MYKOLO ROMERIO UNIVERSITETO
TEISĖS FAKULTETO
BAUDŽIAMOSIOS TEISĖS KATEDRA

IRMANTAS VALUŽIS
Neakivaizdinio skyriaus Teisės ir valdymo studijų programos 965 gr. studentas

INFORMATIKOS BAUDŽIAMOJI TEISINĖ APSAUGA

Magistro baigiamasis darbas

Darbo vadovas -
doc. dr. Olegas Fedosiukas

Vilnius 2004

Turinys

Įvadas

Apibrėždamas pomodernią visuomenę, A.Augustinaitis, smagiai perfrazuodamas K.Markso postulatą, teigia: „Informacinėje visuomenėje „gamybinius santykius“ keičia „informaciniai santykiai“, kuriuos lemia būtent žinojimo ir žinijos procesų organizavimo būdas“[1].

Iš tiesų - šiandien informacija bei komunikacijos tampa visų veiklos sferų pamatu, o tai ir būtų galima įvardinti informacinės visuomenės prielaida.

Žinoma, informacija, kaip konkrečios veiklos, konkretaus sprendimo priėmimo intencija, visada buvo svarbi, tačiau niekada anksčiau ji nebuvo tokia gausi, taip plačiai taikoma ir, daugeliu atvejų, visuotinai prieinama (galimybės/potencijos, o ne aktualumo prasme). Niekada anksčiau informacijos gavimo kanalai ir formos nevaidino visuomenės narių individualizuojančio, struktūruojančio vaidmens. Greičiau priešingai - informacija vienydavo kolektyvizuodavo jos turėtojus.

Informacijos ir komunikacinių technologijų sklaida įprasmina galimybę kalbėti apie informaciją kaip apie bet kurios socialinės sferos suminį elementą, neatsiejamą dalį, tame tarpe ir neteisėtos arba nusikalstamos veikos, kaip vienos iš socialinių struktūrų, dedamąją. Juk akivaizdu, kad per visą žmonijos istoriją mokslo ir technikos laimėjimai naudojami ne tik pozityviems tikslams.

XX a. paskutiniajame dešimtmetyje daugelis išsivysčiusių valstybių (t.y. valstybių, kuriose informacinių-telekomunikacinių technologijų sklaida buvo sąlygiškai sparti) susidūrė su kompiuterinių technologijų panaudojimo nusikalstamiems tikslams pavojais. Lietuvos Respublikoje šie procesai sutapo su nepriklausomybės atstatymu, o tai reiškė, kad įstatymų leidėjas susidūrė ne tik su patirties stoka leisti savarankiškos valstybės įstatymus, bet ir su iš esmės kokybiškai pasikeitusia komunikacine aplinka. Kalbant apie baudžiamosios teisės normų kūrimą, įstatymų leidėjas susidūrė su naujomis nusikalstamomis veikomis, su naujomis "senųjų/tradicinių" nusikalstamų veikų raiškos formomis, su moderniųjų/pomoderno laikų teisiniais gėriais, kuriuos ir turėjo apsaugoti laikmečiui adaptuotos baudžiamosios teisės normos.

Informacinių technologijų vystymosi kontekste vis labiau atsiskleidžia nusikaltimų

---

[1] Augustinaitis A. *Informacinės visuomenės mokslo bruožai* // Sociologija. Mintis ir veiksmas, 1998/2.

informatikai problematikos aktualumas ir jos analizės svarba auga pagal geometrinės progresijos kreivę.

Kompiuteriniai tinklai ir elektroninė informacija vis dažniau naudojami įvairiausių nusikaltimų darymui, pradedant nesankcionuota prieiga ir baigiant pornografinio turinio informacijos, ypač susijusios su nepilnamečių asmenų vaizdavimu, platinimu. Nusikalstamų veikų įvairovė valstybes verčia vienytis kovoje su tokių nusikaltimų darymu. Šios nusikalstamos veikos ypatingos tuo, kad jos daromos visiškai naujoje ir vienai valstybei nepavaldžioje virtualioje - elektroninėje erdvėje.

Tik tarptautinės pastangos gali sukurti efektyvią elektroninių nusikaltimų užkardymo ir kovos su jais priemonių teisinio bendradarbiavimo schemą. Todėl neabejotina, kad Europos konvencijos dėl elektroninių nusikaltimų ratifikavimas buvo būtinas Lietuvos žingsnis prisidedant prie šio aktualaus tikslo įgyvendinimo.

Europos konvencija dėl elektroninių nusikaltimų kiekvieną ją pasirašiusią ir ratifikavusią valstybę įpareigoja savo nacionalinę teisę suderinti su konvencinėmis nuostatomis, kriminalizuojant visą eilę nusikalstamų veikų bei sutvarkant procesinių priemonių, skirtų konkrečių nusikalstamų veikų tyrimui, taikymą. LR BK XXX skyrius “Nusikaltimai informatikai” ir buvo sukonstruotas daugiau ar mažiau prisilaikant Konvencijoje dėl elektroninių nusikaltimų aprašytų nusikalstamų veikų modelio.

Magistro baigiamojo darbo objektas – nusikaltimų informatikai baudžiamosios teisinės apsaugos efektyvumo analizė.

Baigiamojo darbo tikslas – atskleisti Lietuvos Respublikoje už nusikaltimus kibernetinėje erdvėje atsakomybę numatančių baudžiamosios teisės normų dispozicijų trūkumus, trukdančius/galinčius trukdyti šias normas taikyti praktikoje.

Siekiant nurodyto tikslo keliami šie uždaviniai:

išanalizuoti pagrindines nusikaltimų virtualioje erdvėje atsiradimo priežastis,

įvertinti pagrindinius nusikaltimų informatikai bruožus ir požymius,

išanalizuoti Lietuvos Respublikos Baudžiamojo Kodekso (toliau LR BK) XXX skyriuje „Nusikaltimai informatikai“ išvardintų nusikaltimų sudėtis,

įvertinti nusikaltimų informatikai ikiteisminio tyrimo ir teismų praktikos formavimosi problemas, išprovokuoti akademines diskusijas apie šių baudžiamosios teisės normų tobulinimo galimybes.

Rašant magistro baigiamąjį darbą buvo naudotasi tarptautiniais ir nacionaliniais

norminiais teisės aktais, interneto resursais, buvo panaudota medžiaga iš šiuo metu tiriamų baudžiamųjų bylų. Formuluojant tam tikras koncepcijas ir išvadas, buvo pasinaudota lietuvių ir užsienio autorių moksliniais darbais. Lietuvoje nusikaltimų informatikai analizė dar nėra ta sritis, kuri patrauktų teisės mokslininkų ir teisininkų-praktikų dėmesį. Šiuo metu lietuvių kalba turime tik autorių kolektyvo (redaktorius T.Klimas) išleistą knygą „Šiuolaikinis nusikalstamumas“, kurioje šalia kitų pomoderno nusikalstamų veikų nagrinėjama ir nusikaltimų informatikai problematika (analizuojama Elektroninių nusikaltimų konvencija). Epizodiškai nusikaltimų kibernetinėje erdvėje problemas analizuoja L.Sodžiutė ir V.Sūdžius knygoje „Elektroninė komercija: prielaidos struktūra ir procesai“ bei autorių kolektyvas knygoje „Informacinių technologijų visuomenė: humanitarinės interpretacijos“. Reikia pripažinti, jog rusų autoriai gerokai anksčiau pradėjo domėtis nusikaltimų informatikai („kompiuterinių nusikaltimų“) analize. Taigi rašant šį rašto darbą, taip pat buvo panaudota literatūra rusų kalba.

Baigiamąjį darbą sudaro įvadas dvi pagrindinės dėstomosios dalys, išvados, santrauka ir bibliografijos sąrašas: pirmojoje dėstomojoje dalyje analizuojami sociokultūriniai pokyčiai betampančioje informacinėje visuomenėje, įvardijamos šių socialinių kaitos procesų apspręstos nusikalstamų veikų transformacijos; antrojoje - pateikiama nusikaltimus informatikai reglamentuojančių teisės normų analizė, praktiniai šių normų taikymo aspektai, formuluojami probleminiai klausimai.

Rašant baigiamąjį darbą, buvo naudoti šie tyrimo metodai: loginis-analitinis (tame tarpe teksto analizės), statistinės analizės, lyginamasis, indukcijos, dedukcijos.

Loginio-analitinio tyrimo metodo pagalba pabandyta analizuoti baudžiamosios teisės normas, numatančias atsakomybę už nusikaltimus elektroninėje erdvėje, pabandyta įžvelgti šių teisės normų dispozicijų trūkumus, pateikti pasiūlymus, kaip tuos trūkumus būtų galima pašalinti.

Pasinaudojus statistinės analizės metodu, pabandyta įvertinti baudžiamųjų įstatymų taikymo efektyvumą. Rašant baigiamąjį darbą, buvo panaudota empirinė medžiaga (šiuo metu Lietuvoje yra užregistruota 15 ikiteisminių tyrimų pagal LR BK XXX skyriaus straipsnius. Betarpiškai bendraujant su tyrėjais, kurių žinioje yra šios baudžiamosios bylos, buvo aiškinamasi, su kokiomis praktinėmis problemomis jie susiduria, tirdami nusikaltimus informatikos sferoje). Ši medžiaga, neatskleidžiant konkrečių baudžiamųjų bylų duomenų, buvo panaudota formuluojant tam tikras išvadas.

Lyginamojo tyrimo metodo pagalba siekta įžvelgti LR BK XXX skyriaus straipsnių

dispozicijų trūkumus/pranašumus, lyginant jas su tarptautinių dokumentų bei kitų šalių kodeksų atitinkamų straipsnių dispozicijomis.

Indukcijos metodo pagalba buvo bandoma ieškoti LR BK XXX skyriaus straipsnių dispozicijų bendrybių bei skirtumų, leidžiančių tam tikras straipsnių dalis apjungti, siekiant informatikos baudžiamosios teisinės apsaugos efektyvumo.

Dedukcijos metodo pagalba siekta įrodyti, jog teisės normų dispozicijose negali būti bendrybių ir nekonkretumo.

Įvertinęs mokslinėje literatūroje formuluojamos problemos aspektus bei prieinamus empirinius duomenis, magistriniame darbe iškeliu ir ginu tokią hipotezę: teisinių instrumentų taikymas nusikaltimų informatikai tyrimo sferoje yra labai problematiškas visų pirma dėl to, kad šių nusikaltimų dalykas yra nematerialus ir gali būti apčiuopiamas tik panaudojus aukštąsias technologijas. Turint omenyje, jog Lietuvos Respublikos Baudžiamojo Kodekso XXX skyriaus kai kurių straipsnių dispozicijos yra sukonstruotos vadovaujantis tik teisės teorijos principais, kartais ignoruojant kompiuteriuose ir kompiuteriniuose tinkluose vykstančius techninius procesus, darytina prielaida, jog šių teisės normų taikymas negali užtikrinti ikiteisminio tyrimo sėkmės.

1. Informacinės visuomenės tapsmas ir nusikalstamų veikų transformacijų

sąveikos.

1.1. Informacinės visuomenės, informacijos, komunikacijų samprata

Šiandien informacija, kurios vaidmuo bei įtaka vis stiprėja, traktuojama ne tik kaip naujienos/žinios apie įvykius pasaulyje, pranešamos masinės informacijos priemonių pagalba, bet ir kaip komunikacinė struktūra, apimanti žinių kūrimo, sisteminimo, saugojimo, perdavimo, interpretavimo sandus. Informacija šia plačiąja prasme tapo vienu iš bet kokios veiklos ir netgi apskritai žmogiškosios egzistencijos esminių komponentų, esančių šalia materialinių bei energetinių resursų. Kadangi informacinis resursas (išteklius) padeda taupyti daugelį kitų visuomenės resursų, tolimesnis visuomenės progresas didžia dalimi priklauso nuo informacinės infrastruktūros tobulėjimo, nuo informacinių produktų formavimo, saugojimo, platinimo bei naudojimo efektyvumo. Kita vertus, sociumo vystymasis naujojoje nuolat tobulėjančioje komunikacinėje erdvėje yra tiesiogiai proporcingas informacinio resurso apsaugos nuo neteisėto naudojimosi juo efektyvumui. Šioje vietoje iškyla teisės ir komunikacijų sąveikos vaidmuo sociumo vystymosi procesams. Teisės vaidmuo reiškiasi tada, kai techninės informacijos apsaugos priemonės nebegali užtikrinti šio socialinio resurso saugos nuo nesankcionuoto poveikio.

Kai informacinė aplinka vertinama kaip informacijos kūrimo, sisteminimo, saugojimo, pertvarkymo, o taip pat perdavimo priemonė/erdvė, ji suvokiama kaip technikos objektas, tarnaujantis tam tikriems žmogiškosios veiklos tikslams.

Per daug neperdedant, galima teigti, jog pati civilizacija formuojasi informacijos bei žinių saugojimo ir perdavimo pagrindu. Raštas (praeities ir ateities ryšys) kaip pirmoji erdviškai nuo subjekto atskirta gamtinio ir socialinio pasaulio modeliavimo forma sukuria visuomenę kaip civilizaciją, t.y. suteikia galimybę operuoti socialine semantine informacija, išvengiant tiesioginio kontakto tarp pranešėjo ir gavėjo. Kalbant apie kitas – modernesnes - informacijos saugojimo ir perdavimo formas, šis teiginys tampa dar prasmingesnis. Taigi, augant komunikacijų svarbai visuomenės vystymuisi, kaip jau buvo minėta, vis aktualesnis tampa ir šio informacinio resurso apsaugos klausimas (pradedant grynai technine apsauga, baigiant teisine ir netgi baudžiamąja-teisine apsauga).

Bet kuri tikslinė sistema visų pirma yra charakterizuojama mainų sistemos efektyvumą tarp jos elementų užtikrinančiomis kvalifikacijomis (materialiniai, energetiniai, informaciniai mainai). Šių elementų svarba kinta istorijos bėgyje. Pagal *informacinės visuomenės* šalininkų

schemą, ekonomikos dalinimas į tris sektorius – pirminį (žemės ūkio), antrinį (pramonės) ir tretinį (paslaugų sferą) – sutampa su socialinio-ekonominio visuomenės išsivystymo atitinkamomis fazėmis. Jeigu industrinei fazei būdingas antrinio, poindustrinei – tretinio sektoriaus dominavimas, tai "informacinėje visuomenėje" svarbiausią vaidmenį įgis informacinis sektorius: "[…] Informacija, o ne darbas ir kapitalas tampa esminiu gamybos faktoriumi. […] Žinios ir jų naudojimas pakeičia darbo jėgą nacionalinėse valstybėse, kaip pridėtinės vertės šaltinį. Šia prasme, informacija ir žinojimas yra esminiai "poindustrinės visuomenės" kintamieji"[2].

Ekonominės ir socialinės kapitalo funkcijos pereina ir informacijai. Ne tik nuosavybė, bet ir žinių lygis tampa socialinę diferenciaciją apsprendžiančiu faktu. Neinformuotieji (žmonės, kurių informuotumo lygis žemas) – tai individai, pamažu tampantys "užribio klasės" atstovais - naujaisiais skurdžiais.

Taigi esminiu informacinės visuomenės elementu turėtų tapti informacijos gamyba bei naudojimas ir tai savo reikšme ir svoriu turėtų persverti materialinę produkciją, energetikos išteklius ir neinformacinio pobūdžio paslaugas.

Vis tik, nepaisant šio užsibrėžto idealo, tenka pripažinti, jog bent jau šiandieninės visuomenės ir toliau yra organizuojamos gamybos bei kapitalo kaupimo, o ne technologiniu-informaciniu pagrindu. Technologijos bei informacijos rolė yra antrinė ir determinuota ekonominių faktorių. Technokapitalizmu ir būtų galima įvardinti kapitalo bei technologijos sintezę, kurioje esminė rolė vis tik tenka kapitalui (informacija bei informacinės technologijos yra tik būtinas kapitalo augimo faktorius). Sutinku, kad informacijos rolė auga ir turbūt augs ateityje. Tačiau ji neatlieka ir neatliks autonominio vaidmens visuomenės vystymosi procese. Informacija visada liks priemone, siekiant kitų – pirminių tikslų. Kartu reikia pabrėžti, kad šie tikslai ne visada bus lojalūs egzistuojančiai teisinei sistemai ir tvarkai.

