakomos. Atakų, kurių metu virusais užkrėstų kompiuterių tinklas, siunčia į taikinį milžinišką užklausų kiekį, o srauto neatlaikę serveriai nulūžta. Įsigyti galima ir specifinių kenkėjiškų programų. Vienas programišius skelbia: „Rašau ir parduodu „trojanus“ ir kitas kenkėjiškas programas. „Trojanas“ banko duomenų vagystėms – 1,3 tūkst. dolerių, įsilaužimui į vartotojo interneto naršyklę – 850 dolerių, DDoS „bot‘as“ – 350 dolerių, kreditinių kortelių tikrinimo programa – 70 dolerių.“[88] 2013 metais buvo įvykdyta kibernetinė ataka prieš Londone ir Ženevoje įsikūrusią kompaniją „Spamhaus“ ekspertai jau vadina didžiausia istorijoje. Surengtas išpuolis buvo toks intensyvus, kad dėl jo lėčiau veikė viso pasaulio internetas. „Tokių išpuolių metu programišiai pasitelkia savo kontroliuojamus serverius, bei į „botnet“ tinklą sujungtus kompiuterius, kurie siunčia atakuojamam serveriui milžinišką beprasmių duomenų kiekį, tikėdamiesi jį tiesiog „nulaužti“ ir bent laikinai nutraukti jo darbą.“[89]
- Jurisdikcija sukelia problemų; pavyzdžiui, Yahoo.com byloje kaltinimą palaikė LICRA – tarptautinė lyga prieš rasizmą ir antisemitizmą, jie skundėsi kad internetiniame www.yahoo.com aukcione buvo pardavinėjamos nacistinio pobūdžio relikvijos. LICRA rėmėsi Prancūzijos baudžiamojo kodekso R 645-1 straipsniu, kurio normos šiuo atveju draudžia nacistinių simbolių eksponavimą ar kitokį jų panaudojimą. Yahoo.com kompanija teigė, kad nėra techninių priemonių užkirsti kelią Prancūzijos gyventojams dalyvauti jų aukcionuose, nesukuriant papildomų finansinių sunkumų. Taip pat jie pažymėjo, kad jų serveriai buvo įsikūrę JAV teritorijoje, jų paslaugos pirmiausia buvo skiriamos JAV gyventojams ir, kad ginčas turi būti priskiriamas JAV jurisdikcijai.[90] Prancūzijos

[88] Kibernetinė ataka. http://www.15min.lt/mokslasit/straipsnis/verslas/programisiu-duona-ar-sunku-suorganizuoti-kibernetine-ataka-649-340567 [žiūrėta2015-04-12]
[89] Kibernetinė ataka. http://it.lrytas.lt/techno/didziausia-visu-laiku-kibernetine-ataka-suletino-pasaulini-interneta.htm [žiūrėta2015-04-12]
[90] Byla LICRA prieš Yahoo. http://en.wikipedia.org/wiki/LICRA_v._Yahoo [žiūrėta2015-04-12]

aukščiausiasis teismas nusprendė, jog buvo pakankamas ryšys su Prancūzija suteikti jai visišką jurisdikciją nagrinėti skundą. Nacių relikvijų aukcionai buvo atviri dalyviams iš bet kurios šalies, įskaitant Prancūziją. Yahoo.com žinojo, kad Prancūzijos gyventojai naudojosi aukciono svetaine, nes atveriant svetainę iš Prancūzijos ji buvo rodoma prancūzų kalba. Yahoo.com nusprendė paduoti ieškinį JAV apygardos teismui San Franciske, tikėdamiesi gauti nutartį, kad Prancūzijos teismo nutartis negali būti vykdoma prieš Yahoo.com Jungtinėse Amerikos Valstijose. JAV apygardos teisėjas Jeremy Fogel nustatė, kad Prancūzijos teismo sprendimas yra nesuderinamas su pirmąja pataisa į JAV Konstituciją, kuri garantuoja žodžio ir saviraiškos laivę, ir kad bet koks mėginimas priversti vykdyti teismo sprendimą JAV prieštarauja JAV Konstitucijai.[91] Nusikaltimai elektroninėje erdvėje yra plataus pobūdžio veikla, kuri dėl savo sudėtingumo tampa sunkiai atskleidžiama. Tarptautinės jurisdikcijos ribų neaiškumas tiriant elektroninius nusikaltimus, prisideda prie techninio tyrimo sudėtingumo. Dar vienas jurisdikcijos atvejis byloje Bavarija v Somm, kurioje vienos Vokietijos įmonės generalinis direktorius, kuris turėjo Šveicarijos pilietybę, buvo atsakingas už prieigas Vokietijoje į smurtinius, vaikų pornografijos interneto tinklapius, kurių serverio paslaugas atliko Vokietijos kompanija, tačiau patys serveriai buvo JAV. Teismas nusprendė, kad ginčą turi nagrinėti Vokietijos teismas nes generalinis direktorius faktiškai gyvena Vokietijoje ir nusikalstama veika padaryta šios valstybės teritorijoje, nepaisant to kad jis yra Šveicarijos pilietis.[92]

- Skirtingas nusikalstamų veikų kriminalizavimas, skirtingose šalyse; Pavyzdžiui, 2000 metais kompiuterinis virusas „Love Bug'' padarė žalą dešimtims milijonų kompiuterių visame pasaulyje. JAV agentai greitai atsekė į Filipinus, vietą iš kurios kilo virusas. Tačiau Filipinai savo baudžiamajame įstatyme neturėjo kriminalizavę tokios nusikalstamos veikos kaip įsilaužimas į kompiuterį. Spraga įstatyme sudarė sąlygas, likti nenubaustiems.[93] Tendencijos rodo, jog nusikaltėliai, imasi priemonių, siekdami apsunkinti nusikaltimų tyrėjų darbą: taiko duomenų šifravimo metodikas, naudoja automatizuotas įkalčių naikinimo priemones bei vengia tiesiogiai naudoti savo kompiuterius nusikaltimams vykdyti. Todėl asmenims, tiriantiems šias nusikalstamas veikas, reikalingas nuolatinis žinių ir techninės bazės atnaujinimas.

2009 metų Baudžiamojoje byloje Yahoo! Inc., kaltinamasis buvo Yahoo kaltinamas ir pripažintas kaltu, dėl Tiesiogiai įvykdė nusikaltimą ar baudžiamąjį nusižengimą, arba tiesiogiai

[91] Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme http://cyber.law.harvard.edu/is02/readings/yahooorder.htm [žiūrėtas 2015-04-12]

[92] People v. Somm, Case 8340 Ds 465 Js 173158/95 (Amstsgericht, Munchen, Bavaria)

[93] Philippine investigators detaion man in seach for 'Love Bug' creator Clinton to attend funeral of cardinal John O'Connor http://www.mail-archive.com/htmlquicknews@cnnimail4.cnn.com/msg00036.htm [žiūrėta2015-04-13]

dalyvavo vykdyme, teikė pagalbą vykdymo per kokio nors veiksmo, kokia tokiu būdu, kad nusikaltimas ar baudžiamasis nusižengimas negalėjo būti padarytas be jos pagalbos, arba turintys tiesiogiai skatina nusikalstamumą ir pažeidė JAV baudžiamojo kodekso 66 straipsnis: Atsižvelgiama į tai, kad Belgijos kodeksą pažeidė 46bis straipsnį.

Prieiga prie informacinės sistemos siaurinama Kanzaso valstijos Aukščiausiojo Teismo 1996 m., šioje baudžiamojoje byloje nustatyta, kad kaltininkas naudojo savo kompiuterį su įrengtu modemu bandydamas apie 28 kartus interneto ryšiu susisiekti su „Southwestern Bell Telephone“ bendrovės kompiuterio sistemos įrenginiais, kontroliuojančiais tarpmiestinių skambučių jungiklius. Sėkmingo sujungimo atveju, jam būtų suteikta galimybė padaryti neribotą skaičių nemokamų tarpmiestinių skambučių. Teismas byloje prieigą prie kompiuterinės sistemos išaiškino pagal įprastinę suprantamą jos reikšmę. Konstatuota, kad ko kaltininkas veikė neperžengdamas sistemos nustatytų apribojimų, negalima teigti, kad jis siekė pasinaudoti kompiuteriais ar gauti naudos.

2013 metais Lewys Martin Didžiosios Britanijos pilietis nuteistas 2 metų laisvės atėmimo bausmė, kadangi įsilaužė į Kembridžo universiteto ir Oksfordo universiteto interneto svetainėse. Buvęs NullCrew įsiskverbė ir į Gynybos departamento (DoD), Pentagonas, NASA, NSI, kitos JK valdžios institucijų tinklavietes, serverius.

Adrian Lamo Jungtinėse Valstijose 2004 metais dėl kompiuterinių nusikaltimų prieš Microsoft , LexisNexis ir "The New York Times", nuteistas šešių mėnesių laisvės atėmimo bausme, plius dveji metai lygtinai ir maždaug JAV restitucijos 65.000 $

Cameronas Lacroix Jungtinės valstijos nuteistas 2005 metais, dėl įsilaužimo į mobiliųjų telefonų sąskaitos įžymybių Paris Hilton ir dalyvavo duomenų surinkimo įmonės atakos LexisNexis grupėse ir nuteistas 11 mėnesių Massachusetts nepilnamečių įkalinimo įstaigos.

Nikolajus Riteris Jungtinėse Valstijose 2014 metais nuteistas, dėl įsilaužimų, neteisėtų veiksmų, kuriais siekta pakenkti Vidaus saugumo departamentui, Kongreso biblioteka, ir daugybė kitų vyriausybinių ugdymo įstaigų.

Analizuojant Lietuvos Respublikos elektroninių nusikaltimų praktiką, BK 198- 1 str numatytą neteisėto prisijungimo prie informacinės sistemos 2012 metai birželio 26 d. baudžiamojoje byloje Nr. 2K-375/2012[94] Joje sprendžiama numatytų veikų 198 ir 215 str., pažymėta, kad kaltininko veiksmai neteisėtai prisijungus prie internetinės bankininkystės sistemos, panaudojant svetimus identifikavimo duomenis, galėtų būti kvalifikuojami pagal BK 198 -1 str., kaip neteisėtas prisijungimas prie informacinės sistemos pažeidžiant apsaugos priemones. Pavyzdžiui Klaipėdos miesto apylinkės teismas baudžiamojoje byloje Nr 1-740-93-2009[95] V.B. nuteistas už neteisėta

[94]Baudžiamoji byla LAT Nr. 2K-375/2012
[95]Baudžiamoji byla Klaipėdos miesto apylinkės teismas Nr 1-740-93-2009

prisijungimą prie informacinės prekybos sistemos. Teismas pripažino kaltu padarius nusiklastamą veiką numatytą BK 198-1 straipsnio 1 dalyje.

Baudžiamojoje byloje 2K-29-2014[96] A. V. pirmosios instancijos teismo nuosprendžiu nuteistas pagal BK 1982 straipsnio 1 dalį už tai, kad, turėdamas tikslą daryti nusikalstamas veikas, numatytas BK 197 straipsnyje, nenustatytu laiku, tačiau ne vėliau kaip 2010 m. lapkričio 2 d., internetu įgijo programinę įrangą, skirtą elektroninės paslaugos trikdymo atakoms vykdyti, ją skaitmeninėje išorinėje USB laikmenoje laikė bei 2010 m. lapkričio 2 d. perdavė UAB „R.“ darbuotojui P. P. nusikalstamoms veikoms, numatytoms BK 197 straipsnio 1 ir 3 dalyse, vykdyti.