Informacija – tai valdomas resursas (priemonė), padedantis valdyti kitus – materialinius-energetinius resursus, kuriuos ir galima įvardinti visuomenės egzistavimo baze. Taigi tik nuo subjekto priklauso informacijos/žinių panaudojimo kryptingumas, tik veikiantysis subjektas gali nuspręsti informacinį resursą panaudoti priešingais teisei arba sociumo narių teisėtus interesus atitinkančiais tikslais.

---

[2] Современный капитализм: критический анализ буржуазных политологических концепций / К.С.Гаджиев, А.К.Гливакщвский, Г.В.Каменская и др.-Москва, 1988, ст. 140.

Apibūdinant informacinę visuomenę, paprastai yra taikomi maksimalistiniai reikalavimai, nes tai kol kas yra tik idealus projektas.

Vienu iš visuomenės perėjimo iš poindustrinės į informacinę vystymosi stadiją kriterijų yra gyventojų, užimtų informacinių paslaugų sferoje, procentas (užimtumas informacijos gamybos, apdorojimo ir perdavimo sferoje vis auga).

Prisilaikant tradicijos, kuri susiformavo industrinės, poindustrinės visuomenės vystymosi fazių analizėje, teigiama, jog, jeigu daugiau nei 50 % visuomenės narių yra užimti informacinių paslaugų sferoje, visuomenė laikytina informacine.

"Visuomenė yra informacinė, jeigu :

bet kuris individas, asmenų grupė, įstaiga ar organizacija bet kuriame šalies taške ir bet kuriuo laiku nemokamai ar už atlygį gali gauti bet kokią savo veiklai, asmeninės bei socialinės reikšmės sprendimams būtiną informaciją ir žinias;

bet kuriam visuomenės individui ar jų grupei yra prieinama šiuolaikinės informacinės technologijos;

vyksta visų šakų gamybos ir valdymo automatizacija ir robotizacija;

vyksta radikalūs socialinių struktūrų pokyčiai, kurių pasėkoje plečiasi informacinės veiklos ir paslaugų sfera"[3].

Šia prasme teisė, kaip viena iš socialinių struktūrų, taip pat turi keistis - atitikti nūdienos reikalavimus, adaptuotis ir duoti atkirtį moderniems teisės pažeidėjų iššūkiams.

Tačiau, kad šis idealistinis projektas pradėtų funkcionuoti, būtinos ne tik išvardintos galimybės individo ar grupės raiškai. Būtinas ne tik priėjimas prie informacinių technologijų bei informacinis atvirumas, bet ir adekvati tikrovei informacija apie visas socialines sferas bei adekvatus informacijos suvokimas iš individo pusės.

Plačiąja prasme informacija yra žinia, siunčiama informacijos kanalais. Komunikaciniame procese egzistuoja žinojimo, žinios sukūrimo ir jos, kaip informacijos, pasiuntimo komunikaciniu kanalu sampratos[4].

Žinojimas – tai visų pirma intelektualinis resursas. Intelektualiniu-informaciniu resursu jis tampa tik komunikacijos procese. Informacija savyje visada talpina žinių perdavimo informaciniais kanalais "transportinį" elementą, tuo tarpu, žinios visada yra

[3] Ракитов А.И. Философия компъютерной революции. – Москва, 1991, ст 32-33.

[4] Fiske J. Įvadas į komunikacijos studijas.-Vilnius, 1998.

susietos su asmenybe – jų kūrėju.

Žinios/žinojimas – tai individo pažintinės veiklos, kurios pagalba įgyjama samprata apie tikrovę, rezultatas. Jų pristatymas – tai procesas, kurio tikslas yra "įpakuoti" tam tikrą žinių apimtį, kad ši galėtų pradėti judėti informacinio pasikeitimo kanalais arba būti saugoma (knyga, audio-video pranešimas, kompiuterinė informacija). Būtent žinojimas, pateiktas bei išsaugotas kaip informacija ir tampa nusikaltimo dalyku, nes, kaip jau minėta, žinojimas, pateiktas tokia forma, kad galėtų būti perduodamas informaciniais kanalais (arba informacija) tampa svarbiausiu socialiniu resursu.

Tačiau kiekybinės informacijos pagrindu visuomenė niekada netaps labiau informuota (informacinės trombozės reiškinys - techninių priemonių pagalba įmanoma skleisti didesnį informacijos kiekį, nei visuomenė yra pajėgi priimti). Taigi technologijų vystymosi pasėkoje, visuomenė tampa įgali atlikti tik daugiau komunikacijų, bet tai nesuponuoja jos galimybių priimti daugiau informacijos (šio gebėjimo augimas yra baigtinis). Tai reiškia, jog perspektyvoje individai gali tapti kompetentingesni savo domėjimosi bei raiškos sferose. Tačiau tai visiškai nereiškia, jog jų kompetencija bei informuotumas išaugs totaliai, t.y. visose gyvenimo sferose. Informacinės/komunikacinės technologijos skverbiasi į visas būties sferas, ko pasėkoje vis sudėtingiau tampa apsaugoti socialinių santykių dalyvių teisėtus interesus tose tikrovės srityse, kuriose jų (kiekvieno atskirai) žinojimas yra silpniausias. Būtent todėl informacijų technologijų vystymosi kontekste vis didesnis pavojus kyla dėl galimo nusikalstamo technologinio progreso panaudojimo.

1.2. Socialinių struktūrų (tame tarpe teisinių santykių kibernetinėje erdvėje)

kismas informacinėje visuomenėje

Reikia pripažinti, jog kartais reikalavimai visuomenei, kurią būtų galima vadinti informacine, yra absoliučiai minimalizuojami. Teigiama, jog Interneto vystimasis – tai lemiamas žingsnis kelyje į informacinę visuomenę. Tai yra pripažįstama, jog visuomenės informuotumo ir intelektualinio potencialo augimas, būtinas kvalifikuotai veiklai, priklauso būtent nuo internetinės informacijos sklaidos. Tačiau galbūt internetas mus atitolina nuo informacinės visuomenės? Internete labai mažai kas belikę iš tradicinės informacijos (arba žinojimo, kuris komunikacijos pasėkoje tampa informacija) ir beveik nieko iš tradicinės visuomenės[5]. Taigi mūsų epochos svarbiausiu fenomenu tapo Internetas. Tačiau būtent ši virtuali erdvė atvėrė naujas galimybes ir nusikaltėliams.

Nors pats internetas atsirado ganėtinai nesenai, jis jau vaidina nemažą reikšmę socialiniame gyvenime. Internetu naudojasi beveik du šimtai milijonų pasaulio gyventojų ir jų skaičius nuolat auga. Internetas ir kompiuteriniai komunikacijos ryšiai sukūrė naują socialinę terpę, kurioje vyksta nuolatinis bendravimas tarp individų. Tokiu būdu šioje terpėje formuojasi ne tik įvairios virtualios bendruomenės, virtualūs miestai bet ir kiti realiam socialiniam gyvenimui būdingi atributai – įvairios laisvalaikio praleidimo, edukacijos formos ir kita. Vienas iš tokių atributų yra nusikaltimai elektroninėje erdvėje.

Pačios nusikaltimo priemonės, tokios kaip kompiuteris, mobilios ryšio priemonės, organizacinė technika (skaneriai, lazeriniai spausdintuvai, kopijavimo aparatai) šiuo metu yra lengvai prieinamos kone kiekvienam individui. Netgi žinojimas, kuris reikalingas atlikti nusikaltimus informacinių technologijų pagalba yra lengvai pasiekiamas. Interneto svetainėse apstu pradedantiesiems įstatymų pažeidėjams detalizuotos medžiagos, kurioje išsamiai išdėstyti algoritmai, kurių procese pralaužiami programų, svetainių ar asmeninių skaitmeninių dokumentų kodai. Interneto tinklapiuose galima surasti organizacijas, kurių narius jungia vienas bendras interesas - sugebėjimas įveikti elektronines apsaugos priemones.

Nusikaltimai kurie yra atliekami naudojant informacines technologijas, tokias kaip mobilios ryšio priemonės, nešiojami bei stacionarūs kompiuteriai, profesionali organizacinė technika, nereikalauja didelių laiko ir erdvės sąnaudų. Sudėtingus nusikaltimus gali atlikti net vienas asmuo.

---

[5] Пугачев В.П. Информационная властъ и демократия // Общественные науки и современостъ, 1999/4.

Elektroninės erdvės apsaugojimas tampa nuolatiniu procesu, pagrįstu sunkiai įgyvendinamu principu: saugumo technologijos turi tobulėti greičiau nei grėsmes keliančios technologijos.

Analizuojant Interneto ir informacinės visuomenės santykį, būtina akcentuoti, jog Internetas – tai visų pirma egzistavimo ne visuomenėje priemonė ir aplinka, jeigu visuomenę suprastume kaip socialinių institutų sistemą. Visuomenė, kaip normatyvinė struktūra neveikia komunikacijos per Internetą procese. Dar daugiau – Internetas yra virtualių bendruomenių, alternatyvių realiai visuomenei, vystimosi aplinka (virtualiųjų "aš" bendravimas, nuasmeninimas, identifikacijos išplovimas). Internetas keičia sociokultūrinį bei istorinį fenomeną – asmenybę. Komunikacijos Internetu metu vyrauja beasmeniškumas, savęs "sukonstravimo" galimybė (tai virtualių įvaizdžių bendravimas), kas dažnu atveju kalbant apie nusikaltimus, "išplauna" veikos ir atsakomybės santykį.

Jeigu visuomenės virtualizaciją mes pripažįstame esmine šiandienos vystimosi tendencija, tampa aišku, kodėl taip audringai plečiasi Internetas, išlaisvinantis komunikaciją nuo socialinių institutų kontrolės. Čia ir kyla konfliktas: socialiniai institutai nebepajėgūs kontroliuoti kibernetinės tikrovės bei esančiųjų joje (*hacker*`ių fenomenas). Šiame kontekste kalbant apie teisę, kaip apie vieną iš socialinių institutų/struktūrų, atliekančių sociume saugiklio bei padarinių šalintojo vaidmenį, būtina akcentuoti, kad neatsitiktinai bet kurioje išsivysčiusioje valstybėje kuriamos naujos teisės normos, modifikuojamos senosios, stengiantis teisę, kaip institutą adaptuoti prie kintančių sąlygų. Socialinio kismo kontekste, teisės normų kaita turėtų bent vienu žingsniu lenkti kitų socialinių struktūrų kismą. Deja, dažnu atveju, teisės normos kuriamos tik kaip priemonės sociumo kismo iššauktiems padariniams šalinti. Teisė formuojasi šimtmečiais. Teisės paskirtis užtikrinti visuomenės stabilumą ir tolygų vystimąsi. Teisė - viena konservatyviausių socialinių struktūrų, ir, deja, ši jos savybė stabdo galimybes "pavyti" informacinių technologijų proveržio pasėkoje sparčiai kintančius visuomeninius santykius bei absorbuoti naujus iššūkius tradiciniams socialiniams santykiams[6].

Internete komunikacijos srautai, nešantys įvaizdžius (virtualius kūnus, asmenybes, bendruomenes) neįsikomponuoja į visuomenę, į visuomenėje nusistovėjusias socialines struktūras bet ir nepertvarko jų – jie jas ignoruoja, simuliuoja, išnaudoja trūkumus.

---

[6] Informacinių technologijų visuomenė: humanitarinės interpretacijos – monografija. V.: Lietuvos teisės universiteto leidybos centras, 2002 m., p. 77.

Internetas negali realizuoti informacinės visuomenės, kuri būtų suprantama labiau tradiciškai, idėją. Tačiau galbūt informacinė visuomenė ir yra virtualios realybės erdvė, be suverenių valstybių sienų, be socialinių struktūrų kontrolės?

Neatsitiktinai atskiros nusikaltimų rūšys (kurias sąlygiškai būtų galima pavadinti "pomoderno laikų nusikaltimais") reiškiasi būtent virtualioje erdvėje, ir net "tradiciniai" nusikaltimai įgauna virtualias raiškos formas.

Komunikacinių technologijų vaidmens iškilimo sociume kontekste, ypatingą reikšmę įgyja priemonės (techninės, teisinės, kultūrinės, edukacinės ir kt.), padedančios apsaugoti komunikacijas plačiąja prasme nuo neteisėto naudojimosi jomis.

Taigi, elektroninės skaičiavimo technikos sukūrimas, jos platus pritaikymas ekonominėje, socialinėje ir valdymo sferose, personalinių kompiuterių vartotojų rato išsiplėtimas yra ne tik techninį visuomenės progresą liudijantys faktoriai, bet ir negatyvias nusikaltėlių pasaulio vystymosi bei tobulėjimo tendencijas apsprendžiantys socialiniai fenomenai, sąlygojantys naujų nusikalstamų veikų formų ir būdų radimąsi. Organizuotos nusikaltėlių grupės ir pavieniai nusikaltėliai savo veikloje vis aktyviau pradeda naudoti naujausius mokslo ir technikos pažangos pasiekimus. Neteisėtų siekių vedini, nusikaltėliai vis dažniau savo veikoje naudojasi savo veiksmų planavimo sistemine prieiga, kuria konspiracijos ir slapto ryšio sistemas, naudoja modernias technologijas ir specialiąją techniką, o tame tarpe ir įvairiausius kompiuterinius įrenginius bei informacijos apdorojimo technologijas.

Pasaulinė praktika liudija, kad žala, padaroma nusikaltimais informatikai, vertintina sumomis, viršijančiomis kai kurių valstybių metinius biudžetus. Europos ir Amerikos žemynų valstybėse iš nusikaltimų informatikai gaunamas nelegalus pelnas, lygintinas su pelnu, gaunamu iš narkotikų biznio, prostitucijos, prekybos ginklais[7].

Kalbant apie mūsų šalį, pavojų liudija tas faktas, kad Lietuvos Respublikoje taip pat atsiranda naujos nusikalstamos veikos rūšys, kurios anksčiau nebuvo žinomos nei teisės mokslui, nei praktikai. Tai nusikalstamos veikos, susijusios su kompiuterinės technikos bei informacijos apdorojimo technologijų naudojimu arba nusikaltimai kibernetinėje erdvėje.

Dar visai neseniai įstatymų leidėjas baudžiamosios teisės normomis apskritai

---

[7] Уголовное право. Особенная часть. Учебник. Под ред. д.ю.н. проф. А.С. Михлина, М.: Юриспруденция, 2000. – с. 289

nereglamentavo tos socialinės tikrovės, kurią šiandien vadiname nusikaltimais informatikai – tai apsprendė bendra kriminogenine situacija Lietuvoje, kompiuterinių technologijų menkesnis panaudojimas, o taip pat informacinės sferos specifika, reikalaujanti specialiųjų žinių (kita vertus, kol nebuvo garsiai kalbama apie pavojus kompiuterinei informacijai, "nebuvo ir problemos"). "Problemos nematymo" fone nusikaltimų informatikai pavojus tik dar labiau išauga – ypatingai tai pasakytina apie nusikaltimus informatikai tokiose visuotinai svarbiose sferose kaip socialinė sauga, transporto sistema, valstybės gynybos sistema, atominės energetikos sistema ir daugelis kitų. Tai liudija ne apie hipotetinį, bet apie realų nusikaltimais informatikai keliamą pavojų sociumui.

2. Informatikos baudžiamoji teisinė apsauga.

2.1. Santykių informatikos srityje teisinis reguliavimas Lietuvos Respublikoje.

Aštuntajame dešimtmetyje didelė kompiuterinių sistemų atmintis bei greitas priėjimas prie duomenų per kompiuterių tinklus sukėlė realų pavojų žmogaus privatumui. Todėl daugelyje

Vakarų Europos šalių palaipsniui buvo priimti įstatymai dėl asmens duomenų apsaugos (žemiau pateikta lentelė paimta iš knygos Informacinių technologijų visuomenė: humanitarinės interpretacijos – monografija. V.: Lietuvos teisės universiteto leidybos centras, 2002 m., p. 124-125).

Šalis	Įstatymo pavadinimas	Įsigaliojimas
Austrija	Duomenų apsaugos aktas	1978
Danija	Danijos privačių registrų aktas; Danijos viešųjų registrų aktas	1978
Norvegija	Asmens duomenų registrų aktas	1978
Liuksemburgas	Asmens duomenų panaudojimo aktas apdorojant kompiuteriu	1979
Didžioji Britanija	Duomenų apsaugos aktas	1984
Suomija	Asmens duomenų failų aktas	1987
Airija	Duomenų apsaugos aktas	1988
Olandija	Duomenų apsaugos aktas	1988
Šveicarija	Federalinis duomenų apsaugos aktas	1988
Slovėnija	Duomenų apsaugos aktas	1989
Švedija	Duomenų aktas	1989
Islandija	Asmens įrašų apsaugos aktas	1989
Vokietija	Duomenų apdorojimo ir duomenų apsaugos aktas	1990
Portugalija	Asmens duomenų apsaugos aktas	1991
Belgija	Duomenų apsaugos aktas	1993

Tačiau informatikos baudžiamąja teisine apsauga susidomėta ne iš karto. "Europos Taryba, turbūt net aplenkdama laiką, 1989 m. valstybių narių įstatymų leidėjams patvirtino gaires materialinės baudžiamosios teisės kompiuterinių nusikaltimų srityje harmonizavimui"[8].

Prancūzijos Respublikos Baudžiamajame Kodekse tik 1992 m. pirmą kartą buvo papildytas skyrius dėl nusikaltimų nuosavybei atskira dalimi „Nusikalstamos veikos prieš automatizuotas duomenų apdorojimo sistemas", kurioje numatoma baudžiamoji atsakomybė

[8] Šiuolaikinis nusikalstamumas / Autorių kolektyvas. Redaktorius Tadas Klimas – Kaunas: VDU l-kla, 2002 m., p 28.

už neteisėtą priėjimą prie visos ar dalies automatizuoto duomenų apdorojimo sistemos, už tokios sistemos darbo trikdymą ar sistemos darbo tvarkos pažeidimą, arba įvedimą į tokią sistemą melagingos informacijos, arba duomenų bazės sunaikinimą arba jos pakeitimą. Kriminogeninės situacijos pokyčių priverstos ir kitos technologiškai išsivysčiusios valstybės priiminėjo analogiškas baudžiamųjų įstatymų pataisas.

Ilgainiui tapo aišku, jog kova su nusikaltimais kibernetinėje erdvėje išeina už suverenios valstybės jurisdikcijos ribų. Europos Taryba 2001 m. lapkričio 23 d. Budapešte priėmė specialią konvenciją, kuri skirta nusikaltimų kompiuterinės informacijos srityje problemai. Prie šios konvencijos gali prisijungti nebūtinai Europos žemyno valstybės.

Lietuvoje įstatymų leidėjas palyginti neseniai pradėjo nagrinėti teisinių santykių, susijusių su automatinio informacijos apdorojimo priemonių neteisėtu panaudojimu, reglamentavimo klausimą. 1996-01-30 d. buvo priimtas Lietuvos Respublikos kompiuterių programų ir duomenų bazių teisinės apsaugos įstatymas. Šis įstatymas gynė kompiuterinių programų kūrėjų ir savininkų teisėtus interesus. Įstatymas nustojo galiojęs 1999-06-09 d., priėmus Autorių teisių ir gretutinių teisių įstatymą. Palyginimui, pavyzdžiui, kaimyninėje Rusijos Federacijoje (RF) 1992 m. Buvo priimtas įstatymas „Dėl elektroninių skaičiavimo mašinų programų ir duomenų bazių teisinės apsaugos“[9]. Šiame RF įstatyme nustatytų teisės normų nesilaikymas užtraukė baudžiamąją atsakomybę, nors pačiame RSFSR Baudžiamajame Kodekse ir nebuvo atskiro straipsnio, numatančio atsakomybę už nusikaltimus informatikos srityje (arba „kompiuterinius nusikaltimus“ – šiandien galiojančiame RF BK būtent šitaip yra įvardinti nusikaltimai kibernetikos sferoje).

Iš tiesų, Lietuvoje teisiniai santykiai kibernetikos srityje pavėluotai buvo pradėti reglamentuoti tiek baudžiamosios teisės, tiek ir kitų teisės šakų rėmuose (pavyzdžiui ATPK 214(10) straipsniu “Autorių teisių ir gretutinių teisių pažeidimas”, kuriuo administracinė atsakomybė numatyta už neteisėtą literatūros, mokslo ar meno kūrinio (įskaitant kompiuterių programas ir duomenų bazes), audiovizualinio kūrinio ar fonogramos viešą atlikimą, atgaminimą, viešą paskelbimą, kitokį panaudojimą bet kokiais būdais ir priemonėmis siekiant turtinės naudos, taip pat neteisėtų kopijų platinimą, laikymą, importavimą, eksportavimą ar gabenimą siekiant turtinės naudos, buvo papildytas tik 2002 metų pabaigoje; LR CK, galiojęs nuo 1965-01-01 iki 2001-06-30 d. visada savyje talpino KETVIRTĄJĮ SKYRIŲ

[9] Закон РФ " О правовой охране программ для электронно-вычислительных машин и баз данных".

„AUTORINĖ TEISĖ“. Tačiau tik 1994 m. (Nr.I-459; 1994.05.17.; Žin., 1994, Nr.44-805) šio kodekso 515 straipsnyje “Kūriniai, kuriems taikoma autorinė teisė” atsirado papildymas, į autorinės teisės dalykų sąrašą įtraukęs dar vieną punktą – „kompiuterių programos ir duomenų bazės“.

Įstatymų leidybos “informatikos teisės” srityje pagrindas yra LR Konstitucijos ir Civilinio kodekso bei tarptautinių dokumentų normos. Sąlygiškai informatikos teisės norminiais aktais LR būtų galima įvardinti sekančius teisės aktus:

Lietuvos Respublikos KONSTITUCIJA

Elektroninio parašo įstatymas

Visuomenės informavimo įstatymas

Asmens duomenų teisinės apsaugos įstatymas

Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose

Dėl duomenų apsaugos plėtojimo 2002-2004 metais programos patvirtinimo

Dėl Asmens duomenų valdytojų valstybės registro įsteigimo ir šio registro nuostatų patvirtinimo

Dėl Asmens duomenų valdytojų valstybės registro reorganizavimo, šio registro nuostatų ir asmens duomenų valdytojų pranešimo apie duomenų tvarkymą automatiniu būdu tvarkos patvirtinimo

Dėl valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo

Dėl Tipinių duomenų saugos nuostatų patvirtinimo

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EC)

Valstybės ir tarnybos paslapčių įstatymas

Elektroninių ryšių ĮSTATYMAS

Dėl Lietuvos Respublikos elektroninių ryšių įstatymo koncepcijos patvirtinimo

Lietuvos Respublikos kompiuterių programų ir duomenų bazių teisinės apsaugos įstatymas – Negalioja de jure

ĮSTATYMAS dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo

Konvencija dėl elektroninių nusikaltimų 2001 11 23/Ratifikuota nuo 2004 01 22; Įsigaliojo nuo 2004 07 01

Valstybės ir tarnybos paslapčių įstatymas

Lietuvos Respublikos ryšių įstatymas – Negalioja de jure

Patentų įstatymas

Europos patentų konvencija

Autorių teisių ir gretutinių teisių įstatymas

Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio ĮSTATYMAS

Dėl Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo

Dėl Viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo

Dėl Lietuvos Respublikos Vyriausybės 2003 m. kovo 5 d. nutarimo Nr. 290 "Dėl Viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo"

Nusikaltimų informatikai baudžiamąja teisine apsauga Lietuvos Respublikoje, kaip jau minėta, taip pat buvo susirūpinta neseniai. 1961 m. Baudžiamojo Kodekso redakcijoje, su tam tikrais pakeitimais galiojusioje iki 2003-05-01 d., apie baudžiamąją teisinę informatikos apsaugą buvo kalbama tik kaip apie tam tikrų teisinių gėrių apsaugą, kurie iš esmės mažai ką turi bendro su šiandien naudojama sąvoka „nusikaltimai informatikai“. Pavyzdžiui, 1997 m. (Nr. VIII-527, 97.11.20, Žin., 1997, Nr.108-2737 (97.11.28)) buvo priimta BK pataisa - 135(2) straipsnis “Tyčinis poveikis kompiuterinei informacijai ar jos apdorojimui”. Tačiau šiame straipsnyje išimtinai kalbama tik apie „kompiuterinės informacijos“ (neteisinga kompiuterinė programa, klaidingi duomenys, kitoks tyčinis poveikis kompiuterinei informacijai ar jos apdorojimui) apsaugą, kuri susijusi tik su rinkimų ar referendumo rezultatų objektyvumo apsauga. 1961 m. BK redakcijoje kaip vienas iš informacijos teisinės apsaugos objektų taip pat įvardijamos autoriaus ir išradėjo teisės (142 str.). Tačiau šiame straipsnyje autorystės teisės objektais pripažįstami tik literatūros, muzikos ar dailės kūriniai bei išradimai ar racionalizaciniai pasiūlymai. Tik 2000 m. (Nr. VIII-1646, 00.04.20, Žin., 2000, Nr.38-1054 (00.05.10)) buvo priimta BK 142 straipsnio pataisa, aukščiau minėtą autorystės teisės objektų išsamų sąrašą papildžiusi dar dviem punktais – kompiuterių programos ir duomenų bazės. Taip pat BK buvo papildytas 142(1) straipsniu - Literatūros, mokslo ar meno kūrinio, audiovizualinio kūrinio ar fonogramos neteisėtas atgaminimas, neteisėtų kopijų importavimas, eksportavimas, platinimas, gabenimas ar laikymas; 142(2) straipsnis. Informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas; 142(3) straipsnis. Neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas.

Šias pataisas, kaip ir daugelį kitų, iššaukė grynai praktinė būtinybė: iki tol galiojusių baudžiamųjų teisinių instrumentų pagalba nebuvo įmanoma nubausti asmenis, įvykdžiusius

aukščiau įvardintas nusikalstamas veikas, kai, tuo tarpu, asmenų, vykdžiusių šiuos nusikalstamus, radosi vis daugiau. Įstatymų leidėjo skubą šiuo klausimu liudija ir pati 142 straipsnio dispozicija – ji nebuvo pakeista iš esmės. Dispozicijos formuluotė buvo paprasčiausiai papildyta pagal prasmę mažai susijusiu „prielipu“ skliausteliuose: „[...] literatūros, mokslo ar meno kūrinio (įskaitant kompiuterių programas ir duomenų bazes)“.

Visgi baudžiamoji teisinė sistema ir toliau logiškai buvo vystoma pagal modelį, vis labiau užtikrinantį kompiuterinės informacijos apsaugą. 2003-05-01 d. įsigaliojo teisininkų praktikų taip vadinamas „naujasis“ LR BK (kuris buvo priimtas dar 2000-09-26 d. Baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymu Nr. VIII-1968). Būtent šiame baudžiamajame kodekse buvo įtrauktas atskiras XXX skyrius - NUSIKALTIMAI INFORMATIKAI, susidedantis iš trijų straipsnių.

2.2. Pagrindinės sąvokos.

Prieš analizuojant nusikaltimų informatikai sudėtis, būtina paaiškinti pagrindines šiame darbe naudojamas sąvokas, susijusias su nusikaltimais kibernetinėje erdvėje.

Informacija

Svarbu atskirti informaciją kaip kasdienio gyvenimo kategoriją ir kaip teisinę sąvoką. Informacija kaip tokia yra ideali kategorija, ji neapčiuopiama ir todėl negali būti teisinių santykių objektu, kol nėra susiejama su jos nešėju, turiniu, identifikuojančiais požymiais.

Teisėje informacija suprantama kaip duomenys apie asmenis, daiktus, faktus, įvykius,

reiškinius ir procesus, esančius ir vykstančius informacinėse sistemose. Informacijos samprata gana tampriai yra susieta su informacinių resursų definicija, kurią reikėtų suprasti kaip atskirus dokumentus ir atskirų dokumentų masyvus informacinėje sistemoje.

Kompiuterinė informacija

Kaip jau minėta, informacija – tai duomenys apie asmenis, daiktus, faktus, įvykius, reiškinius ir procesus, nepriklausomai nuo tų žinių išraiškos formos. Sąvokos „kompiuterinė informacija“ panaudojimas baudžiamajame kodekse yra naujovė – anksčiau tokia sąvoka LR įstatymuose naudojama nebuvo. Teisės doktrinoje yra pateikiama įvairių kompiuterinės informacijos definicijų. Vieną iš universaliausiai suprantamų kompiuterinės informacijos kaip nusikalstamos veikos objekto apibrėžčių pateikia rusų mokslininkas V.Krylovas: „Kompiuterinė informacija - tai duomenys, žinios ar komandų rinkinys (programa), pritaikyti naudoti IBM arba reikalingi jos valdymui, esantys IBM arba informacijos laikmenose. Kompiuterinė informacija - tai identifikuojamas informacinės sistemos elementas, turintis savininką, nustačiusį tokios informacijos naudojimo taisykles“[10]. Taigi tiek teisininkai praktikai, tiek teoretikai linkę susiaurinti šį apibrėžimą ir kompiuterine informacija įvardinti ne pačius duomenis, o tik tuos duomenis, kurie yra patalpinti informacijos laikmenose – t.y. tam tikrą simbolių visumą, užfiksuotą kompiuterio atmintyje ar kitoje informacijos laikmenoje (lanksčiajame diskelyje, kompaktinėje plokštelėje, universaliame optiniame diske ar kitame materialiame įrenginyje). Beje, informacinių technologijų specialistai dar pridėtų, jog, esant atitinkamoms sąlygoms, fizikiniai poliai taip pat gali tapti informacijos perdavimo priemonėmis, o tuo pačiu ir laikinais informacijos nešėjais.

Konfidenciali/slapta informacija arba informacija, saugoma įstatymų

Tai informacija, skirta ne visuotiniam naudojimui. Tokios informacijos platinimas gali padaryti žalą ją pateikusio asmens arba jos savininko teisėms ir teisėtiems interesams. Tai dokumentinė informacija, priėjimas prie kurios reglamentuojamas specialiais įstatymais. Vadovaujantis teisės aktais, konfidencialia informacija laikytina tokia informacija, kurios tyrinys sudaro valstybės paslaptį (LR Valstybės ir tarnybos paslapčių įstatymas), informacija, perduodama susirašinėjimų, telefoninių pokalbių, telegrafavimo ar kitokiu būdu (Konstitucija, Operatyvinės veiklos įstatymas), informacija apie įvaikinimo paslaptį (Vaiko teisių apsaugos

[10] Крылов В. Информационные преступления — новый криминалистический объект //Российская юстиция.— 1997.— № 4, с. 22

pagrindų įstatymas), informacija apie komercinę paslaptį, bankinę paslaptį, (Civilinis kodeksas), informacija, esanti autorinių ir gretutinių teisių objektu (Autorių teisių ir gretutinių teisių įstatymas), informacija apie asmens tapatybės duomenis (Asmens duomenų teisinės apsaugos įstatymas) ir kt.

Informaciniai resursai

Informacinių resursų samprata tampriai susieta su informacijos definicija. Informaciniai resursai – tai informacinės sistemos atskiri dokumentai ir dokumentų masyvai (duomenų bankai), kurių pagrindu informacinėje sistemoje modifikuojami seni duomenys bei kuriami nauji.

Kibernetinė teisė

Terminas „kibernetinė teisė“ atsirado ekonomiškai išsivysčiusiose valstybėse XX a. viduryje, kaip elektroninių skaičiavimo mašinų ir su jomis susietų technologijų pritaikymo daugelyje gyvenimo sferų pasekmė. Kibernetinė teisė – tai naujų socialinių santykių, atsirandančių dėl informacinių technologijų panaudojimo gamyboje, visuomeninėje veikloje, asmeniniame gyvenime, formavimosi juridinis įprasminimas. Nė vienoje valstybėje „kibernetinė teisė“ neperaugo į atskirą teisės šaką, bet susideda iš įvairaus hierarchinio lygmens ir įvairių teisės šakų teisinių norminių aktų: konstitucinės, administracinės, civilinės, baudžiamosios teisės.

Neteisėta prieiga prie kompiuterinės informacijos

Teisės doktrinoje neteisėta prieiga prie kompiuterinės informacijos yra įvardijama informacijos savininko nesankcionuotas susipažinimas su duomenimis, esančiais kompiuterio atmintyje (kietajame diske) ar kitoje informacijos laikmenoje. Profesorius V.S.Komisarovas neteisėta prieiga prie kompiuterinės informacijos įvardija situaciją, kai kaltininkas įgyja galimybę susipažinti su informacija ar ja disponuoti savo nuožiūra, be informacijos savininko ar jo įgalioto asmens sutikimo. Atskira neteisėtos prieigos prie kompiuterinės informacijos forma yra atvejai, kai į kompiuterinę sistemą, kompiuterių tinklą ar tam tikrą informacijos masyvą be savininko sutikimo yra įvedama žinomai neteisinga informacija, kuri iškreipia to informacijos masyvo prasmę ir kryptingumą.