LAT baudžiamojoje byloje 2K-93-489/2015[97] E. K. buvo kaltinamas tuo, kad būdamas UAB „R.“ direktorius, vadovaujamos įmonės veiklos vietoje, naudodamasis įmonės interneto ryšio elektroninės prieigos adresu ir kompiuterine technika, 2011 m. rugpjūčio 10 d. 14.36 ir 14.52 val., pažeisdamas informacinės sistemos apsaugos priemones, neteisėtai pasinaudodamas žinomu prisijungimo prie elektroninės pašto dėžutės vardu ir slaptažodžiu, prisijungė prie elektroninio pašto dėžutės, kuri priklauso UAB „C. “ ir naudojama šios įmonės komercinei veiklai bei UAB „C. “ direktorės B. K. asmeniniams susirašinėjimams. Prisijungimo laiku neteisėtai, neturėdamas elektroninio pašto dėžutės savininko UAB „C. “ ir naudotojos B. K. leidimo, stebėjo elektroninių ryšių tinklais siunčiamos informacijos turinį. UAB „R.“ kurios direktorius E. K. turi teisę atstovauti bendrovei, jos vardu priimti sprendimus bei kontroliuoti bendrovės veiklą, buvo kaltinama tuo, kad įmonės veiklos vietoje, naudojant įmonės interneto ryšio elektroninės prieigos adresą) ir kompiuterinę techniką, 2011 m. rugpjūčio 10 d. 14.36 ir 14.52 val., pažeidžiant informacinės sistemos apsaugos priemones, neteisėtai pasinaudojant prisijungimo prie elektroninės pašto dėžutės vardu ir slaptažodžiu, prisijungė prie elektroninio pašto dėžutės .Prisijungimo laiku neteisėtai, neturint elektroninio pašto dėžutės savininko UAB „C. “ ir naudotojos B. K. leidimo, stebėjo elektroninių ryšių tinklais siunčiamos informacijos turinį.

Taigi, nusikaltimai elektroninėje erdvėje yra labai plataus pobūdžio veikla, kuri dėl savo sudėtingumo tampa sunkiai atskleidžiama.

3.1. Nusikaltimų elektroninėje erdvėje prevencija ir problemos

Nusikaltimų elektroninėje erdvėje prevencija, tai saugumo priemonės kuriomis siekiama išvengti nusikaltimų. Prevencijos tikslas užkirsti kelią nusikaltimams atsirasti ir plisti.

Nusikaltimų elektroninėje erdvėje prevencijos kryptimis ir strategijomis, siekiama nutraukti bei užkirsti kelią elektroniniams nusikaltimams daryti. Europos Sąjungos šiuo metu tikslas kibernetinio

[96] Baudžiamoji byla LAT 2K-29-2014
[97] Baudžiamoji byla LAT 2K-93-489/2015

saugumo didinimas Europos Sąjungoje. 2014 metais kovo 13d., Europos Parlamentas priėmė direktyvą, dėl tinklų ir informacinių sistemų saugumo. „Tai svarbi kibernetinio saugumo strategijos dalis. Pagal ją visos Europos Sąjungos valstybės narės, pagrindinių interneto paslaugų teikimo bendrovės ir infrastruktūros operatoriai būtų įpareigoti užtikrinti saugią ir patikimą skaitmeninę aplinką visoje Europos Sąjungoje. Kadangi dabartinis požiūris į tinklų ir informacinių sistemų saugumą yra grindžiamas savanoriškais veiksmais, nacionaliniai pajėgumai ir privačiojo sektoriaus dalyvavimo ir pasirengimo lygis valstybėse narėse labai skiriasi. Direktyvos projektu siekiama vienodų sąlygų, nustatant suderintas taisykles, kurios būtų taikomos visose Europos Sąjungos šalyse.[98] Siūlomos priemonės:

- Kiekvienai Europos Sąjungos valstybei narei keliamas reikalavimas priimti tinklų ir informacinių sistemų saugumo strategiją ir paskirti tinklų ir informacinių sistemų saugumo instituciją, turinčią pakankamai išteklių užkirsti kelią tinklų ir informacinių sistemų saugumo rizikai ir incidentams, juos spręsti ir imtis atsakomųjų veiksmų;

- Valstybių narių ir Komisijos bendradarbiavimo mechanizmo, skirto teikti išankstinius perspėjimus apie riziką ir incidentus, keistis informacija ir kovoti su tinklų ir informacinių sistemų saugumo grėsmėmis bei incidentais, sukūrimas;
- Tam tikroms skaitmeninių paslaugų bendrovėms ir tarnyboms keliamas reikalavimas priimti rizikos valdymo priemones ir pranešti apie didelius tinklų ir informacinių sistemų saugumo incidentus kompetetingai nacionalinei valdžios institucijai.

Reikalavimu pranešti apie tinklų ir informacinių sistemų saugumo incidentus siekiama sukurti rizikos valdymo kultūrą ir užtikrinti, kad privatusis ir viešasis sektoriai keistųsi informacija. Jis taikomas:

- Ypatingos svarbos infrastruktūros objektų operatoriams tokiuose sektoriuose kaip finansinės paslaugos, transportas, energetika ir sveikatos priežiūra;
- Tinklų ir informacinių sistemų saugumo paslaugų bendrovėms, įskaitant programėlių parduotuves, e. prekybos platformas, mokėjimų internetu platformas, debesijos kompiuterijos platformas, paieškos sistemas ir socialinius tinklus;
- Viešojo administravimo įstaigoms.[99]

Užsienio reikalų ministerijos 2015 metų veiklos prioritetai stiprinti transatlantinius santykius su JAV, siekiant glaudesnio JAV ir Lietuvos bendradarbiavimo kibernetinio saugumo srityje, užtikrinti JAV indėlį bendro veiksmų plano kibernetinio saugumo srityje įgyvendinimą.[100]

[98] Kibernetinio saugumo didinimas ES. http://www.consilium.europa.eu/lt/policies/cyber-security/ [žiūrėta2015-04-04]
[99] Ten pat. [žiūrėta2015-04-03]

Londono Globalinio Universiteto (UCL) Jill Dando saugumo ir kriminologijos institutas 2015 metų vasario 26-27 dienomis Mančesteryje (Jungtinė Karalystė) organizuoja Tarptautinę nusikaltimų ir informacijos analizės konferenciją (International Crime and Intelligence Analysis Conference). Konferencija skirta žvalgybos profesionalams, analitikams, tyrėjams ir mokslininkams, besidomintiems šiomis problemomis ir siekiantiems užkirsti kelią nusikaltimams elektroninėje erdvėje. Didžiausias dėmesys bus skirtas praktiniams metodams ir jų taikymui, orientuojantis į policijos darbo gerinimą bei viešojo saugumo užtikrinimą, nors mielai laukiami ir akademinio darbo atstovai. Konferencijos metu vyks mokymai bei bus sudarytos galimybės pasidalinti gerąja patirtimi, naudojantis realių bylų modeliais bei kartu ieškant optimalių sprendimo būdų, remiantis naujaisiais tyrimų metodais bei tos srities lyderių patirtimi.[101]

Taip pat yra vykdomos tarptautinio ir nacionalinio pobūdžio konferencijos, rengiami strateginiai planai. Tai tik parodo, kad valstybės ieško sprendimo būdų, kaip užkisti kelią elektroniniams nusikaltimams ir neleisti jiems plisti.

Elektroninių nusikaltimų prevencinės priemonės yra skirstamos į teisines, organizacines – technines ir kompleksines.

Teisinės elektroninių nusikaltimų prevencijos priemonės, tai:

1. Teisės aktai, kurie reglamentuoja elektroninius nusikaltimus, vidines organizacijų taisykles.
2. Priimami įstatymai, kurie numato atsakomybę už padarytą nusikalstamą veiką.

Organizacinės – techninės elektroninių nusikaltimų priemonės, tai:

1. Organizacinės.
2. Techninės.
3. Kompleksinės.[102]

1. Organizacinė priemonės, tai personalo tikrinimas, instruktavimas, planų sudarymas, kompiuterinių priemonių priežiūra, atsakomybės nustatymas asmenims dirbantiems su kompiuterine technikas nustatymas.

Organizacinės priemonės:

1. Organizacinis saugumas: Tai priemonės kurias reikia įgyvendinti, norint užtikrinti administracinį saugumą. Numatomos saugumo pareigos, atsakomybė paskiriama, kurių reikia laikytis. Planai ruošiami nenumatytų atvejų, tokių kaip atsarginis išėjimas iš pastato, gaisro metu.

---

[100]Užsienio reikalų ministerijos 2015 metų veiklos prioritetai. https://www.urm.lt/default/lt/uzsienio-politika/naujienos-kalbos-publikacijos/uzsienio-reikalu-ministerijos-2015-metu-veiklos-prioritetai [žiūrėta2015-04-07]

[101]International Crime and Intelligence Analysis Conference 2015 http://www.ucl.ac.uk/jdi/events/int-CIA-conf/#tabs-3 [žiūrėta2015-04-10]

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

2. Personalinis saugumas: Tai priemonės, kurios yra nukreiptos į personalo saugumą, identifikaciją, pavaldumą, pareigas, kvalifikacijos kėlimas ir pan. Kompiuterines sistemas ir informaciją dažniausiai pažeidžia pats žmogus, iš nežinojimo, nemokšiškumo ar saugumo nesilaikymo. Kai kurie gali pažeisti kompiuterines ar informacines sistemas ir iš nusikalstamų tikslų, siekimo atkeršyti ar pasipelnyti. Tokie asmenys gali būti profesionalūs nusikaltėliai kurių tikslas pasipelnyti, gali ir kerštauti buvę ar nepatenkinti darbuotojai. Kad apsisaugoti kompiuterines sistemas ir jose esančią informaciją nuo nusikaltimų reikia, didelį dėmesį skirti personalui dirbančiam ir naujiems pretendentams pageidaujantiems dirbti. Taip pat reiktų personalo darbuotojus supažindinti su naujovėmis, vesti mokymus, kad klaidų personalas kuo mažiau pridarytų ir žinotų kaip reikia tinkamai elgtis su kompiuterine sistema ir joje esančia informacija.

Vienas iš pagrindinių kompiuterinės informacijos incidentų priežastis tai, nepakankamas švietimas personalo darbuotojų informacijos saugumo srityje.

3. Prevencinis saugumas: Tai priemonės kuriomis siekiama užkirsti kelia kompiuteriniams nusikaltimams atsirasti ir plisti.

Personalo darbuotojų švietimas užtikrina kompiuterių ir informacijos apsaugą:

- Prieigą prie informacinės sistemos turi turėti autorizuoti vartotojai;
- Turi būti užtikrinamas ankstyvas sukčiavimo ir kitų nusikaltimų aptikimas ir nustatymas;
- Jei nusikaltimas padarytas, tai turi būti sumažinamas žalos dydis.
- Turi būti sudarytos galimybės prarastos informacijos atkūrimui.