Kompiuterinės informacijos sunaikinimas

Tai informacijos laikmenoje saugomos informacijos būsenos pakeitimas tokiu būdu, kai ją dėl tokio pakeitimo naudoti pagal paskirtį iš esmės tampa nebeįmanoma.

Kompiuterinės informacijos užblokavimas (naudojimo apribojimas)

Tai būsena, kai techninių priemonių, programinės įrangos pagalba yra sukuriama neprieinamumo prie informacijos situacija, ko pasėkoje neįmanomas tolesnis jos naudojimas (yra užblokuojamas tolesnis kompiuterinių komandų vykdymo eiliškumas, išjungiamas kuris nors kompiuterio įrenginys/įrenginiai, blokuojama kompiuterio įrenginio reakcija informacijos išsaugojimo metu ir pan.).

Informacijos pakeitimas

Tai pirminės informacijos pakeitimas be jos savininko ar kito teisėto asmens sutikimo tokiu būdu, kai nebeįmanoma atkurti pirminės informacijos, tačiau informacijos pakeitimas nėra esminis.

Informacijos kopijavimas

Tai originalios informacijos dublikato padarymas, nepažeidžiant pirminės informacijos ir išsaugant galimybę pirminę informaciją naudoti pagal paskirtį.

Kompiuterio, kompiuterio sistemos ar kompiuterių tinklo darbo sutrikdymas

Kompiuterio, kompiuterio sistemos ar kompiuterių tinklo darbo sutrikdymas – tai tokios neordinarinės situacijos tyčinis sukėlimas, kai dėl trikdžių nutraukiamas/išvedamas iš rikiuotės kompiuterinės įrangos darbas, kai sistema teisėtam vartotojui ima teikti neteisingą ar apskritai „atsisako“ pateikti informaciją. Tačiau visais šiais atvejais būtinoji sąlyga yra tai, kad kompiuteris, kompiuterio sistema ar kompiuterių tinklas fizine prasme kaip daiktai lieka nepažeisti. Priešingu atveju mes jau kalbėtume ne tik apie kompiuterio, kompiuterio sistemos ar kompiuterių tinklo darbo sutrikdymą, bet ir apie turto sunaikinimą ar sugadinimą – LR BK 187 str. (sutaptis).

Informacijos laikmenos

Tai mobilūs informacijos kaupimo įrenginiai, užtikrinantys kompiuterio kietajame diske esančios informacijos judėjimą materialiame pavidale bei sąveiką su aplinka (lankstieji diskeliai, išoriniai kietieji/standieji diskai, kompaktinės plokštelės ir universalieji optiniai diskai, USB atmintinės ir kt.).

Kompiuterių sistema (serveris)

Tai visuma tarpusavyje susietų kompiuterių ir jų priedų, kurie sujungti tarpusavyje tikslu pakelti darbo efektyvumą (ši kompiuterių visuma dar vadinama *serveriu*).

Kompiuterių tinklas

Tai kompiuterių, priedų ir ryšio kanalų visuma, leidžianti naudoti bet kurio į tinklą įjungto kompiuterio informacinius ir skaitmeninius resursus, nepriklausomai nuo to, kurioje

vietoje yra pats įrenginys.

2.3. Nusikaltimų informatikai samprata

Šiuo metu Lietuvos teisės moksle vis dar nėra aiškios nusikaltimo informatikai sampratos. Kitų šalių mokslininkai taip pat pateikia skirtingus požiūrius į nusikaltimų informatikos srityje fenomeną, skirtingai klasifikuoja nusikaltimus kibernetinėje erdvėje.

Egzistuoja dvi pagrindinės mokslinės minties srovės, skirtingai traktuojančios elektroninių nusikaltimų esmę. Viena jų prie nusikaltimų kibernetinėje erdvėje priskiria visus nusikaltimus, kuriuose kompiuteris bei kompiuterinė informacija yra tiek nusikaltimo objektas, tiek nusikalstamos veikos priemonė. Kita – prie nusikaltimų informatikai priskiria tik priešingus teisei veiksmus, informacijos elektroninio apdorojimo procese. Pastarieji mokslininkai pagrindiniu kvalifikuojančiu požymiu, leidžiančiu tam tikrus nusikaltimus

išskirti į atskirą nusikaltimų informatikos srityje grupę, įvardina specifinių nusikalstamos veikos būdų, priemonių ir objektų bendrybę. Kitaip tariant, nusikalstamos veikos objektas yra informacija, apdorojama kompiuterinės technikos pagalba, o kompiuteris tarnauja nusikalstamos veikos priemone tai informacijai gauti, pakeisti, sunaikinti ir pan. Daugelio šalių (tame tarpe ir Lietuvos) įstatymų leidėjai pasirinko būtent pastarąją koncepciją ir būtent šios koncepcijos rėmuose vysto įstatymų leidybą, siekdami kovoti su nusikaltimais informatikos srityje.

Prisilaikant etatistinės koncepcijos, nusikaltimas yra pavojinga ir baudžiamuosiuose įstatymuose uždrausta veika (t.y. apibrėžtus požymius atitinkanti veika, formalizuota baudžiamajame įstatyme). Baudžiamosios teisės teorijoje nusikaltimo samprata yra formuluojama iš materialistinių pozicijų - bet kurio nusikaltimo esmė yra ta, kad jo padarymu yra keičiami, nutraukiami konkretūs nusistovėję visuomeniniai santykiai, kurie įprasmina atitinkamus baudžiamosios teisės normomis saugomus materialinius, socialinius, ideologinius teisinius gėrius. Išeinant iš šios pozicijos, dėl nusikaltimų informatikos srityje dalyko dviejų nuomonių būti paprasčiausiai negali – akivaizdu, kad dalykas yra pati informacija, o nusikaltėlio veiksmai vertintini kaip kėsinimasis į informacinius visuomenės santykius.

Nusikaltimų informatikos srityje (kai kurie autoriai naudoja „kompiuterinių nusikaltimų“ sąvoką, kas, mano galva, nėra tikslu – ši definicija labiau atspindi „išplėstinį“ požiūrį į šiuos nusikaltimus) subjektas gali būti tiek bendrasis, tiek ir specialusis. Subjektas nusikalstamą veiką kibernetinėje erdvėje paprastai padaro veikdamas tiesiogine tyčia, tačiau materialiose nusikaltimų sudėtyse jo santykis su tokios veikos pasekmėmis gali būti ir neatsargumas.

Taigi *nusikaltimai informatikai* yra baudžiamajame įstatyme numatyta visuomeniškai pavojinga veika, kurios objektas yra visuomeniniai santykiai, susiję su kompiuterinės informacijos saugiu naudojimu, o nusikalstamos veikos dalykas yra kompiuterinė informacija, kompiuterinė programa.

2.4. LR BK XXX skyriaus "Nusikaltimai informatikai" baudžiamoji teisinė charakteristika - bendrieji nusikaltimų kibernetinėje erdvėje bruožai

Naujajame Lietuvos Respublikos Baudžiamajame kodekse pirmą kartą mūsų valstybės baudžiamosios teisės tapsmo istoriniame procese buvo kriminalizuota atskira nusikaltimų rūšis – t.y. nusikaltimai informatikos srityje (kai kurių valstybių įstatymuose dar vadinami „kompiuteriniais nusikaltimais“). Pirmą kartą tokio pobūdžio nusikaltimai, kurių dalykas yra labai specifinis - kompiuterinė informacija - įstatymo leidėjo buvo įvardinti visuomeniškai pavojingomis veikomis.

Nusikaltimai, kurių dalykas yra tik kompiuterinė įranga ir jos priedai (šių daiktų vagystė, sunaikinimas, sugadinimas), priskirtini visai kitoms nusikaltimų rūšims ir baudžiamoji atsakomybė už tai numatyta kituose BK specialiosios dalies skyriuose

(nusikaltimai nuosavybei) ir atitinkamuose straipsniuose. Nors, žinoma, pagrobus, sugadinus ar sunaikinus kompiuterį, dažnu atveju tyčia neteisėtu būdu yra pasisavinama, sugadinama ar sunaikinama ir jo standžiajame diske buvusi informacija. Tokiu atveju, papildomai nusikalstamą veiką tenka kvalifikuoti ir pagal atitinkama straipsnį iš „nusikaltimų informatikai“ skyriaus. Kenkėjiškas poveikis kompiuterio informacinėms komandoms gali būti daromas ir netiesiogiai: pavyzdžiui, kompiuterio procesoriaus darbo „užciklinimas“ tokiu būdu, kad, net minimaliai pagal paskirtį naudojant kompiuterio resursus, jis pradeda kaisti ir galiausiai perdega, ko pasėkoje, gali būti prarasta informacija/informacijos dalis, esanti ir kietajame diske. Tokia veika turėtų būti kvalifikuojama pagal atitinkamus BK straipsnius tiek iš „nusikaltimų informatikai“, tiek iš „nusikaltimų nuosavybei“ skyrių (sutaptis) – šioje situacijoje būtų pažeisti du baudžiamosios teisinės apsaugos dalykai. Tačiau svarbu pabrėžti, jog jeigu nusikalstamos veikos dalykas yra ne informaciniai resursai, o grynai kompiuterinės technikos elementas (pavyzdžiui, vaizduoklio fizinis apgadinimas), tokia veika negali būti priskiriama prie nusikaltimų informatikai, nes, tokiu atveju, kompiuterinė technika bus tik fizinis daiktas kaip ir bet kuris kitas materialus aplinkos elementas. Jeigu buvo sugadinta kompiuterinė technika, pareigūnas tiriantis bylą ir turi įrodyti, ar tokiu sugadinimu buvo siekiama vienokiu ar kitokiu būdu paveikti (pakeisti, sunaikinti, pasisavinti ir pan.) informacijos laikmenose buvusią informaciją. LR BK ir buvo papildytas visiškai nauju skyriumi „nusikaltimai informatikai“ tikslu užtikrinti informacinės aplinkos saugumą. Tik kaip šalutinis/pagalbinis tikslas būtų kompiuterinių techninių priemonių apsauga, bet tik tiek, kiek ši technika yra materiali informacinių resursų laikmena.

Neteisėto informacijos panaudojimo pasekmės gali būti pačios įvairiausios – tai ne tik intelektualinės nuosavybės neliečiamumo pažeidimas, bet ir duomenų apie asmeninį žmogaus gyvenimą paviešinimas, juridinio ar fizinio asmens reputacijos praradimas, normalios/įprastinės fizinio ar juridinio asmens veiklos sutrikdymas ir t.t. Šia prasme nusikaltimų informatikai bendruoju objektu gali būti visuomeninių santykių, saugomų baudžiamojo įstatymo visuma, kaip kompiuterinės informacijos naudojimo saugumo užtikrinimo išraiška. Tačiau specialusis rūšinis objektas šiuo atveju bus tik visuomeniniai santykiai žinijos/informacijos socialinės apyvartos sferoje. Nusikaltimų informatikai dalykas yra įvardintas konkrečiose LR BK XXX skyriaus straipsnių dispozicijose, kur nusikaltimų sudėtys yra formuluojamos iš alternatyvių nusikaltimo subjekto veiksmų.

Kartais tiek teisininkų praktikų, tiek mokslininkų gretose ginčijamasi – ar visada

kompiuterinė informacija yra tik nusikalstamos veikos dalykas, ar vis tiktai ji gali būti ir nusikaltimo padarymo priemone, kai elektroninė-skaičiavimo technika yra naudojama kitos nusikalstamos veikos padarymui ir ta veika yra kėsinamasi į visai kitus baudžiamojo įstatymo saugomus teisinius gėrius/nusikaltimo objektus.

Pastaroji pozicija, žinoma, nėra be pagrindo (vien tas faktas, jog tiriant nusikaltimus ar baudžiamuosius nusižengimus, kuriuos padarant vienaip ar kitaip buvo naudojamas kompiuteris ar kompiuterinė informacija, yra naudojamos analogiškos procesinės priemonės kalba pats už save), bet akivaizdu, kad toks požiūris išplėstų „nusikaltimų informatikai“ sampratą, kas tik apsunkintų tiek įstatymus leidžiančių, tiek juos taikančių institucijų darbą. Bet kuri juridinė sąvoka visų pirma turi būti operacionalizuojama – t.y. aiškiai ir suprantamai apibrėžiama ir maksimaliai „priartinama“ prie socialinės tikrovės.

Lietuvos Respublikos įstatymų leidėjas neatsitiktinai pasirinko pirmąjį kelią, formuluodamas naujojo LR BK XXX skyriaus nusikaltimų sudėtis tokiu būdu, kad tik kompiuterinė informacija (bei kompiuterinė programa, kuri tam tikra prasme taip pat yra kompiuterinė informacija) kiekvienu atveju yra pateikiama nusikaltimų informatikai dalyku.

Tokia situacija, kaip minėta, aiškinama grynai praktiniais motyvais. Tačiau negalima paneigti, jog dėl tokio požiūrio susilpnėja baudžiamoji teisinė apsauga nuo tų nusikaltimų, kurių padarymui kompiuterinė informacija ir kompiuterinė technika naudojami kaip įrankis – t.y. pati kompiuterinė informacija gali tapti visuomeniškai pavojingos veikos įrankiu ir netgi pagrindu.

Visi LR BK XXX skyriuje aprašyti nusikaltimai informatikai, vadovaujantis LR BK 11 str., priskirtini tyčinių nesunkių nusikaltimų grupei – tai yra tyčiniai nusikaltimai, už kuriuos baudžiamajame įstatyme numatyta didžiausia bausmė neviršija trejų metų laisvės atėmimo. Tik už nusikaltimą, numatytą LR BK 198 str. 2 d. yra numatyta 4 m. laisvės atėmimo bausmė ir ši nusikalstama veika priskirta prie apysunkių tyčinių nusikaltimų.

Charakterizuojant objektyviąją analizuojamų nusikaltimų sudėties pusę, pažymėtina, jog dalies šių nusikaltimų sudėtys yra formaliosios (tokios veikos kvalifikavimui užtenka įvykdyti tam tikrus alternatyvius veiksmus) kita dalis - materialiosios sudėtys, numatančios ne tik visuomeniškai pavojingos, baudžiamuoju įstatymu uždraustos veikos įvykdymą (veikimu), bet ir būtiną visuomeniškai pavojingų pasekmių atsiradimą bei priežastinio ryšio tarp veikos ir tų pasekmių nustatymą.

Pagal LR BK 3 str. 1 d., „Nusikalstamos veikos padarymo laikas yra veikimo laikas

arba baudžiamojo įstatymo numatytų padarinių atsiradimo laikas, jeigu asmuo norėjo, kad padariniai atsirastų kitu laiku“. Žinoma, ši taisyklė taikytina ir nusikaltimų informatikai atveju.

Pagal LR BK 4 str. 2 d., „Nusikalstamos veikos padarymo vieta yra vieta, kurioje asmuo veikė arba turėjo ir galėjo veikti, arba vieta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai“. Vėlgi, šis teiginys taikytinas ir nusikaltimams informatikai (nors teiginys apie padarinių atsiradimo vietą taikytinas tik materialiosioms nusikaltimų sudėtims). Praktikoje nusikaltimų informatikai padarymo vietos konstatavimas yra gana keblus klausimas. Pasinaudojant tinkle sujungtais kompiuteriais ir kitomis technologijomis, nusikaltimus juk galima daryti per atstumą – kabeliniu ar bevieliu ryšiu. Nusikaltėliui nereikia būti toje vietoje, kurioje jis yra sumanęs atsirasiant nusikalstamos veikos pasekmes. Be to, nereikėtų pamiršti, kad bet kuris nusikaltimas kibernetinėje erdvėje gali būti tarptautinis. Vis tik, atsižvelgiant į tai kas pasakyta, aukščiau aprašytas LR BK bendrinis nusikaltimo vietos konstatavimo principas tinka ir kalbant apie nusikaltimus informatikai. Materialiosios nusikaltimo sudėties atveju (LR BK 196, 197 straipsniai), nusikaltimo vieta bus pripažįstama ta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai (didelė žala dėl kompiuterinės informacijos ar kompiuterinės programos sugadinimo, sunaikinimo ar kitų dispozicijose išvardintų nusikalstamų veikų). Formaliosios nusikaltimo sudėties atveju (LR BK 198, $198^{(1)}$, $198^{(2)}$ straipsniai), nusikaltimo vieta bus pripažįstama ta, kurioje veikė nusikaltimo subjektas.

Nusikaltimai informatikai padaromi tik veikimu ir tyčia. (LR BK 16 str. 4 d. pasakyta: „Asmuo baudžiamas už nusikaltimo ar baudžiamojo nusižengimo padarymą dėl neatsargumo tik šio kodekso specialiojoje dalyje atskirai numatytais atvejais“). Remdamiesi LR BK 15 straipsniu, visais nusikaltimų informatikai atvejais mes galime kalbėti tik apie tiesioginę subjekto tyčią santykyje su veika - t.y., kai: *pirma* - nusikaltimą darydamas asmuo suvokė pavojingą nusikalstamos veikos pobūdį ir norėjo taip veikti; *antra* – nusikaltimą darydamas asmuo suvokė pavojingą nusikalstamos veikos pobūdį, numatė, kad dėl jo veikimo ar neveikimo gali atsirasti baudžiamajame kodekse numatyti padariniai, ir jų norėjo.

Pasekmių norėjimas ar nenorėjimas – tai valinis tyčios elementas. Pasekmių norėjimas kaip tiesioginės tyčios elementas yra būtinas materialiosiose nusikaltimų sudėtyse (tokios yra ir LR BK XXX skyriaus 196 ir 197 straipsniuose numatytų nusikaltimų sudėtys). Tuo tarpu formaliosiose nusikaltimų sudėtyse pasekmės nėra būtinasis požymis, todėl jų norėjimas neturi reikšmės. Nors netiesioginė tyčia galima tik materialiosiose nusikaltimų sudėtyse,

sunku įsivaizduoti situaciją, kai kompiuterinė informacija, kompiuterinė programa sunaikinama ar pakeičiama netiesiogine tyčia – t.y. numatant, jog dėl pavojingo nusikalstamos veikos pobūdžio gali atsirasti aukščiau išvardinti padariniai, bet jų nenorint ir vis tiktai sąmoningai leidžiant jiems atsirasti. „Pažymėtina, jog tais atvejais, kai asmuo numato, jog pasekmės atsiras neišvengiamai, nors jis jų ir nenori, ir vis dėlto elgiasi nusikalstamai, tai toks asmuo veikia tiesiogine tyčia“[11]. Nors aplinkybių išsiaiškinimas, ar asmuo, padaręs nusikaltimą informatikai, suvokė, jog vienokia ar kitokia visuomeniškai pavojinga nusikalstama veika neišvengiamai iššauks atitinkamas neigiamas pasekmes, yra ikiteisminio tyrimo dalykas, manau, akivaizdu, kad nusikaltimų informatikai atveju, subjektas yra intelektualus ir jis, žinoma, suvokia jog dėl tam tikros veikos pasekmės kils neišvengiamai.

Fakultatyviniai nusikaltimų informatikai subjektyviosios pusės požymiai neturi reikšmės šių nusikaltimų kvalifikavimui. Paprastai tokių nusikalstamų veikų motyvai būna savanaudiškos arba chuliganiškos paskatos (kas, žinoma, tuo pačiu yra ir atsakomybę sunkinančios aplinkybės), bet ne išimtis ir siekis nuslėpti kitą nusikaltimą. Neatsitiktinai įstatymų leidėjas už nusikaltimų informatikai padarymą suteikią teisėsaugos institucijoms galimybę baudžiamojon atsakomybėn traukti ir juridinį asmenį (pavyzdžiui, daugelyje įmonių buhalterinė apskaita tvarkoma kompiuterių ir specialios programinės įrangos pagalba – taigi kompiuterinė informacija gali būti sunaikinama, siekiant nuslėpti spausdintų dokumentų ir kompiuterio atmintyje esančių duomenų neatitikimus).

Už nusikaltimus informatikai pagal LR BK 13 str. 1 d. atsako asmuo, kuriam iki nusikaltimo padarymo buvo suėję šešiolika metų. Taip pat toks asmuo turi atitikti subjektyviosios pusės požymį – t.y. būti pakaltinamas.

LR BK XXX skyriaus straipsnių dispozicijos iš esmės yra aprašomosios. Visose jose aprašomos nusikaltimų sudėtys su alternatyviais veiksmais. Tačiau yra ir blanketinių nusikaltimų informatikai sudėčių. Daugelyje valstybių jau šiandien egzistuoja ne tik asmens duomenų apsaugos įstatymai, bet ir, pavyzdžiui, „kompiuterio eksploatavimo taisyklės“. Lietuvoje taip pat galioja teisės aktai, į kuriuos nukreipia BK XXX skyriuje įtvirtintos teisės normos – Elektroninio parašo įstatymas, Įstatymas dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo ir 2004-07-01 Lietuvos Respublikoje įsigaliojusi Europos Tarybos

[11] Baudžiamoji teisė. Bendroji dalis.- Vilnius, Eugrimas, 1996, p. 201.

konvencija dėl elektroninių nusikaltimų bei kt.

LR BK už nusikaltimus informatikai numatytos alternatyvios sankcijos. Taip pat, kaip jau minėta, už šias veikas atsako ir juridinis asmuo (juridinių asmenų baudžiamosios atsakomybės bendrosios sąlygos ir principai įtvirtinti šio kodekso bendrojoje dalyje – 20 ir 43 straipsniuose).

Tik įsigaliojus naujajam LR BK (2003-05-01), XXX skyrių sudarė trys straipsniai (196, 197 ir 198). Dėl teisininkų ir informatikos mokslų atstovų pastabų 2004-01-29 d., įsigaliojus BK pakeitimams, atsirado dar du straipsniai, kurie, siekiant išvengti kodekso straipsnių struktūros keitimo, buvo užvardinti $198^{(1)}$ ir $198^{(2)}$. Taigi analizuojamų teisės normų dispozicijos konstravimui didelę įtaką turi specialios techninės žinios.

Šiuo metu BK XXX skyrius atrodo sekančiai:

196 straipsnis. Kompiuterinės informacijos sunaikinimas ar pakeitimas,

197 straipsnis. Kompiuterinės programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas,

198 straipsnis. Kompiuterinės informacijos pasisavinimas ir skleidimas,

$198^{(1)}$ straipsnis. Neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo,

$198^{(2)}$ straipsnis. Neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti.

2.4.1.LR BK 198(1) straipsnio „Neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo“ baudžiamoji teisinė analizė.

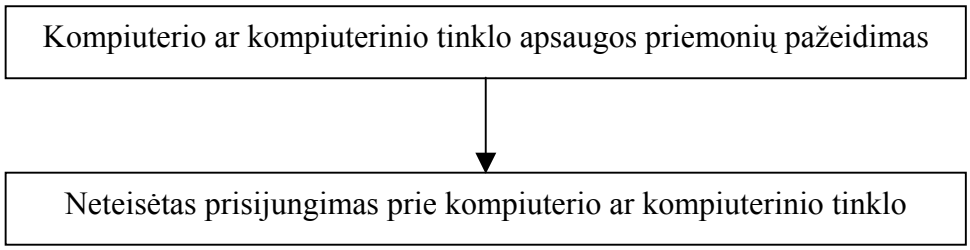
Pastaruoju metu ir Lietuvoje vis labiau plinta hakerių (kompiuterinių įsilaužėlių – chuliganų) fenomenas. Tam palankią dirvą sukuria kompiuterio vartotojų kompiuterinio raštingumo trūkumas – dažnos įmonės/įstaigos kompiuterių tinkle (su prieiga prie Interneto) esanti informacija nėra apsaugota net elementariais vartotojų prisijungimo slaptažodžiais, nekalbant jau apie kompiuterinių programų, apsaugančių nuo „Trojos arklių“ ir kitų virusų-šnipų, ugniasienių (*firewall*) įdiegimą. Net ir tuo atveju, jeigu yra įdiegtos ugniasienės, jos yra konfigūruojamos, nustatant leistinus/draustinus IPN/A (*Internet Protocol Number/Address*), kas dažnu atveju palieka „skylę“ hakeriams. Sunku pasakyti, kokį mastą Lietuvoje yra įgijęs hakeriavimas – specialių tyrimų šioje srityje atlikti neįmanoma. Apie šį negatyvų informacinės aplinkos reiškinį paprastai sužinome tik iš pranešimų per masinės informacijos priemones, kai įžūlūs kompiuteriniai įsilaužėliai valstybinių įstaigų oficialiuose tinklapiuose patalpina savo informaciją arba „ženklus“, įrodančius, jog jie įveikė kompiuterio ar kompiuterinio tinklo technines bei programines apsaugos priemones (pavyzdžiu galėtų pasitarnauti prieš pora metų LR vyriausybės tinklapyje patalpinta pornografinė vaizdo medžiaga, kurią galėjo matyti neregistruoti tinklapio lankytojai). Žinoma, pats prisijungimas prie svetimo kompiuterio ar kompiuterinio tinklo nėra labai pavojinga nusikalstama veika – tai nėra susiję su informacinių resursų naikinimu, modifikavimu, pasisavinimu ar panašiai. Tai greičiau chuliganiški veiksmai virtualioje erdvėje, neatskleidžiant nukentėjusiajam savo tapatybės ir parodant jam, jog kompiuteris/kompiuterinis tinklas, prie kurio neteisėtai buvo prisijungta, yra pažeidžiamas iš išorės (kartais fiziniai ar juridiniai asmenys yra net šantažuojami, primenant jiems, jog jų kompiuteriuose, kompiuteriniuose tinkluose saugoma informacija gali būti panaudota neteisėtiems tikslams).

Tokios neteisėtos prieigos būdai paprastai yra šie: svetimo vartotojo vardo panaudojimas, IPN/A (Internet Protocol Number/Address) arba techninio įrenginio fizinio adreso pakeitimas, slaptažodžio parinkimas, programinių „skylių“ suradimas ir jų panaudojimas, bei kiti sistemos “apgavimo” būdai (yra net kuriamos kompiuterinės programos, generuojančios vartotojo vardo ir slaptažodžio variantus, „atskleidžiančios“ žvaigždutėmis rodomą slaptažodį ir panašiai, už ką, beje, LR BK 198(2) straipsnyje taip pat numatyta baudžiamoji atsakomybė).

2004-01-29 d., įsigaliojus naujojo LR BK pakeitimams, XXX skyrius buvo papildytas

198(1) straipsniu, nukreiptu prieš hakerių fenomeną. Šis straipsnis teigė, jog nusikalstamai veikia tas, „kas neteisėtai prisijungė prie kompiuterio ar kompiuterinio tinklo pažeisdamas kompiuterio ar kompiuterinio tinklo apsaugos priemones“.

Nusikaltimo, numatyto LR BK 198(1) straipsnyje, objektyviosios pusės grafinė išraiška.



„Neteisėtą prisijungimą“ reikėtų suprasti kaip tokį, kai veikiantysis subjektas neturi jokio teisinio pagrindo prieiti prie pavieniame ar į tinklą pajungtame kompiuteryje/serveryje saugomos informacijos – t.y., kai veikiantysis subjektas neturi prieigos teisės, grindžiamos nuosavybės, darbo santykiais, įgaliojimu ar kitokiais pagrindais (tai yra, kai asmuo nėra teisėtas kompiuterinės informacijos vartotojas arba neturi leidimo dirbti su tam tikro lygmens informacija).

Iš LR BK 198(1) straipsnio dispozicijos matyti, jog kalbama ne apie bet kokį neteisėtą prisijungimą prie kompiuterio ar kompiuterinio tinklo, bet tik apie tokį, kurio įvykdymui buvo reikalinga pažeisti kompiuterio apsaugos priemones. Taigi jeigu nukentėjusysis savo kompiuteryje esančią informaciją yra bent jau subendrinęs tam, kad ją būtų galima naudoti tinkle ir tokio naudojimo galimybės nėra užslaptinęs (nėra prisijungimo slaptažodžių ir pan.), priėjimas prie tokiame kompiuteryje/kompiuterių tinkle esančios informacijos nebus nusikalstamas. Ar galima tokia situacija praktikoje, sunku pasakyti. Tiek Windows, tiek Linux sistemų baziniuose nustatymuose duomenų naudojimas tinkle nėra subendrintas. Visais atvejais vartotojai, siekdami, kad kompiuterinė informacija būtų prieinama tinkle, patys turi atitinkamai pakeisti tinklo parametrus, patys nuspręsti, leisti arba neleisti (jeigu leisti, tai kokia apimtimi) keisti savo duomenis, o taip pat, kokiems subjektams tai leisti ir kokiomis sąlygomis (slaptažodžių įvedimas ir pan.). Windows NT/2000/XP sistema vartotojui apskritai „neleidžia“ sukonfigūruoti tinklo, nenaudojant slaptažodžių (ankstesnėse Windows versijose tai nebuvo privalomas elementas, bet tai jau yra numatyta iš Interneto parsisiunčiamuose atnaujinimuose). Taigi patys sisteminių kompiuterinių programų gamintojai rūpinasi, kad

laisvas neteisėtas prisijungimas prie kompiuterių ar kompiuterinio tinklo būtų negalimas ir įsilaužėliai, siekdami tai padaryti, turėtų atlikti aktyvius veiksmus. Tokio pobūdžio nusikaltimas („įsilaužimas“) tik signalizuoja apie informacijos, saugomos kompiuteryje pažeidžiamumą, tačiau jis nėra tiesiogiai susijęs su informacijos praradimu, jos kopijavimu ar kitokiu neigiamu poveikiu kompiuterinei informacijai. Nusikaltimo subjektui, sėkmingai prisijungusiam prie kompiuterio ar kompiuterinio tinklo, atsiveria galimybė peržiūrėti kompiuteryje saugomą informaciją (ar bent jos dalį – apsaugos priemonės gali būti panaudotos ir atskirų dokumentų saugumo užtikrinimui), daryti jai poveikį. Tačiau poveikio kompiuterinės informacijos atžvilgiu įvykdymas kvalifikuojamas pagal kitus LR BK XXX skyriaus straipsnius.

Žinoma, hakeriai įsilaužinėja į kompiuterių sistemas ne dėl malonumo įveikti kompiuterio apsaugas. Kompiuterinis „įsilaužimas“ kaip toks, mano galva, nėra savipakankama veika, kad ją būtų galima įvardinti nusikaltimu (nors įstatymų leidėjas ir išreiškė tokią valią, manau, kad akademinėje bendruomenėje ją galima kritikuoti). Manau, jog realybėje bet kokį prisijungimą prie kompiuterio ar kompiuterinio tinklo, pažeidžiant apsaugos priemones, tektų papildomai kvalifikuoti ir pagal kitus LR BK XXX skyriaus straipsnius, nes „grynasis“ kompiuterinis įsilaužimas egzistuoja tik labai trumpą laiko atkarpą kaip pereinamoji grandis. Pavyzdžiui, Rusijos Federacijos Baudžiamojo kodekso atitinkamame 272 str. „Neteisėta prieiga prie kompiuterinės informacijos“ teigiama, jog „neteisėta prieiga prie įstatymo saugomos kompiuterinės informacijos, t.y., informacijos, esančios elektroninėje laikmenoje, elektroninėje skaičiavimo mašinoje (IBM), ar jų tinkluose ar IBM sistemoje, jei tokia veika įtakojo informacijos sunaikinimą, užblokavimą, modifikavimą arba tokia informacija buvo kopijuojama, jeigu dėl to buvo pažeistas IBM ar jų tinklo arba sistemos darbas, baudžiama [...]“. Akivaizdu, kad neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo yra tik priemonė (labai svarbi ir būtina priemonė) daryti kitus nusikaltimus informatikos sferoje, ir, manau, būtų logiška, kad tokie nusikaltėlių veiksmai nebūtų išskirti į atskirą nusikalstamą veiką, bet inkorporuojami į kitų nusikaltimų informatikai sudėtis.

Net ir tuo atveju, kai kompiuterinės informacijos įsilaužėliai nenaikina, nekopijuoja ir pan., o tik papildo, į kompiuterio kietąjį diską įrašydami savo informacija, tai vis tiek nebus tik prisijungimas prie kompiuterio ar kompiuterinio tinklo. Tokie veiksmai būtų prilyginti informacijos modifikavimui – t.y. kompiuterio atmintyje esančios informacijos

visumos/viseto pakeitimui (nors, iš pirmo žvilgsnio, kompiuteryje buvusi informacija nebūtų net paliesta).

Yra grynai teorinė galimybė, kad įsilaužėlis, dėl kokių nors priežasčių (priklausančių arba nepriklausančių nuo jo valios), neteisėtai prisijungęs prie kompiuterio ar kompiuterinio tinklo, nespės/negalės/nenorės padaryti nusikalstamas veikas, numatytas LR BK 196, 197, 198 straipsniuose - t.y. jis bus tik „neteisėtai prisijungęs“ prie kompiuterio ar kompiuterinio tinklo. Iš tiesų, paaiškėjus tokiai situacijai, būtų lyg ir akivaizdu, kad veikiantysis subjektas įvykdė visuotinai pavojingą veiką, tačiau už tai nebūtų įmanoma jo patraukti baudžiamojon atsakomybėn pagal 196, 197, 198 BK straipsnius.