Norint užtikrinti personale gerą informacijos saugumą būtina:

- Įdiegti ugniasienę. Kuri riboja programų ar kitų kompiuterių sąveiką su internetu. Kadangi įmonės kompiuteriniame tinkle yra daug naudingos informacijos, kuri be ugniasienės yra lengvai prieinama įsibrovėliams. Įsibrovėliai gali pasisavinti neteisėtai kompiuteriniame tinkle esančią informaciją.
- Įdiegti geras antivirusines sistemas, kurios apsaugotų kompiuterį nuo virusų.
- Įdiegti modernias duomenų kopijų darymo sistemas. Duomenų kopijos po incidentų leis greičiau grįžti prie normalaus darbo tempo.
- Įsitikinti darbuotojų sąžiningumu ir įvertinanti riziką.

2. Techninės priemonės tai, techninių priemonių organizavimas, siekiant apsaugoti kompiuterinėje sistemoje esančią informaciją, tai vartotojų teisių sistema, antivirusinių programų diegimas į kompiuterines sistemas.

Taigi technines priemones galima suskirstyti į du apsaugos tipus:

- Fizinė įranga. Tai kompiuterinė įranga, nešiojamos bei saugojimo laikmenos ir kita informacijos saugojimo ar perdavimo įranga. Kurios veikimo principas, apsaugoti

kompiuterinę sistemą nuo pašalinio poveikio. Fizinė apsauga apsaugo visus su kompiuterine 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.[103] Pavyzdžiui, fizinės įrangos būna, prietaisai apsaugantys nuo įtampos šuolių, identifikacijos vartotojų bandančių prisijungti prie kompiuterinės sistemos, signalizacinės priemonės ir pan. Kompiuterio fizinė apsauga naudojama ir nenumatytų atvejų, nelaimių prevencijai, bei padarytos žalos sumažinimui.

- Programinė įranga. Tai programinė įranga ir programavimo priemonės. Programinė įranga skirta apsaugoti programinei informacijai.

Prie problemų, susijusių su programine apsauga, reikėtų paminėti ir apsaugos nuo kompiuterinių virusų problemą. Čia reikia aktyviai naudoti specialias antivirusines programas. Tačiau atkreiptinas dėmesys į tai, jog antivirusinės programos aptinka jau esančius virusus, kirminus ir kitas kenkėjiškų programų formas, kai tuo tarpu šios antivirusinės programos negali apsaugoti nuo užkrėtimo tokiomis kenkėjiškomis programomis.[104] Apsaugai taip pat reiktų informuoti įstaigos darbuotojus apie galimas grėsmes kompiuterinėje sistemoje. Europos Sąjungos valstybės atkreipia dėmesį, kad būtinas valstybių didesnis bendradarbiavimas,

3. Kompleksinės priemonės tai, kompleksinė apsauga verčia sukurti vieningą sistemą, kuri galėtų atremti visas galimas atakas, nukreiptas į kompiuterinę sistemą - nuo durų išlaužimo ir aparatinės įrangos pavogimo iki informacijos vagystės iš kompiuterinės sistemos. Į kompleksinę apsaugą integruojamos visos anksčiau minėtos apsaugos priemonės.[105]

Pateikiami pagrindiniai elektroninio saugumo principai:[106]

1. Pagrindinių žmogaus teisių, nuomonės reiškimo laisvės, privatumo ir asmens duomenų apsauga.[107]

[103] Petrauskas, R.; Štitilis, D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 56.
[104] Ghosh, S.; Turrini, E. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag, 2010, p. 110.
[105] Petrauskas, R.; Štitilis, D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademija, 2000, p. 61.
[106] Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace. file:///D:/My%20Documents/Downloads/1CybersecurityStrategyoftheEuropeanUnionAnOpenSafeandSecureCyberspace-JOIN20131final-722013%20(1).pdf [žiūrėta2015-04-10] p.1,2.
[107] Elektroniniai nusikaltimai. Metodinė priemonė./ Doc. dr. Darius Štitilis – Vilnius: Mykolo Romerio universitetas 2011.

Elektroninis saugumas gali būti efektyvu tik tuo atveju, jei pagrįstas pagrindinių teisių ir laisvių apsauga ir Europos Sąjungos vertybėmis. Asmenų teisės nageli būti tinkamai užtikrintos be saugių tinklų ir sistemų. Bet koks informacijos dalinimasis kibernetinio saugumo tikslais, kai įtraukti asmens duomenys, turi būti vykdomas laikantis ES duomenų apsaugos reguliavimo ir užtikrinti visapusišką individų teisių apsaugą šioje srityje.

2. Prieiga visiems Ribota prieiga prie interneto ar tokios prieigos nebuvimas sukelia nepatogumus piliečiams. Kiekvienas turi turėti prieigą prie interneto bei informacijos. Interneto integralumas bei saugumas turi būti garantuojamas, kad būtų užtikrinta saugi prieiga visiems.

3. Demokratinis ir efektyvus valdymas Skaitmeninis pasaulis nėra kontroliuojamas vienos struktūros (bendrovės). Šiuo metu yra keletas „žaidėjų“, kurių daugelis yra komerciniai arba nevyriausybiniai dariniai ir kurie įsitraukę į kasdieninį interneto resursų valdymą, protokolų ir standartų internetui kūrimą. Pabrėžtina tokių „žaidėjų“ svarba dabartiniame interneto valdymo modelyje ir parama šiam daugialypio valdymo požiūriui.

4. Bendra atsakomybė užtikrinant saugumą Didėjanti priklausomybė nuo informacijos ir komunikacijų technologijų suponavo pažeidžiamas vietas, kurios turi būti išanalizuotos, sumažintos ir apgintos. Tiek viešasis sektorius, tiek privačios įmonės, tiek individualūs vartotojai turi pripažinti šią bendrą atsakomybę, imtis apsaugos priemonių ir, jei reikia, – užtikrinti koordinuotus veiksmus, siekiant sustiprinti kibernetinį saugumą.

Kibernetinio saugumo strategijoje akcentuojami penki strateginiai prioritetai:[108]

1. Pasiekti elektroninį atsparumą.
2. Sumažinti elektroninių nusikaltimų skaičių.
3. Sukurti elektroninės gynybos politiką ir pajėgumus, kiek tai susiję su bendra saugumo ir gynybos politika.
4. Plėtoti pramonės ir technologinius išteklius, skirtus elektroniniam saugumui užtikrinti.
5. Sukurti nuoseklią tarptautinę elektroninės erdvės politiką ir remti pagrindines Europos Sąjungos vertybes.

Prevencijos kryptys turėtų būti taikomos:

- Siekimas užkirsti kelią elektroniniams nusikaltimams atsirasti ir plisti, tai pozityvi prevencija. Kuri yra vykdoma iki nusikaltimo padarymo. Pavyzdžiui, žmonių švietimas, mokymas, įtraukimas į darbinę veiklą.

[108] Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace. file:///D:/My%20Documents/Downloads/1CybersecurityStrategyoftheEuropeanUnionAnOpenSafeandSecureCyberspace-JOIN20131final-722013%20(1).pdf [žiūrėta2015-04-10] p.2.

- Siekimas užkirsti kelią plisti ir sustabdyti, jau padarytą nusikaltimą elektroninėje erdvėje, bei paskirti atsakomybę. Turėtų būti taikoma ir pozityvi ir negatyvi prevencija. Pavyzdžiui. Bausmė, žalos atlyginimas, kompensacija, reabilitacija.

Prevencija gali būti nukreipta į objektą:

- Bendroji, nukreipta į nusikalstamumą elektroninėje erdvėje skatinančių veiksnių šalinimą.
- Individualioji, nukreipta į tiesiogiai individualius asmenis, ar grupes. Siekiant paveikti, kad nedarytu nusikaltimų ir nuo jų tinkamai apsisaugotų.

Individualioji priemonė taikymo metodai:

- Įtikinimo metodas, tai reglamentuojančių įstatymų aiškinimas, supažindinimas su atsakomybę, veikų pavojingumu.
- Prievartos metodas, taikomas kai yra nustatyti teisės pažeidimai, ir taikoma atsakomybė.
- Pagalbos metodas, taikomas supažindinti kaip elgtis atitinkamose situacijose ir kur kreiptis pagalbos.

Prevencijos reikalavimai:

- Priimtinumas; Taikomos prevencinės priemonės turi būti priimtinos visuomenei, turi būti prevencinių priemonių realumas, reikalingumas.
- Teisėtumas; Taikomos prevencinės priemonės turi būti teisėtos, pagrįstos ir neviršijančios savo įgaliojimų. Turi būti nustatyta veiklos kompetencija, atsakomybė.
- Dinamiškumas; Prevencijos priemonės turi būti lanksčios, žvelgiančios į ateitį, galimus pokyčius.
- Darnumas; Prevencinių priemonių, projektų būtinas tarpusavio suderinamas.
- Tinkamumas; Prevencijos tikslai, uždaviniai yra tinkamai suformuluoti, sprendžiamiems klausimams spręsti.

Ankstyvosios prevencinės priemonės nukreiptos į rizikos veiksnius, duoda kur kas geresnius rezultatus, nei kontrolės priemonės. Prevencinėmis priemonėmis žmonėms suteikiamos žinios, jie jaučiasi saugesni, žino kaip elgtis atitinkamose situacijose. Turima dėti kuo didesnes pastangas kovai su elektroniniais nusikaltimais, nes kitaip gali grėsti didesnė grėsmė visuomenės saugumui. Tai visuotinė problema, reikia parengti tinkamus bendradarbiavimo planus, vadovautis geriausiais tyrimo metodais ir naujausia praktika, nes elektroniniai nusikaltimai gali smogti iš bet kurio pasaulio krašto.

Prevencinių priemonių problemos:

- Taip pat yra nepakankama prevencinė politika, pavyzdžiui neįprastai didelis informacijos srautas kompiuteryje gali byloti apie jo apkrovą ir leidžia daryti prielaidą, kad galbūt

vykdomi neteisėti procesai, tačiau į tai laiku nekreipiamas tinkamas dėmesys ir nereaguojama.

- Ilgas paskirtų informacinių technologijų tyrimų atlikimo terminas – iki 2 metų.

- Ribotos techninės galimybės, nes kasdien atsiranda įvairios piratinės programos, kurių pagalba keičiami IP adresai, jie užkrečiami virusu.

- Specialistų trūkumas ir nepakankamas tyrėjų, atliekančių ikiteisminius tyrimus dėl elektroninėje erdvėje padarytų nusikaltimų, mokymų organizavimas (arba jų organizavimas užsienio kalba).

- Internetinėje erdvėje atsirado galimybė keisti IP adresą ir tokiais atvejais yra visiškai neįmanomo surasti nusikalstamą veiką darančius asmenis.

- Šalys duomenų pateikti negali, nes praeina laikas, numatytas informacijai apie IP naudotoją saugoti. Būtina svarstyti apie galimybę tokius duomenis gauti be teisinės pagalbos prašymo siuntimo užsienio valstybėms., pvz. : pasinaudojant LR baudžiamojo proceso kodekso 155 str. numatyta galimybe gauti informaciją siunčiant prašymą tiesiogiai įmonei, administruojančiai atitinkamą IP adresą.