LR BK 22 str. kalbama apie pasikėsinimą padaryti nusikalstamą veiką: „Pasikėsinimas padaryti nusikalstamą veiką yra tyčinis veikimas ar neveikimas, kuriais tiesiogiai pradedamas daryti nusikaltimas ar baudžiamasis nusižengimas, jeigu veika nebuvo baigta dėl nuo kaltininko valios nepriklausančių aplinkybių“. Tačiau aukščiau aprašytoje teorinio modeliavimo situacijoje, kol veikiantysis asmuo, neteisėtai prisijungęs prie kompiuterio ar kompiuterinio tinklo, nepradės daryti nusikalstamas veikas, numatytas LR BK 196, 197, 198 straipsniuose, tol tokio pobūdžio neteisėtas „įsilaužimas“ nebus traktuojamas nei kaip pasikėsinimas.

Turint omenyje grynai teorinio modelio realizavimosi tikimybę, LR BK $198^{(1)}$ straipsnio gyvavimas turi sau pateisinimą. Juolab, kad dėl nusikalstamų veikų, numatytų LR BK 196 ir 197 straipsniuose, baudžiamoji atsakomybė kyla tik tuo atveju, jeigu dėl tokios veikos buvo padaryta didelė žala (tiesa, kas tai yra, kol kas neaišku – LR BK 190 str. yra išaiškinta turto vertė, taikoma XXVIII skyriaus nusikaltimams; turto vertė yra atskirai išaiškinama ir kalbant apie kai kuriuos kitus nusikaltimus, pavyzdžiui, kyšininkavimą, papirkimą, kontrabandą. Nusikaltimų informatikai atveju „didelę žalą“ turbūt reikėtų suprasti ne vien kaip turtinę žalą, o jos nustatymo bendrieji principai turėtų išsirutulioti iš teismų praktikos – bent jau tokia turbūt yra įstatymų leidėjo valia). Taigi, net jeigu yra pakankamai įrodymų, jog buvo padarytos nusikalstamos veikos, numatytos LR BK 196 ar 197 straipsniuose, tačiau nebuvo padaryta didelė žala, baudžiamoji atsakomybė gali kilti pagal LR BK $198^{(1)}$ straipsnį (juk paprastai nusikaltimai, už kuriuos atsakomybė numatyta 196, 197 straipsniuose, daromi prisijungiant prie kompiuterio ar kompiuterinio tinklo). Manyčiau, jog „didelės žalos“ problema turėtų būti išspręsta, į 196 ir 197 straipsnius įvedant papildomas straipsnių dalis, kuriose didelė žala būtų numatyta kaip kvalifikuojantis požymis.

Ir vis tik, įvertinęs tai kas pasakyta, manau, jog 198(1) straipsnio sudėtis turėtų būti inkorporuota į kitas nusikaltimų informatikai sudėtis (į 196 – 198 straipsnius, o pastaruosiuose straipsniuose numatyti nusikalstami veiksmai numatomi kaip materialios pasekmės: pavyzdžiui, vietoje veiksmo "sunaikinti kompiuterinę informaciją" – pasekmė "informacijos sunaikinimas") – tai yra „grynasis" neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo neturėtų būti išskirtas kaip atskira nusikalstama veika. *Visų pirma*, kaip jau minėta, „kompiuterinis įsilaužimas" yra tik priemonė kitiems nusikaltimams informatikos sferoje daryti ir visiškai neįtikėtina, jog pavykus pašalinti kompiuterines apsaugas ir prisijungti prie kompiuterio, tuo bus apsiribota (bet kuriuo atveju bus pradėtas daryti poveikis kompiuterinei informacijai – t.y. nusikaltimai, numatyti BK 196 – 198 straipsniuose, nes pažeidus apsaugas, informacija lieka neapsaugota ir pažeidžiama). Tai reiškia, jog kompiuterinė sistema yra saugi, kol ji yra apsaugota techniniais ir programinės įrangos tam tikrais sprendimais. Šias apsaugos priemones pašalinus, nebelieka jokių kliūčių daryti poveikį kompiuterinei informacijai – prisijungimo prie kompiuterio ar kompiuterinio tinklo tikslai gali būti pradėti realizuoti. *Kita vertus*, paties „grynojo prisijungimo" kompiuterio ar kompiuterinio tinklo administratorius net nepastebės, kol nebus pradėtas daryti poveikis informacijai (pagrindinis informacijos kopijavimo, naikinimo, keitimo ir kitokio poveikio signalas yra tinklo neįprastai aukštas apkrovimo lygis, kas ir paskatina administratorių ieškoti to priežasčių). Pati operacinė sistema savęs taip pat negali kontroliuoti – pažeidus apsaugos priemones, bet koks poveikis kompiuterinei informacijai operacinės sistemos bus traktuojamas kaip sankcionuotas. Taigi nerealu tikėtis, jog kompiuterinis įsibrovėlis bus užkluptas ir identifikuotas „prisijungimo" stadijoje, kai faktiškai visi procesai kompiuteryje ar kompiuteriniame tinkle vyksta ordinariai - pagal įprastą tvarka, be jokių trikdžių. Yra daug priežasčių, kodėl Lietuvoje pradėtų ikiteisminių tyrimų nusikaltimų informatikai srityje užregistruojama labai mažai, tačiau akivaizdu, jog LR BK 198(1) straipsnis, sukonstruotas remiantis grynai teoriniais samprotavimais, taip ir liks „socialiai neveikiantis".

2001-11-23 d. Europos konvencijos dėl elektroninių nusikaltimų (Lietuvos Respublikoje ratifikuota 2004-01-22) 2 straipsnyje „Neteisėta prieiga" teigiama, jog „Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą prieigą prie visos kompiuterinės sistemos arba jos dalies. Šalis gali reikalauti, kad toks nusikaltimas būtų padarytas pažeidžiant apsaugos priemones, ketinant gauti kompiuterinius duomenis ar turint

kitą nesąžiningą ketinimą [...]“. Kaip matome, konvencijos autoriai taip pat kalba tik apie tokią sąmoningą ir neteisėtą prieigą, kuri realizuota „pažeidžiant apsaugos priemones, ketinant gauti kompiuterinius duomenis ar turint kitą nesąžiningą ketinimą“. Taigi konvencijos autoriai paties neteisėto prisijungimo prie kompiuterio ar kompiuterinio tinklo nekriminalizuoja, ir kalba apie materialiąją tokio nusikaltimo sudėtį.

Mano manymu, neteisėtą prisijungimą prie kompiuterio ar kompiuterinio tinklo derėtų inkorporuoti į kitų nusikaltimų informatikai sudėtis, ir to pasėkoje, “grynąją” neteisėtą prieigą reikėtų vertinti kaip pasikėsinimą padaryti nusikalstamas veikas, numatytas LR BK 196 - 198 straipsniuose.

Pagal galiojantį BK, tiesioginis neteisėto prisijungimo prie kompiuterio ar kompiuterinio tinklo objektas yra visuomeniniai santykiai, susiję su kompiuterinės informacijos saugumu bei normalaus kompiuterių/kompiuterinio tinklo darbo užtikrinimu. Papildomas objektas yra nuosavybė (kompiuterinė informacija, saugoma materialioje laikmenoje, – tai objektas, dalyvaujantis turtinių mainų santykiuose). Šio nusikaltimo dalykas, kaip materiali teisinio gėrio išraiška materialiame pasaulyje, kurį veikiant nusikalstamu būdu daroma žala (arba kyla žalos grėsmė) teisiniam gėriui yra *kompiuterinė informacija*. LR BK $198^{(1)}$ straipsnyje numatyto nusikaltimo sudėtis yra formalioji – t.y. nusikalstamos veikos kvalifikavimui pakanka tik subjekto veikimo (prisijungimo prie kompiuterio ar kompiuterinio tinklo, pažeidžiant apsaugos priemones), o nusikalstamos veikos pasekmės nereikalingos. Šiuo atveju įstatymo leidėjas konstruodamas nusikaltimo sudėtį apsiribojo tik nusikalstamos veikos aprašymu, o jos pasekmes paliko už nusikaltimo sudėties ribų, o tai reiškia, jog nusikaltimo baigtumui pakanka tik pačios veikos atlikimo.

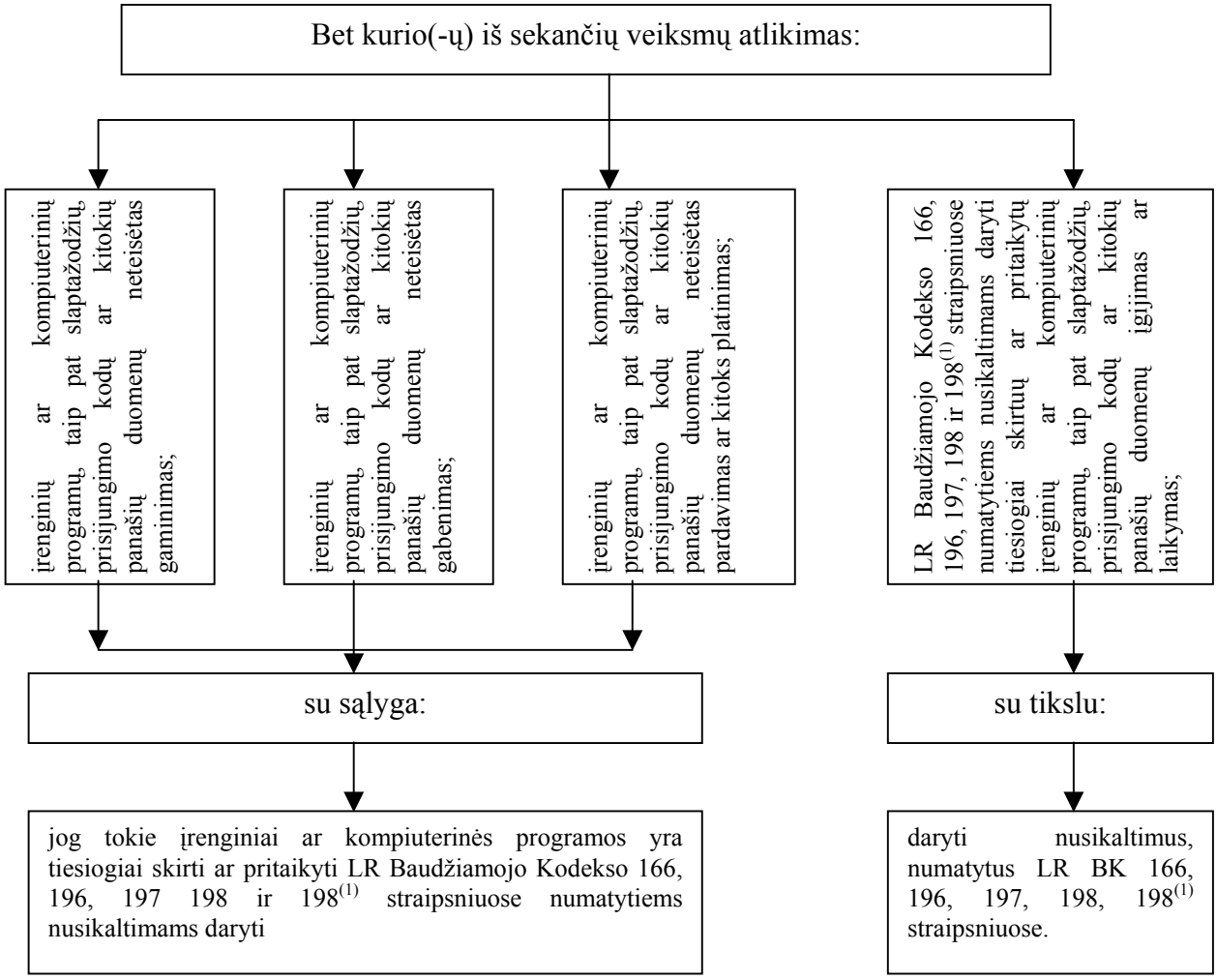
Šio nusikaltimo subjektyviajai pusei būdinga kaltės forma yra tyčia. Santykyje su veika veikiantysis subjektas veikia tiesiogine tyčia (kadangi nusikaltimo sudėtis yra formalioji, veikiančiojo subjekto santykis su pasekmėmis neakcentuojamas). Nusikaltimo numatyto LR BK $198^{(1)}$ straipsnyje subjektu gali būti bet kuris fizinis asmuo, sulaukęs 16 metų amžiaus, ir atitinkantis subjektyviosios pusės pakaltinamumo požymį. Šio straipsnio antrojoje dalyje pasakyta, kad už šią veiką atsako ir juridinis asmuo (juridinio asmens baudžiamoji atsakomybė reglamentuota BK 20 ir 43 straipsniuose). Šią nusikalstamą veiką gali padaryti ir specialusis subjektas, turintis teisę dirbti su dalimi kompiuteryje ar kompiuteriniame tinkle esančios informacijos, jeigu jis bando prisijungti prie tų kompiuterinės informacijos resursų, su kuriais neturi teisės dirbti.

Sankcijoje už neteisėtą prisijungimą prie kompiuterio ar kompiuterinio tinklo alternatyviai numatytos šios bausmės: viešieji darbai arba bauda, arba areštas, arba laisvės atėmimas iki vienerių metų (bausmių rūšys juridiniams asmenims, kaip minėta, numatytos BK 43 straipsnyje). LR BK $198^{(1)}$ straipsnyje numatytas nusikaltimas yra nesunkus, už kurį nustatyta penkerių metų apkaltinamojo nuosprendžio priėmimo senatis.

2.4.2. LR BK 198(2) straipsnio „Neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti“ baudžiamoji teisinė analizė

2004-01-29 d., įsigaliojus naujojo LR BK pakeitimams, XXX skyrius buvo papildytas 198(2) straipsniu. Šis straipsnis teigia, jog nusikalstamai veikia: „1. Tas, kas neteisėtai gamino, gabeno, pardavė ar kitaip platino šio Kodekso 166, 198 ir 198(1) straipsniuose numatytiems nusikaltimams daryti tiesiogiai skirtus ar pritaikytus įrenginius ar kompiuterines programas, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis arba turėdamas tikslą daryti tuos nusikaltimus juos įgijo ar laikė, 2. Tas, kas neteisėtai gamino, gabeno, pardavė ar kitaip platino šio Kodekso 196 ar 197 straipsniuose numatytiems nusikaltimams daryti tiesiogiai skirtus ar pritaikytus įrenginius ar kompiuterines programas, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis arba turėdamas tikslą daryti tuos nusikaltimus juos įgijo ar laikė“. Taip pat šiame straipsnyje numatyta, jog už tokią veiką baudžiamąja tvarka atsako ir juridinis asmuo.

Nusikaltimo, numatyto LR BK 198(2) straipsnyje, objektyviosios pusės grafinė išraiška.



Nesunkiai pastebėsime, kad BK 198(2) straipsnio pirma ir antra dalys skiriasi sankcijos dydžiu (antrojoje dalyje numatyta kvalifikuota šio nusikaltimo sudėtis ir bausmė yra griežtesnė, nors abi veikos priskirtos prie nesunkių nusikaltimų). Šių dviejų straipsnio dalių dispozicijos skiriasi tik vienu aprašomuoju požymiu – t.y. jos išskirtos pagal tai, kokių nusikaltimų darymo tikslu buvo įvykdyta šiame straipsnyje numatyta nusikalstama veika: pirmoje dalyje visi/kai kurie išvardinti nusikalstami veiksmai turėtų būti atlikti su tikslu daryti nusikaltimus, numatytus LR BK 166, 198 ir 198(1) straipsniuose, tuo tarpu antrojoje dalyje išvardinti nusikalstami veiksmai turėtų būti atlikti su tikslu daryti nusikaltimus, numatytus šio Kodekso 196 ar 197 straipsniuose. Kaip matome, pirmojoje 198(2) straipsnio dalyje baudžiamoji atsakomybė numatyta ne tik dėl siekio daryti kitus nusikaltimus informatikos sferoje, bet ir už vieną iš nusikaltimų asmens privataus gyvenimo neliečiamumui – t.y. už BK 166 straipsnyje numatytą neteisėtą susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimą.