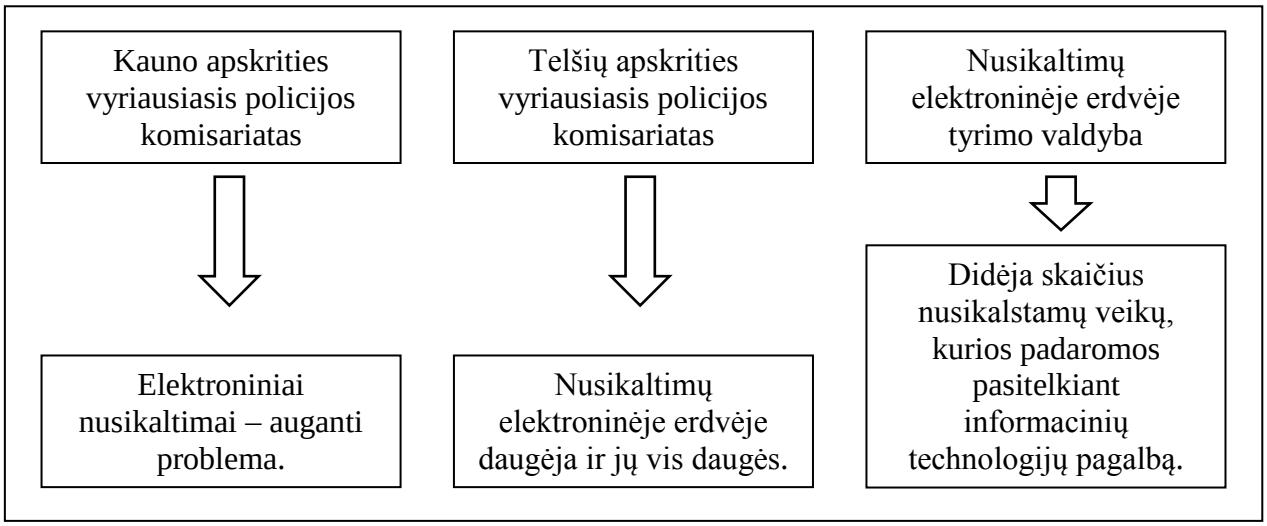
3.2. Pagrindinės nusikaltimų elektroninėje erdvėje tyrimo metodikos ir tobulinimo kryptys

Mokslinėje literatūroje yra pateikiami kriminalistinių metodinių rekomendacijų šaltiniai, kurie nulemia šių rekomendacijų raidą ir tobulinimo kryptis. Pagrindiniai šaltiniai, tai teisės normos, nusikaltimų tyrimo praktika ir mokslas.[109] Nusikaltimų elektroninėje erdvėje tyrimo metodikos atsispindi kriminalistinėje charakteristikoje. Pateikiamos elektroninių nusikaltimų sąvokos įrodinėtinos aplinkybės, padarymo būdus, dalyką, situacijas. Reikalingas kriminologinė charakteristika, kuri suteikia informacijos apie nusikaltimo padarymo priežastis, sąlygas, struktūrą, raidą. Kriminologinė charakteristika svarbi tuo, kad gauti duomenys, palengvintų ieškojime efektyvios prevencinės priemonės. Vienas iš metodikos šaltinių, nusikaltimų tyrimo praktika. Kuri leidžia apibendrinti nusikaltimų padarymą, tyrimo ypatumus, rengti metodines rekomendacijas, daryti išvadas. Kurios duodą gerus rezultatus kriminalistinei nusikaltimų charakteristikai, taip galima planuoti efektyvesnius tyrimus, kelti tikslesnes versijas, sutaupyti laiko.

[109] Kuconis, P. Nusikaltimų tyrimo metodikos raidos perspektyvos. 1993. p. 30.

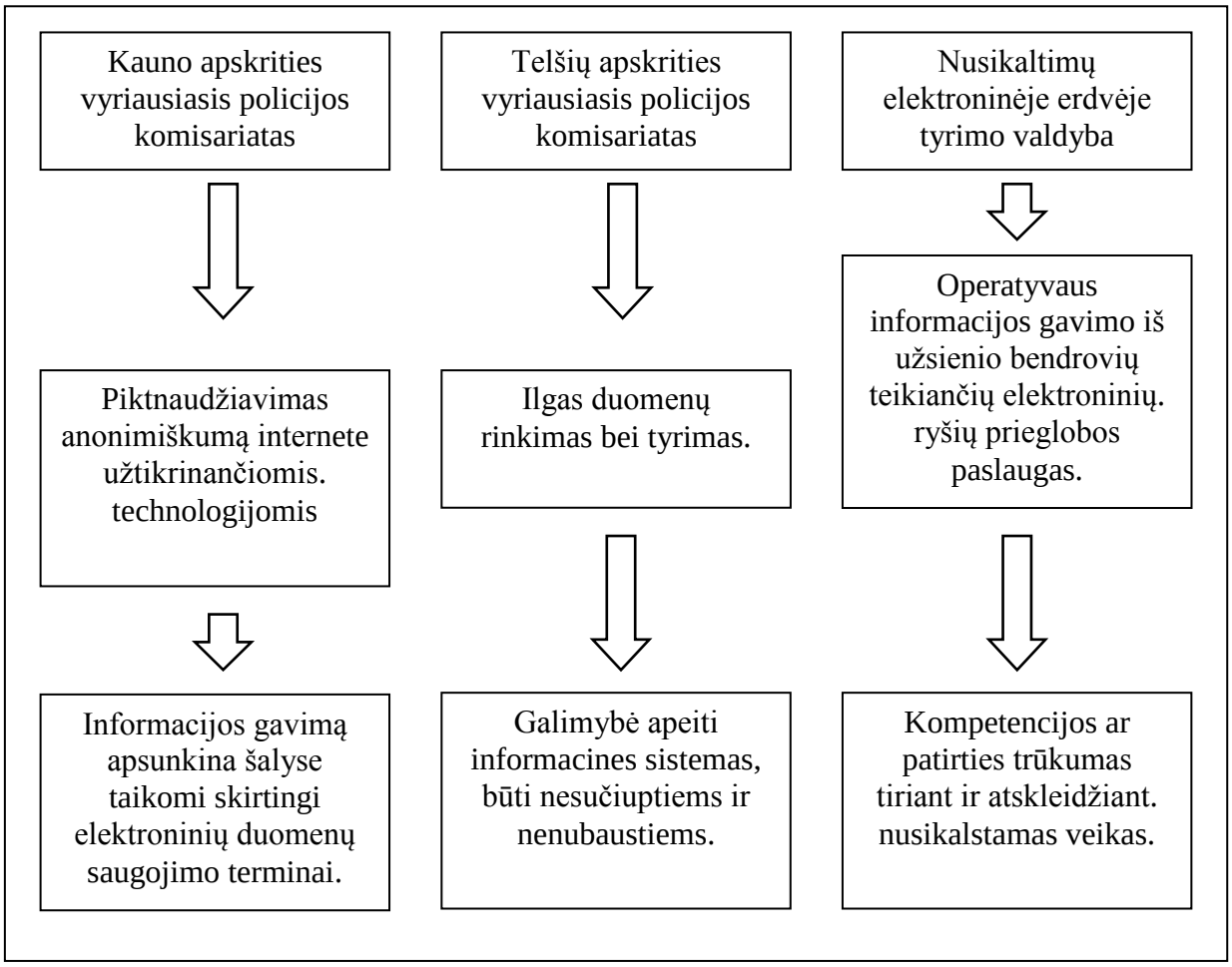
Šiam tyrimui buvo pasirinkti specialistai kurie tiesiogiai dirba su elektroniniais nusikaltimais juos tiria ir sprendžia problemas. Buvo interviu klausimynas pateiktas ir apklausti Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje valdybos du tyrėjai. Bei Kauno ir Telšių AVPK Kriminalinės policijos nusikaltimų nuosavybei tyrimo valdybos pirmojo skyriaus tyrėjai.

Apibendrinant Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo valdybos pateiktus tyrėjų atsakymus į interviu klausimus ir Kauno bei Telšių AVPK Kriminalinės policijos nusikaltimų nuosavybei tyrimo valdybos pirmojo skyriaus pateiktus atsakymus, galime teigti.



3.1. Lentelė. Nusikaltimų elektroninėje erdvėje vertinimas.

Kad nusikaltimus elektroninėje erdvėje vertina, kaip augančią problemą. Dėl nuolatinio technologinio progreso vis daugiau kasdienio gyvenimo procesų persikelia į elektroninę erdvę. Todėl nusikalstamo pasaulio atstovams atsiranda vis daugiau nišų realizuoti savo nusikalstamus ketinimus. Didėja skaičius nusikalstamų veikų, kurios gali būti padaromos pasitelkiant informacines technologijas. Į elektroninę erdvę persikelia net tradicinėmis laikyti nusikaltimai. Tobulėjant technologijoms, tobulėja ir nusikaltimų elektroninėje erdvėje schemos, sudėtingėja šiuos nusikaltimus vykdančių asmenų nustatymas, auga šiais nusikaltimais padaroma žala.



3.2. Lentelė. Nusikaltimų elektroninėje erdvėje tyrimo pagrindinės problemos.

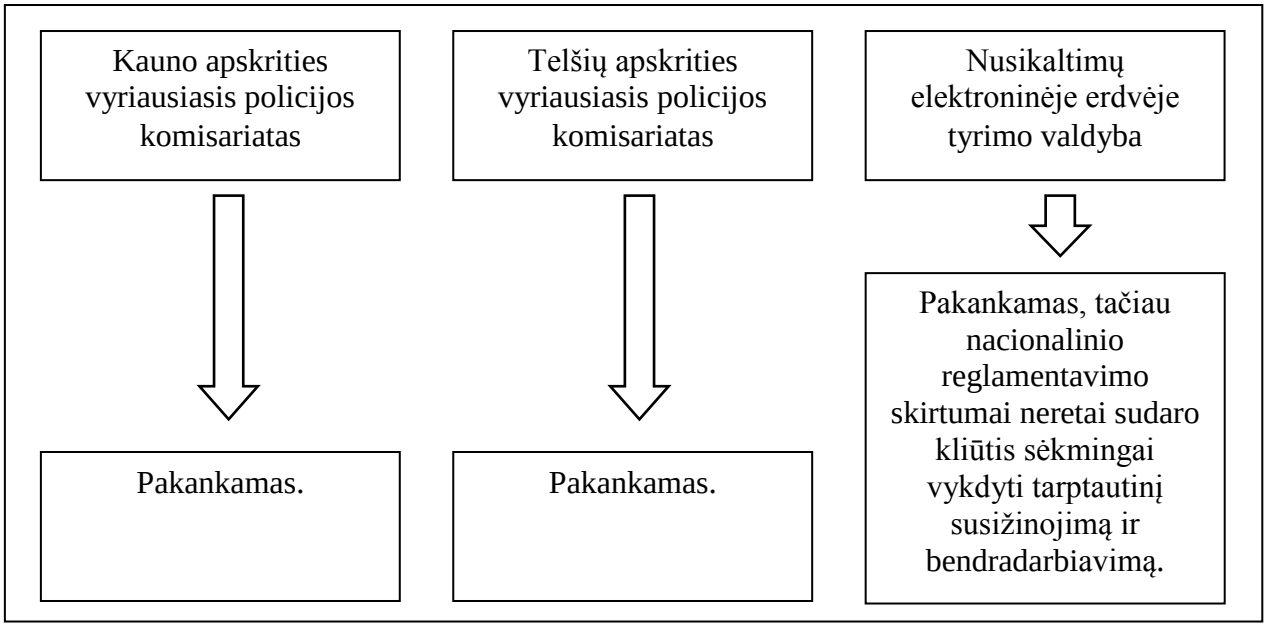
Apibendrinus gautus rezultatus, nusikaltimų elektroninėje erdvėje tyrimo srityje galima būtų įvardinti šiuos pagrindinius probleminius aspektus:

- Operatyvaus informacijos gavimo iš užsienio bendrovių, teikiančių elektroninių ryšių ar elektroninių duomenų prieglobos paslaugas apribojimai. Taip pat informacijos gavimą apsunkina skirtingose šalyse taikomi skirtingi elektroninių duomenų saugojimo terminai.
- Ilgas duomenų rinkimas ir tyrimas. Taip pat duomenų rinkimas iš šifruotų duomenų laikmenų ar laikmenų skirsnių, kuriems iššifruoti reikalinga specializuota techninė ir programinė įranga.
- Piktnaudžiavimas anonimiškumą internete užtikrinančiomis technologijomis. Siekdami paslėpti savo tapatybę, neteisėta veikla elektroninėje erdvėje užsiimantys asmenys naudojasi įvairiais įrankiais ir būdais.
- Baudžiamojo proceso už nusikaltimus elektroninėje erdvėje dalyvaujančių subjektų kompetencijos ir patirties užkardant, tiriant ir nagrinėjant elektroninių nusikaltimų bylas, trūkumas ar nebuvimas.

- Informacinių technologijų specialistų išlaikymas viešajame sektoriuje esant konkurencingai šių specialistų rinkai.

Europos policijos biuras (Europolas) 2014 metais pirmą kartą parengė Organizuoto nusikalstamumo internete grėsmių analizę (iOCTA).[110]

- Nusikaltimų elektroninėje erdvėje mastas ir poveikis;
- Užtikrinti ir analizuoti elektroninius duomenis šalyse, kur kilę elektroniniai išpuoliai, tačiau neveiksmingos teisinės priemonės šalyje;
- Kenkėjiškos programos tampa vis sudėtingesnės;
- „Darknetas“ tai programa siūlanti aukšto lygio anonimiškumo suteikimą, kuris paslepia internetines paslaugas, tokias kaip, pardavimai pavogtų prekių, ginklų, narkotikais, prekyba žmonėmis. Taip pat vis dažniau naudojasi vaikų seksualiniam išnaudojimui, kuriami tam forumus, taip pat pornografinės medžiagos platinimas ir panašiai.

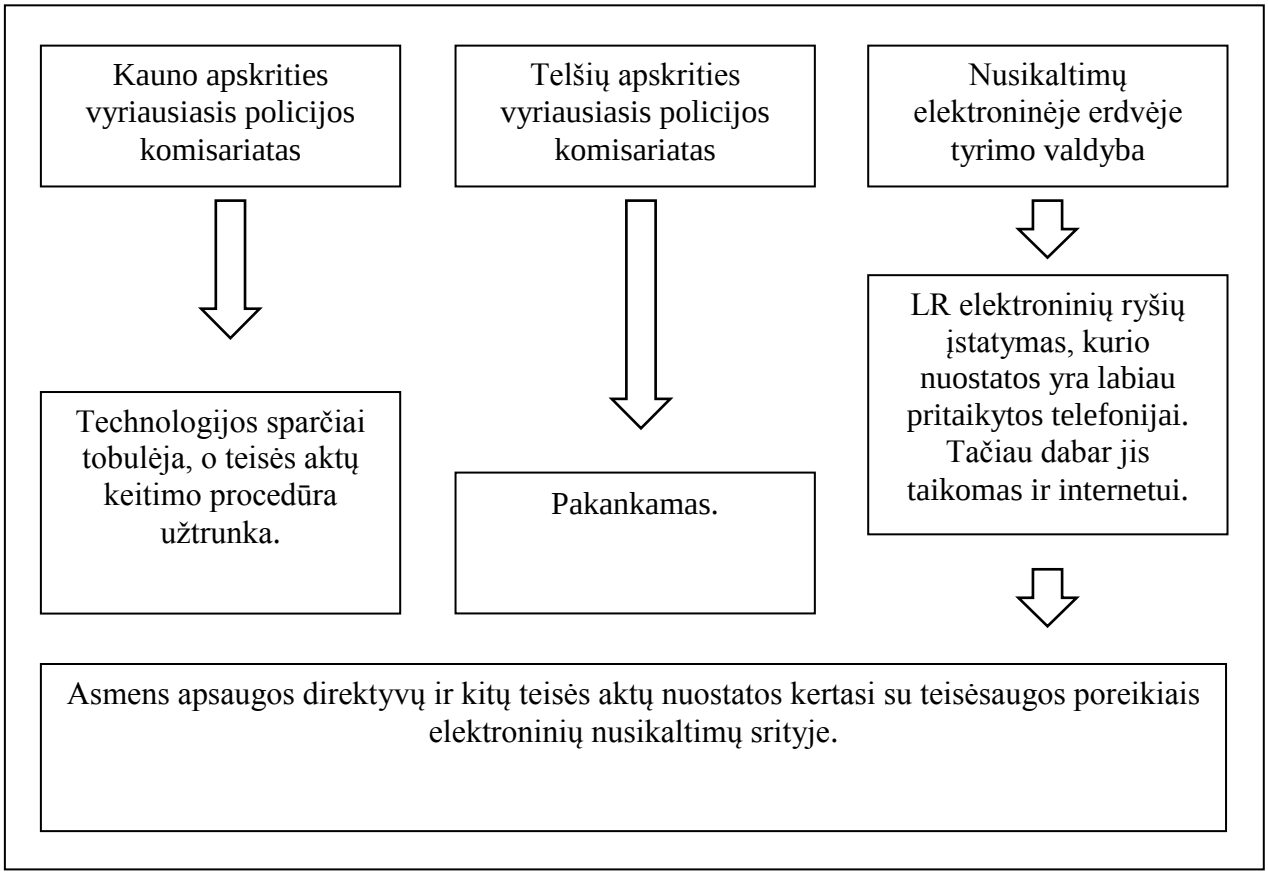


3.3. Lentelė. Nusikaltimų elektoninėje erdvėje tarptautinio bendradarbiavimo vertinimas.

Vertinant tarptautinį bendradarbiavimą, dėl nusikaltimų elektroninėje erdvėje, darytina išvada, kad šiuo metu Europos Sąjungos valstybių narių ir kitų šalių teisėsaugos ir baudžiamojo persekiojimo institucijoms yra sukurta pakankamai teisinių priemonių bei priimta pakankamai teisės aktų, suteikiančių galimybę bendradarbiauti tiriant nusikaltimus elektroninėje erdvėje, nustatančių tokio bendradarbiavimo teisinius pagrindus ir principus. Arčiau nacionalinio reglamentavimo

[110] Europol.https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta [žiūrėta 2015-04-15]

ypatumai ir skirtumai neretai sudaro kliūtis sėkmingai vykdyti tarptautinį susižinojimą ir bendradarbiavimą.

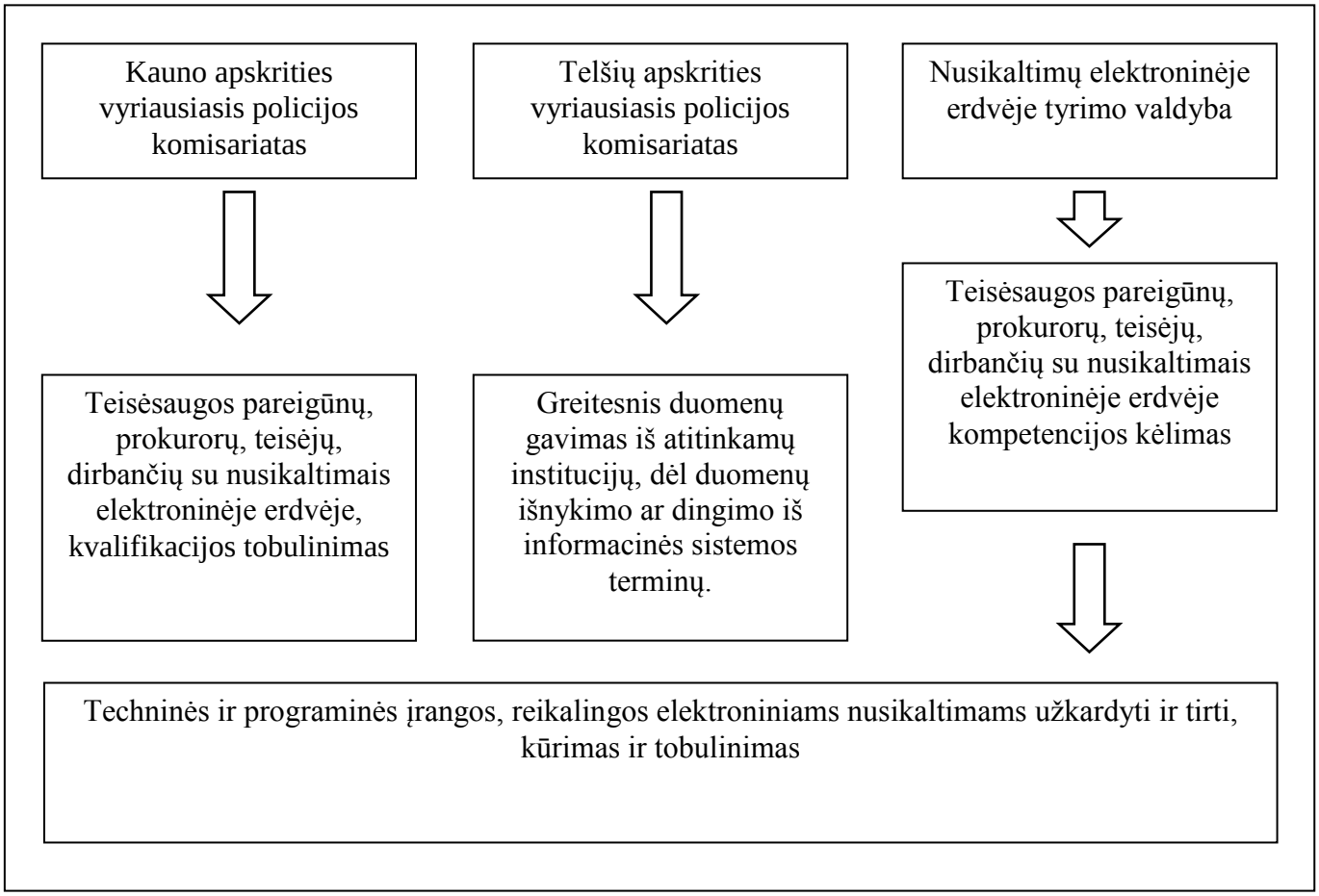


3.4 .Lnetelė. Nusikaltimų elektroninėje ardvėje reglamentavimo pakankamumo vertinimas.