Pastaruoju metu ir Lietuvoje elektroniniu paštu masiškai plinta „kompiuteriniai virusai“ (programavimo teorijoje tai tokia skaitmeninių kodų visuma, kuri pati gali sukurti savo kopijas, pastarosios, savo ruožtu, irgi gali daugintis, ir įterpti į operacinės sistemos failų visumą kompiuteryje ar serveryje. Be to, tos kopijos nebūtinai būna identiškos originalui – jos gali tapti pranašesnės už savo „motiną“, įgyti naujų savybių ir panašiai). Dažnai tokiu būdu platinami virusai „Trojos arkliai“, “vikšrai” galintys padėti užvaldyti kompiuterinę sistemą. Internete yra begalė tinklapių (pvz.: www.astalavista.com), siūlančių už pinigus ar net veltui parsisiųsti slaptažodžių ir vartotojų vardų generatorių (kompiuterinių programų), programų, padedančių „nulaužti“ administratoriaus slaptažodį, „*key finder*“, „*Show password*“ir kt. Globalaus tinklo dėka, visa tai tapo prieinama visiems kompiuterių vartotojams. Akivaizdu, kad tokios kompiuterinės programos gaminamos, gabenamos, platinamos, įgyjamos ir laikomos ne savo kompiuterio ar kompiuterinio tinklo priežiūros tikslais. Nors, šioje vietoje būtų logiška paaiškinti 198(2) straipsnyje naudojamą sąvoką „neteisėtai“. Paradoksalu, tačiau analogiškas kompiuterines programas, įrenginius, prisijungimo kodus, kuriais būtų įmanoma daryti nusikaltimus informatikai, galima gaminti ir teisėtai. Pavyzdžiui, antivirusinių programų, operacinių sistemų kūrėjai visa tai gali gaminti (samdyti netgi hakerius), tikslu patikrinti savo sukurto, kompiuterinės sistemos apsaugai skirto produkto saugumui („Microsoft“ korporacija tikrai Internete yra buvusi paskelbusi, jog sumokės šešiaženklę sumą

asmeniui, įsilaužusiam į jų duomenų bazę ir paaiškinusiam, kaip jam tai pavyko). Jeigu tokie sukurti baudžiamojo įstatymo draudžiami techniniai ir programiniai įrankiai tebus naudojami tik tokiam tikslui ir dar įgaliojimus turinčių asmenų, tai nebus traktuojama kaip nusikalstama veika. Europos Tarybos Elektroninių nusikaltimų konvencijos 6 straipsnio 2 dalyje teigiama: „[...] Šis straipsnis negali būti aiškinamas kaip užtraukiantis baudžiamąją atsakomybę kai šio straipsnio 1 dalyje minimas gaminimas, pardavimas, įsigijimas naudoti, įvežimas, platinimas ir kitoks galimybės naudotis suteikimas arba turėjimas nėra skirtas daryti nusikaltimui, apibūdintam šios Konvencijos 2–5 straipsniuose, o tik sankcionuotam kompiuterinės sistemos tikrinimui arba jos apsaugai“.

LR BK $198^{(2)}$ straipsnyje kalbama ne tik apie nusikalstamais tikslais naudojamas kompiuterines programas, bet ir apie įrenginius, tiesiogiai skirtus ar pritaikytus, minėtiems nusikaltimams daryti. Neatsitiktinai $198^{(2)}$ straipsnio 1 dalyje kalbama ir apie BK 166 straipsnyje numatytą nusikalstamą veiką. Kita vertus, reikia turėti omenyje, jog kompiuterinė informacija saugoma ne tik aukščiau išvardintose informacijos laikmenose, ne tik kompiuterio atmintyje (standžiajame diske, kuris yra kompiuterio sudedamoji dalis, tiesiogiai sujungta su procesoriumi, ir kurioje ne tik saugoma vartotojo sukurta informacija, bet ir tie duomenys, kurie tiesiogiai dalyvauja procesoriaus atliekamose operacijose). Kompiuterinė informacija yra mainų objektas – taigi ji gali būti perduodama ir telekomunikaciniais kanalais iš vieno įrenginio į kitą. Telekomunikaciniai kanalai su atitinkama programine įranga sujungia atskirus kompiuterius ir periferinius įrenginius į tinklą. Taigi kompiuterinė informacija gali būti mobili, ir, reikėtų pabrėžti, jog perdavimo komunikaciniais kanalais metu ji tampa ypač pažeidžiama. Specialios įrangos pagalba, tokia „migruojanti“ informacija gali būti perimta (neatsitiktinai, saugantis tokio perėmimo, kuriami intranetai (vidiniai tinklai), specialiosios/atskirosios komunikacinės linijos ir panašiai).

LR BK $198^{(2)}$ straipsnio sudėtį įstatymų leidėjas sukonstravo kaip formaliąją – t.y. pakanka nustatyti patį faktą, jog asmuo pagamino, gabeno ar platino įrenginius, kompiuterines programas, slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis, ir, kad tokia produkcija yra tiesiogiai skirta ar pritaikyta LR Baudžiamojo Kodekso 166, 196, 197 198 ir $198^{(1)}$ straipsniuose numatytiems nusikaltimams daryti. Čia nebūtinos kokios nors socialiai neigiamos pasekmės. Netgi nesvarbu, ar tokios produkcijos pagalba buvo padaryti minėti nusikaltimai kibernetinėje erdvėje, ir ar nusikaltimo subjektas turėjo tikslą padaryti tokius nusikaltimus ateityje (kalbama tik apie galimybę daryti nusikaltimus informatikai

tokios produkcijos pagalba). Tuo tarpu, kalbėdamas apie minėtos produkcijos įgijimą ir laikymą, įstatymų leidėjas į nusikaltimo sudėtį įtraukia vieną subjektyviosios pusės požymį – tikslo turėjimą daryti aukščiau minėtus nusikaltimus kibernetinėje erdvėje tokių produktų pagalba. Savaime suprantama, jog tyrėjams, atliekantiems ikiteisminį tyrimą, visais atvejais yra nelengva įrodinėti subjektyviųjų požymių egzistavimą nusikalstamos veikos procese. Nusikalstamos veikos subjektas daugeliu atveju ir laikysis versijos, jog jis tik įgijo ir laikė tokio pobūdžio kompiuterines programas, įrenginius ar prisijungimo kodus, nors ir neturėjo tikslo daryti nusikaltimus informatikos srityje (tokios produkcijos gamybą ir platinimą paneigti būtų sunkiau, nes kaip taisyklė egzistuoja kiti įrodymai, tačiau tik gabenimas visada gali sėkmingai būti „transformuotas“ į įgijimą, laikymą).

Šiame straipsnyje nekalbama apie nelegalios/piratinės programinės įrangos naudojimą, panaudojant slaptažodžius, kodus ir panašiai – visa tai paliekama XXIX skyriaus „Nusikaltimai intelektinei ir pramoninei nuosavybei“ reglamentavimui.

Neteisėto disponavimo įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti objektas yra visuomeniniai santykiai, susiję su kompiuterinės informacijos bei normalaus kompiuterių/kompiuterinio tinklo darbo užtikrinimu. Šio nusikaltimo dalykas, kaip materiali teisinio gėrio išraiška materialiame pasaulyje, kurį veikiant nusikalstamu būdu daroma žala (arba kyla žalos grėsmė) teisiniam gėriui yra *kompiuterinė informacija*.

Šio nusikaltimo subjektyviajai pusei būdinga kaltės forma yra tyčia. Santykyje su veika veikiantysis subjektas veikia tiesiogine tyčia (kadangi nusikaltimo sudėtis yra formalioji, veikiančiojo subjekto santykis su pasekmėmis neakcentuojamas.

Nusikaltimo numatyto LR BK $198^{(2)}$ straipsnyje subjektu gali būti bet kuris fizinis asmuo, sulaukęs 16 metų amžiaus, ir atitinkantis subjektyviosios pusės pakaltinamumo požymį. Šio straipsnio antrojoje dalyje pasakyta, kad už šią veiką atsako ir juridinis asmuo (juridinio asmens baudžiamoji atsakomybė reglamentuota BK 20 ir 43 straipsniuose).

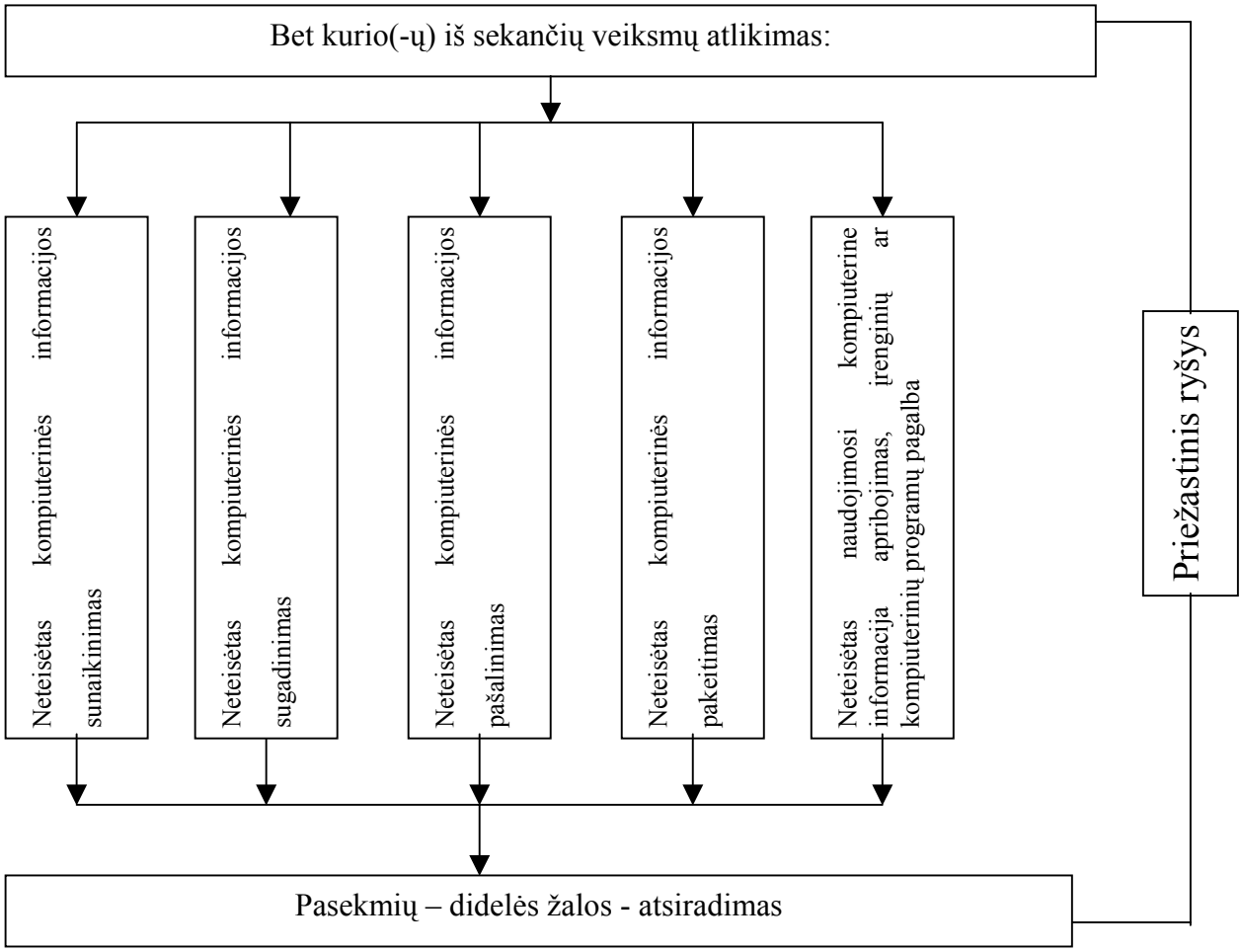
LR BK $198^{(2)}$ straipsnio 1 d. sankcijoje alternatyviai numatytos šios bausmės: viešieji darbai arba bauda, arba areštas, arba laisvės atėmimas iki vienerių metų (bausmių rūšys juridiniams asmenims, kaip minėta, numatytos BK 43 straipsnyje). LR BK $198^{(2)}$ straipsnio 2 d. alternatyviai numatytos bausmės yra: viešieji darbai arba bauda, arba areštas, arba laisvės atėmimas iki trejų metų. Šiame straipsnyje aprašytos veikos priskirtos prie nesunkių nusikaltimų. Kalbant apie BK $198^{(2)}$ straipsnio kvalifikuotąją sudėtį, akivaizdu, kad

disponavimas įrenginiais ar programomis skirtomis sunaikinti kompiuterių programoms ar informacijai yra pavojingesnė veika, nei disponavimas įrenginiais ar programomis, skirtais neteisėtai prisijungti prie tinklo.

2.4.3.LR BK 196 str. „Kompiuterinės informacijos sunaikinimas ar pakeitimas“ baudžiamoji teisinė analizė

Šis straipsnis tokiame būvyje, koks yra ir šiandien, galioja nuo 2003-05-01 d. (t.y. nuo naujojo LR Baudžiamojo Kodekso įsigaliojimo dienos). LR BK 196 straipsnyje teigiama, jog nusikalstamai veikia tas, kas, „neteisėtai sunaikino, sugadino, pašalino ar pakeitė kompiuterinę informaciją arba įrenginiais ar kompiuterinėmis programomis apribojo naudojimąsi tokia informacija padarydamas didelės žalos“. Antrojoje straipsnio dalyje nustatyta, jog už tokią nusikalstamą veiką atsako ir juridinis asmuo.

Nusikaltimo, numatyto LR BK 196 straipsnyje, objektyviosios pusės grafinė išraiška.



„Kompiuterinės informacijos sunaikinimas ar pakeitimas“ – tai bene aiškiausiai suformuluota nusikaltimų informatikai sudėtis, nes faktiškai visi 196 straipsnyje išvardinti alternatyvūs nusikalstami veiksmai turi atitikmenis realiame gyvenime, jeigu kompiuterinę informaciją lygintume su fiziniais aplinkos daiktais.

Mes sąvoką „neteisėtas“ aptarėme analizuodami kitų nusikaltimų kibernetinėje erdvėje sudėtis, todėl nebesikartosime.

Kompiuterinės informacijos sunaikinimas, sugadinimas, pašalinimas, pakeitimas, naudojimosi ja apribojimas – tai tie negatyvūs nusikaltimo subjekto veiksmai, kuriais siekiama teisėtiems kompiuterinės informacijos vartotojams atimti galimybę tokią informaciją naudoti pagal paskirtį. Tačiau šiais veiksmais nusikaltimo subjektas pats taip pat neįgyja galimybės, kad ir neteisėtai naudotis tokia informacija jis informacijos neperima, bet tik sunaikina (arba padaro kitokį aukščiau įvardintą negatyvų poveikį kompiuterinei informacijai). Europos Tarybos konvencijos dėl elektroninių nusikaltimų 4 straipsnyje „Poveikis duomenims“ teigiama: „Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterinių duomenų sugadinimą, sunaikinimą, apgadinimą, pakeitimą arba galimybės naudotis tokiais duomenimis panaikinimą“. LR BK 196 straipsnyje beveik pažodžiui atkartota tokio nusikaltimo sudėtis.

Tačiau kaip nekeista, vadovaujantis LR BK, kompiuterinės informacijos (išskyrus įstatymų saugomą informaciją apie fizinį ar juridinį asmenį) pasisavinimas/kopijavimas negalėtų būti priskirtas prie nusikalstamų veikų kibernetikos srityje, nors Europos Tarybos konvencijos dėl elektroninių nusikaltimų 3 straipsnyje „Neteisėta perimtis“ teigiama: „Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą neviešo kompiuterinių duomenų perdavimo į kompiuterinę sistemą, iš jos ir jos viduje perimtį techninėmis priemonėmis, taip pat už elektromagnetinės emisijos iš kompiuterinės sistemos, perduodančios tokius kompiuterinius duomenis, perimtį“. Mano galva, šio konvencijos dėl elektroninių nusikaltimų reikalavimo įvykdymas visai paprastas – užtektų praplėsti nusikalstamų veiksmų baigtinį sąrašą LR BK 196 straipsnyje (t.y. šalia kompiuterinės informacijos sunaikinimo, pakeitimo ir kt., papildomai kriminalizuoti kompiuterinės informacijos perėmimą/kopijavimą).