Taip pat manytina, kad esamas teisinis reglamentavimas kovos su elektroniniais nusikaltimais srityje, iš esmės, neatitinka realijų.

- Technologijos sparčiai tobulėja, o teisės aktų keitimo procedūros užtrunka. Atsiranda naujos veikos (pavyzdžiui, tapatybės vagystė), kurias reikia kvalifikuoti pagal kelis LR BK straipsnius.
- Teisės aktai, reglamentuojantys nusikalstamų veikų elektroninėje erdvėje tyrimą (pavyzdžiui, Europos Tarybos konvencija dėl elektroninių nusikaltimų), buvo rengiami ir priimti prieš daugiau nei dešimtį metų.
- Taip pat paminėtinas ir LR elektroninių ryšių įstatymas, kurio nuostatos yra labiau pritaikytos telefonijai. Tačiau dabar jis taikomas internetui. Nuo to laiko pasikeitė daugelis su elektronine erdve susijusių sąvokų, iš esmės pasikeitė technologijos.
- Duomenys, anksčiau įvardinti kaip srauto duomenys, dabar jau yra laikomi turinio duomenimis ir pan.

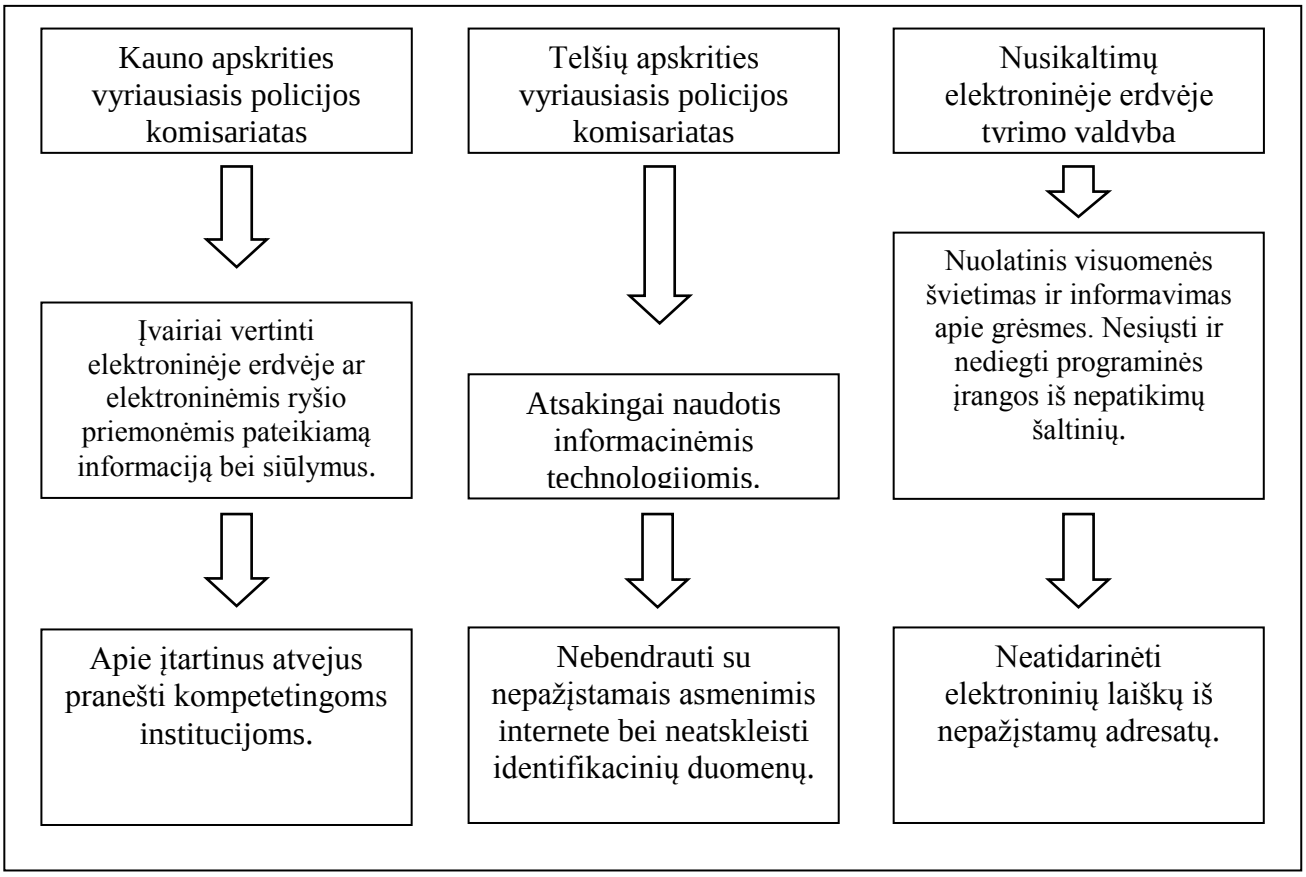
- Asmens duomenų apsaugos srities direktyvų ir kitų teisės aktų nuostatos kertasi su teisėsaugos poreikiais elektroninių nusikaltimų tyrimo srityje.



3.5. Lnetelė. Nusikaltimų elektroninėje erdvėje tyrimo tobulinimo kryptys

Nusikaltimų elektroninėje erdvėje tyrimo tobulinimo kryptis galėtų būti:

- Teisėsaugos pareigūnų, prokurorų, teisėjų, dirbančių su nusikaltimais elektroninėje erdvėje kompetencijos kėlimas, kvalifikacijos tobulinimas.
- Techninės ir programinės įrangos, reikalingos elektroniniams nusikaltimams užkardyti ir tirti, tobulinimas ir kūrimas, ypatingai duomenų šifravimo ir iššifravimo srityje.
- Svarstytinas akademinės bendruomenės pasitelkimas.
- Greitesnis duomenų gavimas iš atitinkamų institucijų, nes pasitaiko atvejų, kad asmenys apgauti ne visada iš karto kreipiasi į policiją, o tik praėjus kažkuriam laiko tarpui, todėl duomenys gali būti išnykę arba likęs mažas terminas iki jų išnykimo, tačiau kol gaunami atitinkami duomenys, nusikaltėlį identifikuojančių duomenų gavimo terminas praėjęs.



3.6. Lentelė. Nusikaltimų elektroninėje erdvėje tyrimo prevencijos priemonės ir saugumas

Pagrindinės prevencinės priemonės ir apsisaugojimo būdai.

- Viena pagrindinių prevencinių priemonių turėtų būti nuolatinis visuomenės ir tikslinių grupių (moksleivių ir mokytojų, studentų, pagyvenusių žmonių, finansinių įstaigų darbuotojų, sistemų administratorių, privataus sektoriaus, žiniasklaidos ir kt.) švietimas ir informavimas apie grėsmes elektroninėje erdvėje.
- Atsakingai naudotis informacinėmis technologijomis. Nuolat atnaujinti kompiuteriuose, telefonuose ir kituose įrenginiuose naudojamą programinę įrangą, ypatingai antivirusines programas ir ugniasienes.
- Rekomenduojama įtariai vertinti elektroninėje erdvėje ar elektroninėmis ryšio priemonėmis pateikiamą informaciją bei siūlymus. Kadangi elektroninėje erdvėje lengva suklastoti informaciją, veikti kitų asmenų vardu.
- Neatidarinėti elektroninių laiškų iš nepažįstamų adresatų, ypatingai jeigu jokių pasiūlymų ar žinučių nelaukiate.
- Nesisiųsti ir nediegti programinės įrangos iš įtartinų tinklalapių ar kitų šaltinių.
- Nebendrauti su nepažįstamais asmenimis internete ir juolab neatskleisti jiems savo asmens, finansinių, prisijungimo prie paskyrų ar kitų reikšmingų duomenų.

- Prekes bei paslaugas įsigyti iš tų interneto svetainių, kurios pateikia atsiskaitymo būdą ir grynaisiais pinigais. Nes internetinės svetainės atstovui jokio skirtumo, kaip asmuo atsiskaito svarbu, kad pirktų prekę. Be to, nepirkti iš fizinių asmenų, kurie pardavinėja įvairias prekes įvairiuose portaluose pigesne kaina nei rinkos.
- Neduoti savo kompiuterio interneto paslaugų tiekėjo gautų slaptažodžių, nes jais gali pasinaudoti kiti asmenys įdiegę savo atsiųstas programas.
- Apie įtartinus atvejus pranešti kompetentingoms institucijoms: policijai, interneto „karštajai linijai“ ir panašiai.

Apibendrint nusikaltimų elektroninėje erdvėje atlikto interviu tyrimo rezultatus, galima daryti išvadą, kad nusikaltimai elektroninėje erdvėje yra auganti problema. Vis daugiau nusikaltimų atliekami elektroninėje erdvėje ir nusikaltimų padarymo skaičius didėja. Nusikaltimų elektroninėje erdvėje tyrimo problemos, sudaro sunkumų tiriant nusikaltimus. Kad šių sunkumų sumažėtų, reikėtų valstybėms taikyti panašius elektroninių duomenų saugojimo terminus. Apribojimus mažinti, dėl operatyvaus informacijos gavimo iš užsienio bendrovių teikiančių elektroninių ryšių ar elektroninių duomenų priglobos paslaugas. Kompetencijos kėlimas subjektų tiriančių ir nagrinėjančių elektroninių nusikaltimų bylas. Taip pat valstybės glaudžiai bendradarbiaudamos turi, rengti teisės aktus, atsižvelgdamos į esamą padėtį, bei numatyti ateitį. Kadangi technologijos sparčiai tobulėja, o teisės aktų keitimo procedūra užtrunka.

IŠVADOS

1. Nusikaltimų elektroninėje erdvėje kriminalistinės charakteristikos struktūrą sudaro keturi elementai ir požymiai: tai nusikalstama veika ir jos padarymo būdas, subjektas įvykdęs nusikaltimus elektroninėje erdvėje, nusikaltimo pasikėsinimo dalykas ir nusikaltimo padarymo situacija.

- Nusikaltimų elektroninėje erdvėje padarymo būdas, tai neteisėti veiksmai, priemonės, įrankiai, kuriais naudojasi asmenys darantys nusikaltimą, kad apeitų sistemas, pasinaudoja spragomis, kuria virusus, pažeidžia asmeninę erdvę.
- Nusikaltimus elektroninėje erdvėje atlieka subjektai, kurie gerai išmano programavimą, turi gerus įgūdžius įsilaužti į kompiuterius, nulaužti ar apeiti saugos priemones, prisijungimo kodus, slaptažodžius. Subjektai gali būti tiek profesionalai, tiek mėgėjai, eiliniai naudotojai, organizuotos grupuotės, tiek įstaigos darbuotojai turintys galimybę prieiti prie informacinės sistemos.
- Apibendrindami pasikėsinimo dalyko sampratą, bei turinį, galime konstatuoti, kad nukentėjusysis tai fizinis ar juridinis asmuo, kuriam yra padaryta žala, fizinė, turtinė ar moralinė.
- Nusikaltimų elektroninėje erdvėje situacija:

1. Yra didelės elektroninių nusikaltimų atakos prieš informacines sistemas.
2. Vykdomos užkrėstų ir valdomų kompiuterių atakos.
3. Nusikalstamos veikos padaromos, panaudojant kompiuterio virusus su tikslu užkrėsti kompiuterius.

Šių keturių elementų ir požymių pagrindu gali būti sudaromos prielaidos pasirenkant kriminalistinius metodus, priemones ir būdus nusikaltimų išaiškinimui ir tyrimui.

2. Nusikaltimų elektroninėje erdvėje reglamentavimo būklė tokia, kad technologijos sparčiai tobulėja, elektroniniai nusikaltimai tampa vis sudėtingesni, o teisės aktų keitimo procedūra užtrunka. Teisės aktai, reglamentuojantys nusikalstamų veikų elektroninėje erdvėje tyrimą, pavyzdžiui, Lietuvos Respublikos elektroninių ryšių įstatymas, kurio nuostatos yra labiau pritaikytos telefonijai. Tačiau dabar jis taikomas internetui. Taip pat viena iš problemų, tai asmens duomenų apsaugos srities direktyvų ir kitų teisės aktų nuostatos kertasi su teisėsaugos poreikiais elektroninių nusikaltimų tyrimo srityje. Nusikaltimų elektroninėje erdvėje tyrimo reglamentavimo, pateikiamos svarbiausios tobulinimo kryptys:

- Valstybės turi labiau analizuoti nusikaltimų darymo, tyrimo praktiką.

- Suvienodinti teisinį reglamentavimą.

3. Nusikaltimai elektroninėje erdvėje yra auganti problema, į elektroninę erdvę persikelia net tradiciniais laikyti nusikaltimai. Tobulėja nusikaltimų elektroninėje erdvėje schemos, sudėtingėja šiuos nusikaltimus vykdančių asmenų nustatymas, tyrimas, mastas ir padaroma žala. Siekiant kovoti su elektroniniais nusikaltimais tarptautiniu ir nacionaliniu mastu, yra būtinas bendradarbiavimas, kad užtikrinti tyrimo harmonizavimą, ieškoti efektyvesnių tyrimo ir prevencijos būdų.

4. Galimos tokios nusikaltimų elektroninėje erdvėje tyrimo metodikos ir plėtros kryptys:

- Šių nusikaltimų baudžiamosios teisinės, procesinės, kriminalistinės ir kriminologinės charakteristikų parengimas.
- Nusikaltimų elektroninėje erdvėje tyrimo praktikos analizė.
- Teisėsaugos pareigūnų, prokurorų, teisėjų, dirbančių su nusikaltimais elektroninėje erdvėje kompetencijos kėlimas.
- Techninės ir programinės įrangos, reikalingos elektroniniams nusikaltimams užkardyti ir tirti, tobulinimas ir kūrimas, ypatingai duomenų šifravimo/iššifravimo srityje.

LITERATŪROS SĄRAŠAS

Knygos.

1. Broderic T. R. Regulation of the Information Technology in the European Union.// London, Kluver Law International, 2000.
2. Civilka M., Lamanauskas T., Osinaitė G., Sauliūnas D. ir kt. Informacinių technologijų teisė.// Vilnius, NVO Teisės Institutas, 2004.
3. Elektroniniai nusikaltimai. Metodinė priemonė./ Doc. dr. Darius Štitilis – Vilnius: Mykolo Romerio universitetas 2011.
4. Ghosh S, Turrini E. Cybercrimes: A Multidisciplinary Analysis.// Springer, 2010.
5. Higgins G.E. Cybercrime:An introduction to an Emerging Phenomen.// Library of Congress Cataloging, 2010.
6. Icove, D. *Computer Crime: a Crimefighter`s Handbook*. O'Reilly Media, 2005.
7. Jablokov, N., P. Kriminalistika [Criminalistics]. Moskva: Norma. 2009.
8. Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. Teisės informatika ir informatikos Teisė.// Vilnius, Mykolo Romerio Universitetas, 2006.
9. Kuconis, P. Nusikaltimų tyrimo metodikos raidos perspektyvos. 1993.
10. McConnell International.Cyber Crim and Punishment? Archaic Laws Threaten Global Information: Archaic Laws Threaten Global Information. December 2000.
11. Petrauskas, R.; Štitilis, D. Kompiuteriniai nusikaltimai ir jų prevencija. Vilnius: Lietuvos teisės akademija, 2000.
12. Susan W. Brenner, Cybercrime and the Law. 2012.
13. Schjolberg S. & Hubbard A.M. Harmonizing national legal approaches on cybercrime // WSIS thematic meeting on cybersecurity. Geneva, 28 June – 1 July. 2005.

Moksliniai straipsniai.

1. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace.// Library of Congress Cataloging, 2010.
2. Grabosky, P 2013, 'Organized Cybercrime and National Security', World Crime Forum, Korean Institute of Criminology, Korea, pp. 19 - 30.
3. Interpol. Cyber-crime. www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf
4. Kurapka, V. E., Malevski, H., Šiuolaikinė nusikaltimų tyrimo koncepcija ir jos kriminalistinis bei procesinis uţtikrinimas. Pirmieji rezultatai. Jurisprudencija, 2003. 43 (35): 81.
5. Kuklianskis, S., Matulienė, S., Kriminalistinės nusikaltimų tyrimo charakteristikos samprata. Jurisprundencija, 200. 29 (21).

6. Matulienė S. Kriminalistinė nusikaltimų charakteristika nusikaltimų tyrimo metodikoje: teorinių ir praktinių problemų šiuolaikinė interpretacija: daktaro disertacija. soc. mokslai: teisė(01S).- Vilnius, 2004.
7. WSIS Thematic Meeting on Cybersecurity. Geneva, June 28 - July 1, 2005. http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf
8. Sofaer A.D., Goodman S.E. Cyber Crime and Security The Transnational Dimension. http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf
9. Sieber U. Legal aspects of Computer-Related Crime in the Information Society. Comcrime study, prepared for European Commission, 1998. http://www.oas.org/juridico/english/COMCRIME%20Study.pdf
10. Štitilis, D.; Krikščiūnas, R.; Petrauskas, Kai kurie konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai. Jurisprudencija, 2005, 67(59).
Wilson C. Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 11. January 29, 2008. https://www.fas.org/sgp/crs/terror/RL32114.pdf

Teisės norminiai aktai.

1. Council of Europe Recommendation No. R(95) 13.
2. Commission of the European Communities COM (2000) 890.
3.Europos Komisijos komunikas KOM (2007) 267. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:PDF
4.Europos Parlamento ir Tarybos direktyva. 2013/40/ES http://eur-lex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:32013L0040&from=LT
5. 2002 m. lapkričio 7 d. Europos Tarybos nusikaltimų elektroninėje erdvėje konvencijos papildomas protokolas (2002)24. http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm
6. Jungtinių Tautų konvencija prieš tarptautinį organizuotą nusikalstamumą. Valstybės žinios. 2002-05-22, Nr. 51-1933. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=166679
7. Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace. file:///D:/My%20Documents/Downloads/1CybersecurityStrategyoftheEuropeanUnionAnOpenSafeandSecureCyberspace-JOIN20131final-722013%20(1).pdf
8. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36- 1188. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

9. Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną.
10. Lietuvos Respublikoje elektroninių ryšių įstatymas Valstybės žinios, 2004-04-30, Nr. 69-2382
11.Recommendations no. R (89)9 on Computer-related crime // http://cm.coe.int/ta/rec/1989/89r9.htm
12. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus įsakymas, dėl nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinio veiklos nuostatai. 2009 m. kovo 20 d. įsakymu Nr. 1V-348.
13. United Arab Emirates, The Federal Law No. (2) on 2006 on The prevention of information Technology. http://www.aecert.ae/Prevention_of_Information_Technology_Crimes_English.pdf

Teismų sprendimai.

1. Baudžiamoji byla LAT Nr. 2K-375/2012
2. Baudžiamoji byla LAT Nr. 2K-375/2012
3. Baudžiamoji byla Klaipėdos miesto apylinkės teismas Nr 1-740-93-2009
4. Baudžiamoji byla LAT 2K-29-2014
5. Baudžiamoji byla LAT 2K-93-489/2015
6. Baudžiamoji byla LAT 2K – 345/2014
7. Yahoo Inc V. La Ligue Contre Le Racisme et Antisemitizme. http://caselaw.findlaw.com/us-9th-circuit/1144098.html#sthash.jhpZB1Bv.dpf
8. Yahoo! v. LICRA Amicus Brief http://www.law.berkeley.edu/4647.htm
9.Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme. http://cyber.law.harvard.edu/is02/readings/yahoo-order.html
10. Tore TVEDT byla Norwegian jailed for Web racism http://edition.cnn.com/2002/WORLD/europe/04/23/norway.web/
11. United Nations, International Criminal Tribunal for Rwanda. http://69.94.11.53/
12. United Nations, International Criminal Tribunal for the Former. Yugoslavia. http://www.icty.org
13. People v. Somm, Case 8340 Ds 465 Js 173158/95 (Amstsgericht, Munchen, Bavaria).
14. Tore TVEDT byla Norwegian jailed for Web racism http://edition.cnn.com/2002/WORLD/europe/04/23/norway.web/

Interneto šaltiniai.

1. AOTD prie KAM 2015 m. veiklos ataskaita. file:///D:/My%20Documents/Downloads/aotd%202014%20viesoji%20ataskaita.pdf

2. AOTD prie KAM Gresmių Nacionaliniam saugumui vertinimas 2013m. file:///D:/My%20Documents/Downloads/aotd%202013%20gr%C4%97smi%C5%B3%20nacionaliniam%20saugumui%20vertinimas%20(ns)%20(1).pdf
3.Afrikos regiono darbo grupė. http://itlaw.wikia.com/wiki/African_Regional_Working_Party_on_Information_Technology_Crime
4. Biograpfhy of Stein Schjolberg. http://www.cybercrimelaw.net/biography.html
5. Cyber attacks: Removing reodblocks to invetigation and informatikon sharing.http://www.gpo.gov/fdsys/pkg/CHRG-106shrg69358/html/CHRG-106shrg69358.htm
6. Cybercrime infographics from april 2014. http://www.hacksurfer.com/posts/15-new-cybercrime-infographics-from-april-2014
7. Europolas patvirtino projektą kovai su kibernetiniais sukčiais. http://www.penki.lt/Sauga-saugos-sprendimai/Europolas-patvirtino-projekta-kovai-su-kibernetiniais-sukciautojais.im?id=349134&f=c
8. Europol.https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta
9. Hakeriai pavogė milijardą dolerių. http://topcom.lt/hakeriai-pavoge-milijarda-doleriu/
10. Hakeris. http://lt.wikipedia.org/wiki/Hakeris
11. Horizon 2020. http://ec.europa.eu/programmes/horizon2020/
12. History of the G8. http://www.g8.co.uk/history-of-the-g8/
13. Interviu S. Skverelis. http://www.delfi.lt/news/ringas/politics/s-skvernelis-nuo-kibernetiniu-ataku-apsiginklavome-bet-truksta-specialistu.d?id=67325526
14. Interpol. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
15. International cybercrime. http://en.wikipedia.org/wiki/International_cybercrime
16. International Crime and Intelligence Analysis Conference 2015.
17. Informatikos ir ryšių departamentas prie LR VRM veikla. http://www.ird.lt/veikla-2/
18. Kibernetinė ataka. http://www.15min.lt/mokslasit/straipsnis/verslas/programisiu-duona-ar-sunku-suorganizuoti-kibernetine-ataka-649-340567
19. KPMG tyrimas. http://www.kpmg.com/LT/lt/IssuesAndInsights/ArticlesPublications/Puslapiai/profiles_of_a_fraudster.aspx
20. Kibernetinio saugumo didinimas ES. http://www.consilium.europa.eu/lt/policies/cyber-security/
21. Lietuvos Respublikos seimo Europos informacijos biuras. http://www.eic.lrs.lt/index.php?18458626,
22. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, atakų šaltinio šalys. https://www.cert.lt/ataku_statistika.html

23. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys. https://www.cert.lt/tipai.html
24. Lietuvos kriminalinės policijos biuras. http://lkpb.policija.lt/index.php?option=com_content&view=category&layout=blog&id=56&Itemid=50
25. 2014 m. Lietuvos respublikos prokuratūros veiklos ataskaita. file:///D:/My%20Documents/Downloads/ataskaita-2014%20(1).pdf
26. Lietuvoje nuteistas komentatorius. http://www.technologijos.lt/n/technologijos/it/S-21755/straipsnis/Lietuvoje-nuteistas-dar-vienas-interneto-komentatorius?l=2&p=1
27. Norwegian jailed for Web racism. http://edition.cnn.com/2002/WORLD/europe/04/23/norway.web/
28. Siaučia vienu pavojingiausių virusų. http://www.delfi.lt/mokslas/technologijos/siaucia-pinigus-vagiantis-kompiuteriu-virusas-zala-skaiciuojama-milijardais.d?id=67667720
29. Susan W. Brenner. https://www.udayton.edu/directory/law/brenner_susan.php
30. 2014 m. Sociologinis visuomenės nuomonės tyrimas, dėl elektroninėje ir neelektroninėje erdvėje vykdomų asmens duomenų vagysčių bei pavogtų asmens duomenų panaudojimo nusikalstamais tikslais. file:///D:/My%20Documents/Downloads/apklausos%20analize_galutinis%20(1).pdf
31. Užsienio reikalų ministerijos 2015 metų veiklos prioritetai. https://www.urm.lt/default/lt/uzsienio-politika/naujienos-kalbos-publikacijos/uzsienio-reikalu-ministerijos-2015-metu-veiklos-prioritetai
32. Vaikų naudojimasis internetu. http://www.draugiskasinternetas.lt/repository/dokumentai/ataskaitos/2014/zero_to_eight_19aug.pdf
33. Vaikų pornografija. http://www.15min.lt/naujiena/aktualu/lietuva/britu-ekspertas-johnas-carras-vaiku-pornografijos-naudotojams-ir-platintojams-neuztektu-visu-pasaulio-kalejimu-56-388174
34. Vaikų seksualinis išnaudojimas. http://www.dhs.gov/news/2011/08/03/secretary-napolitano-and-attorney-general-holder-announce-largest-us-prosecution
35. WSIS Thematic Meeting on Cybersecurity. Geneva, June 28 - July 1, 2005. http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf
36. Žymiausi hakeriai. http://haxaz.awardspace.com/zymiausi_hakeriai.html

ANOTACIJA

Magistro baigiamojo darbo tema „Nusikaltimų elektroninėje erdvėje tyrimas: tarptautinė ir nacionalinė praktika“. Tai aktuali tema, kadangi šiuolaikinėje visuomenėje plačiai paplito informacinių technologijų naudojimas ne tik teisėtiems, bet ir neteisėtiems veiksmams daryti. Pirmoje dalyje atskleidžiama nusikaltimų elektroninėje erdvėje kriminalistinė charakteristika, tai nusikaltimo padarymo būdas, nusikaltimą padarę elektroninėje erdvėje asmenys, pasikėsinimo dalykas, situacija. Antroje dalyje atskleidžiama nusikaltimų elektroninėje erdvėje tarptautinis reglamentavimas ir bendradarbiavimas, tarptautinių organizacijų ir ES dokumentai dėl elektroninių nusikaltimų tyrimo, ir nusikaltimų elektroninėje erdvėje tyrimo reglamentavimas Lietuvoje. Trečioje dalyje atskleidžiama nusikaltimų elektroninėje erdvėje tyrimų tarptautinė ir nacionalinė praktika, nusikaltimų elektroninėje erdvėje prevencija ir problemos, pagrindinės nusikaltimų elektroninėje erdvėje tyrimo metodikos ir tobulinimo kryptys.

ANNOTATION

The topic of Master degree thesis “Cybercrime Investigation: International and National Practice”. It is a relevant topic, since the use of information technologies for both legal and illegal deeds is widely spread in the modern society. The first part reveals criminal characteristics of cybercrimes, which is the nature of a crime, persons that committed a crime in the cyberspace, subject of attempt, and the situation. The second part reveals international regulations and cooperation of cybercrimes, documents of international organizations and the EU, related to the cybercrime investigation, and regulation of cybercrime investigations in Lithuania. The third part reveals international and national practice regarding the cybercrime investigations, prevention and problems of cybercrimes, main methods of cybercrime investigations and trends for improvement.

SANTRAUKA

Magistro baigiamojo darbo tema „Nusikaltimų elektroninėje erdvėje tyrimas: tarptautinė ir nacionalinė praktika“. Tai aktuali tema, kadangi šiuolaikinėje visuomenėje plačiai paplito informacinių technologijų naudojimas ne tik teisėtiems, bet ir neteisėtiems veiksmams daryti. Darant vieną nusikaltimą, gali dalyvauti asmenys iš skirtingų šalių, nereikia fizinio kontakto, jie palaiko ryšį ir bendrauja internete, sudaro planą, pasiskirsto vaidmenimis, vienas kuria virusą, kitas nuima pinigus, kitas juos persiunčia ir tai vyksta pasauliniu mastu. Pirmojoje dalyje atskleidžiama nusikaltimų elektroninėje erdvėje kriminalistinė charakteristika. Kurioje pateikiami nusikaltimo padarymo būdai, praėjusiųjų metų statistika, apie elektroninių nusikaltimų incidentus. Pateikta užfiksuotų kibernetinių atakų iš šalių procentinė dalis nuo visų užfiksuotų atakų, bei išspręstų incidentų skaičius per savaitę. Atskleidžiami asmenys kurie padaro elektroninius nusikaltimus, pateikiami pavyzdžiai, bei atliktas tyrimas pasaulinio audito, mokesčių ir konsultacijų įmonių tinklo tyrimas, apie sukčiavimą bei piktnaudžiavimą. Atskleidžiama nusikaltimų elektroninėje erdvėje pasikėsinimo dalyką, pateikiamas naujausias atliktas „Eurobarometro“ tyrimas 2014 m., taip pat tarptautinis tyrimas „EU Kids Online“ 2013 m., bei 2014 metų sociologinis visuomenės nuomonės tyrimas. Ir atskleidžiama nusikaltimų elektroninėje erdvėje situacija. Pateikiama 2014 metų LR prokuratūros veiklos ataskaita, pateikiami pavyzdžiai.

Antrame skyriuje analizuojama, nusikaltimų elektroninėje erdvėje tyrimo tarptautinis reglamentavimas, bendradarbiavimas bei pateikiami pavyzdžiai. Analizuojami tarptautinių organizacijų ir ES dokumentai dėl elektroninių nusikaltimų tyrimo. Pateikiamos pagrindinės organizacijos, tai Jungtinės Tautos, Europos Taryba, Europos Sąjunga, Europos ekonominio bendradarbiavimo ir plėtros organizacija, Interpolas, didžiojo aštuoneto šalys. Taip pat pateikiamas nusikaltimų elektroninėje erdvėje tyrimo reglamentavimas Lietuvoje.

Trečiajame skyriuje atskleidžiama nusikaltimų tyrimas tarptautiniu ir nacionaliniu mastu. Nagrinėjama nusikaltimų elektroninėje erdvėje prevencija ir problemos. Pateikiami pasiūlymai ir įžvalgos dėl tyrimo metodikos plėtros krypčių.

SUMMARY

The topic of Master degree thesis "Cybercrime Investigation: International and National Practice". It is a relevant topic, since the use of information technologies for both legal and illegal deeds is widely spread in the modern society. One crime may involve persons from different countries, it does not require physical contact, since they communicate on the internet, establish a plan, divide the roles, one of them creates a virus, the other one takes money, another transfer the money, and it happens on a global scale. The first part reveals criminal characteristics of cybercrimes. It provides the nature of crimes, statistics of the last year, and incidents of cybercrimes. It presents a percentage of all reported cyberattacks from different countries and the number of resolved incidents per week. It reveals persons that commit cybercrimes and provides examples. It provides a research on fraud and abuse carried out by the network of global audit, tax, and advisory companies. It reveals the subject of attempted cybercrimes, research of 2014 carried out by "Eurobarometer", international research of 2013 by "EU Kids Online", and a social research of 2014 on society's opinion. It provides the report of 2014 on the activity of Lithuanian prosecutor's office and examples.

The second part reveals international regulations and cooperation of cybercrimes and provides examples. It analyses document of international organization and the EU regarding the cybercrime investigations. It provides the main organizations, such as the United Nations, the Council of Europe, the European Union, the European Economic Co-operation and Development Organization, Interpol, and the Group of Eight. Also, it provides the regulation of cybercrime investigations in Lithuania.

The third part reveals cybercrime investigations on the international and national level. It analyses prevention and problems of cybercrimes. It provides suggestions and insights on the development of investigative methods.

PRIEDAI

NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE TYRIMAS: TARPTAUTINĖ IR NACIONALINĖ PRAKTIKA

INTERVIU KLAUSIMAI
2015 m. balandžio d.

1. Kaip vertinate nusikaltimus elektroninėje erdvėje?

2. Kokios pagrindinės problemos kyla, dėl tyrimo nusikaltimų elektroninėje erdvėje?

3. Ar, Jūsų nuomone, tarptautinis bendradarbiavimas, dėl nusikaltimų elektroninėje erdvėje yra pakankamas? Jei ne, nurodykite ko trūksta.

4. Ar, Jūsų nuomone, yra pakankamas reglamentavimas nusikaltimų elektroninėje erdvėje? Jei ne, nurodykite ko trūksta.

5. Kokias nusikaltimų elektroninėje erdvėje tyrimo tobulinimo kryptis galėtumėte pasiūlyti?

6. Kokias nusikaltimų elektroninėje erdvėje prevencijos priemones galėtumėte pasiūlyti?

7. Kaip tinkamai apsisaugoti nuo nusikaltimų elektroninėje erdvėje?

Forma patvirtinta Mykolo Romerio universiteto
Senato 2012 m. lapkričio 20 d. nutarimu Nr.1SN-10

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2015 05 04
Vilnius

Aš, Mykolo Romerio universiteto Teisės fakulteto, teisės programos baudžiamosios teisės ir kriminologijos specializacijos.

(fakulteto / instituto, programos pavadinimas)

Studentas (-ė)_____Irena Stelmakovaitė _____
(vardas, pavardė)

patvirtinu, kad šis rašto darbas / bakalauro / magistro baigiamasis darbas

„_____“:

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už akademinės etikos pažeidimą.

Irena Stelmakovaitė
(vardas, pavardė)