Kompiuterinės programos, duomenų bazės yra autorių teisių gynimo objektai; įstatymų saugomos informacijos apie juridinį ar fizinį asmenį pasisavinimas užtraukia baudžiamąją atsakomybę pagal LR BK 198 straipsnį. Taigi šie informaciniai resursai atskiros apsaugos nuo neteisėto perėmimo nebereikalauja. Tačiau to negalima pasakyti apie kompiuterinę informaciją apskritai. Juk Europos tarybos konvencijoje dėl elektroninių

nusikaltimų ir kalbama apie kompiuterinę informaciją/kompiuterinius duomenis bendrąja prasme - „kompiuteriniai duomenys“ – tai bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat programa, pagal kurią kompiuterinė sistema gali vykdyti tam tikrą funkciją”. Galima drąsiai teigti, jog mūsų šalyje kompiuterinė informacija baudžiamąja prasme nėra pilnai apsaugota prisilaikant ES reikalavimų – informacijos kopijavimas/perimtis ir yra vienas iš esminių nusikaltimo informatikai aspektų, dėl kurio dažnu atveju praktikoje ir yra “įsilaužinėjama” į kompiuterius ar kompiuterių tinklus.

LR BK 196 straipsnyje numatyto nusikaltimo sudėtis yra materialioji. Įvykdžius alternatyvius(-ų) nusikalstamus(-ą) veiksmus(-ą) (kompiuterinės informacijos sunaikinimas, pakeitimas ir kt.), tam, kad jie butų kvalifikuojami kaip baigta nusikalstama veiką, reikalingos pasekmės – didelės žalos padarymas. “Didelė žala” kaip būtina pasekmė, atsiradusi priežastiniame ryšyje su nusikalstamų veiksmų padarymu, numatyta ne tik LR BK 196, bet ir 197 straipsnyje. Tačiau kokias aplinkybes atsiradusias nusikalstamos veikos realizavimo atveju reikėtų įvardinti kaip „didelę žalą“ lieka neaišku – LR BK 190 str. yra išaiškinta turto vertė, taikoma XXVIII skyriaus nusikaltimams; turto vertė yra atskirai išaiškinama ir kalbant apie kai kuriuos kitus nusikaltimus, pavyzdžiui, kyšininkavimą, papirkimą, kontrabandą. Nusikaltimų informatikai atveju „didelę žalą“ turbūt reikėtų suprasti ne vien kaip turtinę žalą, ir jos mastą, turbūt turėtų kiekvieną kartą įvertinti teismas, nagrinėjantis baudžiamąją bylą.

Vis tik nusikalstamų veikų kibernetinėje erdvėje specifika ir siekis vienodinti teismų praktiką reikalauja įstatyme pateikti labai abstrakčios sąvokos *„didelė žala”* išaiškinimą. Būtų tikslinga BK XXX skyrių papildyti dar vienu straipsniu, kuriame būtų atskleisti du šios sąvokos aspektai – turtinės ir neturtinės žalų turiniai. Ši LR BK atitinkamo skyriaus naujovė būtų vertinga todėl, kad, priešingu atveju, įvairių teismų bei ikiteisminio tyrimo institucijų neaiški juridinė definicija gali būti komentuojama nevienodai. Kita vertus, suprantama, jog įstatymų leidėjui sudėtinga detalizuoti vertinamąjį *didelės žalos* požymį. Šios sąvokos turinys galėtų būti atskleistas teismų praktikoje. Tačiau akivaizdu, kad šią situaciją palikus teismų praktikos formavimosi procesui, didelės žalos samprata kristalizuosis pakankamai ilgą laiką, neišvengiant klaidų, nevienodo veikų kvalifikavimo Lietuvos teismuose.

Kadangi „didelės žalos“ samprata dar neišsirutuliojo, sudėtinga kalbėti apie situaciją, kai aukščiau išvardintais nusikalstamais veiksmais „didelė žala“ nepadaroma. Manytina, kad tokia situacija turėtų būti kvalifikuojama kaip pasikėsinimas padaryti nusikalstamą veiką

pagal LR BK 196 ar 197 straipsnį (t.y. papildomai kvalifikuojama pagal BK 22 straipsnį).

Objektyviąją šio nusikaltimo sudėties pusę sudaro neteisėta prieiga prie kompiuterinės informacijos, ko pasėkoje kompiuteriniai duomenys/kompiuterinė informacija yra sunaikinama ar kitokiu BK 196 straipsnyje numatytu būdu paveikiama.

Tiesioginis šio nusikaltimo objektas yra visuomeniniai santykiai, susiję su saugiu kompiuterinės informacijos naudojimu bei informacijos apsauga. Dalykas – kompiuterinė informacija.

LR BK 196 straipsnyje numatyta baudžiamoji atsakomybė tik už poveikį kompiuterinei informacijai – tai yra informacijai, esančiai kompiuterinėje laikmenoje, kompiuteryje arba kompiuteriniame tinkle (tame tarpe ir duomenų perdavimo kanaluose).

Informacija, ranka užrašyta ant popieriaus, atspausdinta rašomąja mašinėle ar spausdintuvu nebus laikoma tokio nusikaltimo dalyku.

Nusikalstamos veikos baigimo momentas yra veikiančiojo subjekto veiksmas, kuriuo jis duoda neteisėtai naudojamam kompiuteriui komandą sunaikinti, pakeisti (ir t.t.) kompiuterinę informaciją/jos dalį, nepriklausomai nuo dėl tokio veiksmo atsirasiančių pasekmių. Tačiau tam, kad tokią veiką būtų galima pripažinti nusikaltimu, numatytu LR BK 196 straipsnyje, kaip minėta, reikalingos pasekmės – didelė žala.

Negatyvus poveikis informacijai (sunaikinimas, pakeitimas, prieigos prie jos blokavimas ir pan.) – tai toks jos būvio pakeitimas, kai ji netenka visų/dalies savo charakteristikų, kokybinių požymių. Tas faktas, jog teisėtas kompiuterinės informacijos vartotojas turi galimybę tokią negatyviai paveiktą informaciją atstatyti (specialios programinės įrangos pagalba ar gauti ją iš kitų informacijos šaltinių), nusikaltimo subjekto neatleidžia nuo baudžiamosios atsakomybės.

Kalbant apie subjektyviąją tokio nusikaltimo pusę, reikia pabrėžti, jog kaltės forma galima tik tyčia. Santykyje su veika, nusikaltimo subjektas gali veikti tik tiesiogine tyčia, ką liudija ir įstatymo leidėjo naudojama sąvoka „neteisėtai“. Tačiau santykyje su nusikalstamos veikos sąlygotomis pasekmėmis nusikaltimo subjektas gali veikti tiek tiesiogine, tiek netiesiogine tyčia (šių sąvokų turinys yra išaiškintos LR BK 15 straipsnyje).

Kalbant apie nusikalstamos veikos sąlygotas teisines pasekmes, pabrėžtina, jog ikiteisminio tyrimo pareigūnai visais atvejais turėtų aiškintis, ar nusikaltimo subjektas norėjo, jog atlikus BK 196 straipsnyje numatytus veiksmus, būtų padaryta didelė žala. Šioje vietoje dar kartą verta užsiminti apie teisinės sąvokos „didelė žala“ aiškumo stoką ir tokios situacijos

pašalinimo būtinybę. Kadangi baudžiamosios teisės normos atlieka ir informacinį/prevencinį/auklėjamąjį vaidmenį sociumo narių atžvilgiu, būtina aiškiai nustatyti, koks veikos mastas laikytinas ypatingai pavojingu visuomenei, ir koks veikos mastas užtraukia griežčiausią baudžiamąją atsakomybę.

Mano manymu, „didelės žalos“ (šią sąvoką tinkamai apibrėžus) atsiradimas turėtų būti vertinamas kaip nusikalstamą veiką kvalifikuojantis požymis ir tokias pasekmes sukėlusi veika išskirta į atskirą straipsnio dalį, tuo tarpu pirmąsias BK 196, 197 straipsnių dalis suformuluojant kaip formaliąsias nusikaltimų sudėtis.

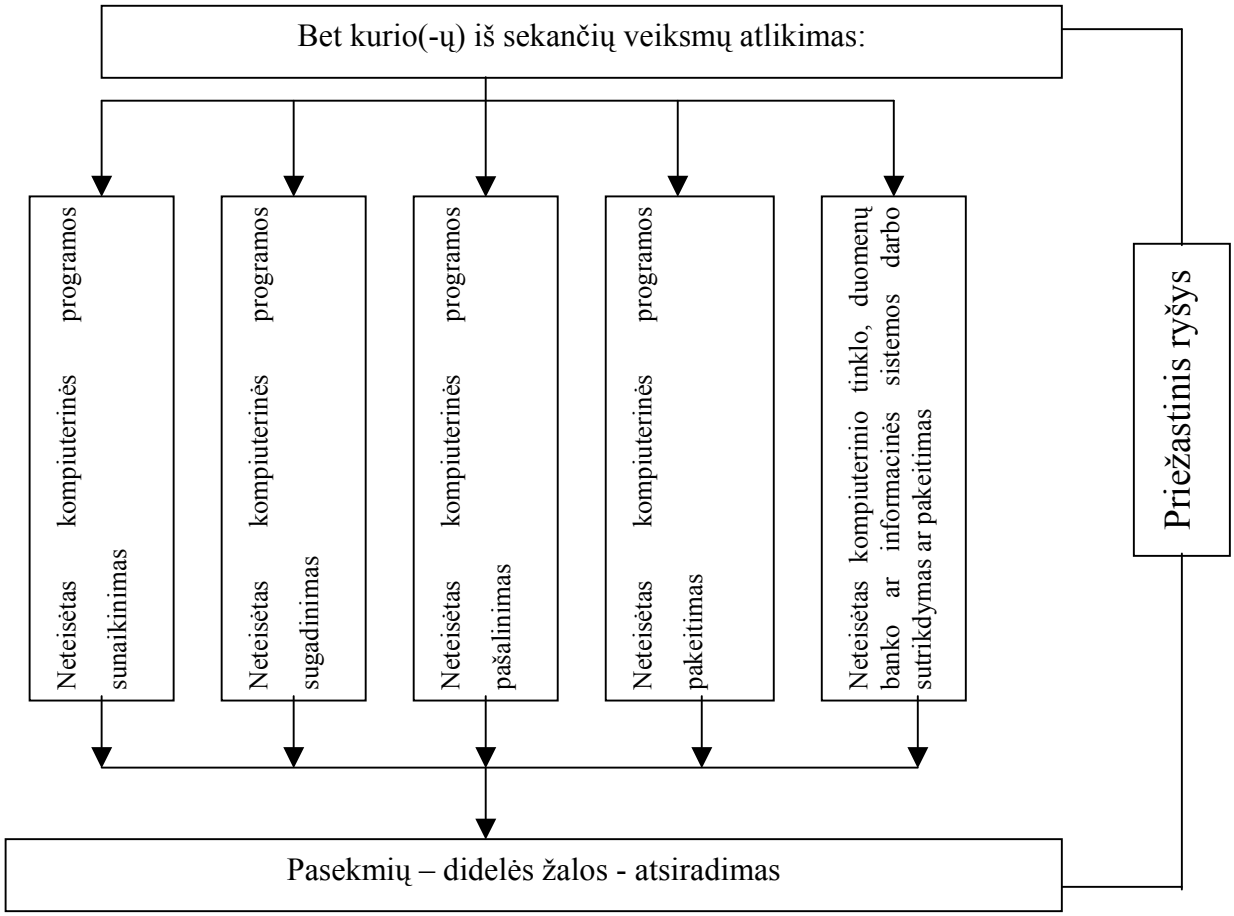
Nusikaltimo subjektu gali būti bet koks fizinis asmuo, sulaukęs 16 metų amžiaus, ir atitinkantis pakaltinamumo požymį. Subjektu gali būti ir teisėtas kompiuterinės informacijos vartotojas, neturintis teisės dirbti su tam tikro lygio informacija. Subjektas gali būti tiek bendrinis, tiek specialusis. Kaip minėta aukščiau, dėl šios nusikalstamos veikos baudžiamojon atsakomybėn gali būti traukiamas ir juridinis asmuo.

Atsižvelgiant į tai, kad BK 196 ir 197 straipsnių normos savo paskirtimi ir sankcijomis yra panašios, manau, būtų tikslinga šiuos straipsnius apjungti į vieną baudžiamojo kodekso straipsnį. Nors, LR BK 196 ir 197 straipsniai numato skirtingą nusikalstamos veikos dalyką: kompiuterinę informaciją (196 str.) ir kompiuterines programas (197 str.), būtų logiška formuluoti šį straipsnį su dviem savo prigimtimi panašiais dalykais – kompiuterinė programa taip pat yra kompiuterinė informacija, talpinanti savyje papildomas funkcijas: kompiuterinė programa yra tie kompiuteriniai duomenys, kurie tiesiogiai dalyvauja procesoriaus atliekamose operacijose. Autorių teisių ir gretutinių teisių įstatymo 2 straipsnio 17 dalyje teigiama: “Kompiuterių programa – žodžiais, kodais, schemomis ar kitu pavidalu pateikiamų instrukcijų, kurios sudaro galimybę kompiuteriui atlikti tam tikrą užduotį ar pasiekti tam tikrą rezultatą, visuma, kai tos instrukcijos pateikiamos tokiomis priemonėmis, kurias kompiuteris gali perskaityti; ši sąvoka apima ir parengiamąją projektinę tokių instrukcijų medžiagą, jeigu pagal ją galima būtų sukurti minėtą instrukcijų visumą”.

2.4.4.LR BK 197 str. „Kompiuterinės programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas“ baudžiamoji teisinė analizė

Šis straipsnis tokiame būvyje, koks yra ir šiandien, galioja nuo 2003-05-01 d. (t.y. nuo naujojo LR Baudžiamojo Kodekso įsigaliojimo dienos). LR BK 197 straipsnyje teigiama, jog nusikalstamai veikia tas, kas, „neteisėtai sunaikino, sugadino, pašalino ar pakeitė kompiuteryje esančią programą arba sutrikdė ar pakeitė kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbą padarydamas didelės žalos“. Antrojoje straipsnio dalyje nustatyta, jog už tokią nusikalstamą veiką atsako ir juridinis asmuo.

Nusikaltimo, numatyto LR BK 197 straipsnyje, objektyviosios pusės grafinė išraiška.



Atidžiau pažvelgę į straipsnio pavadinimą ir į jo dispoziciją, pastebėsime, jog formuluotės skiriasi. Pavadinimas skamba taip: „Kompiuterinės programos sunaikinimas ar pakeitimas *ir* kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo

sutrikdymas“, tuo tarpu dispozicijoje lygtai viskas sudėliota į savas vietas: „tas, kas neteisėtai sunaikino, sugadino, pašalino ar pakeitė kompiuteryje esančią programą *arba* sutrikdė ar pakeitė kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbą [...]“. Tokiu principu (panaudojant jungtuką „ir“) formuluoti straipsnio pavadinimą, manyčiau, būtų korektiška vieninteliu atveju – jeigu dvi veikos (pirma – kompiuterinės programos sunaikinimas ar pakeitimas; antra – kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas) būtų išdėstytos skirtingose to paties straipsnio dalyse. Žinoma, nusikalstama veika yra kvalifikuojama ne pagal straipsnio pavadinimą, o pagal teisės normos dispoziciją. Vis tik tokių neatitikimų, mano galva, baudžiamųjų įstatymų sąvade neturėtų būti. Galbūt tai liudija apie nepakankamą įstatymo kūrėjų dėmesingumą.

Magistro baigiamajame darbe jau buvo išreikšta nuomonė, jog derėtų apjungti LR BK 196 ir 197 straipsnius. Šioje darbo dalyje nebeplėtosime tos pačios minties ir argumentacijos. Daugelis minėtuose straipsniuose naudojamų juridinių definicijų kartojasi, todėl šioje rašto darbo dalyje jos nebus analizuojamos iš naujo (tokios sąvokos kaip „neteisėtas“, „didelė žala“).

Nusikaltimas, numatytas LR BK 197 straipsnyje, yra padaromas alternatyviais veiksmais – sunaikinant, sugadinant, pašalinant, pakeičiant kompiuterinę programą, taip pat sutrikdant arba pakeičiant kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbą. Iš esmės šio straipsnio dispozicija yra analogiška 196 straipsnio dispozicijai – skiriasi tik dalykas (196 str. kalbama apie kompiuterinę informaciją, 197 str. – apie kompiuterinę programą). Tiesa, kompiuterinio tinklo ar duomenų bazės darbo sutrikdymas ar pakeitimas gali būti padaromas ir kitais veiksmais (nebūtinai neteisėtai vienu iš dispozicijoje išvardintų būdų paveikiant kompiuterinę programą). Tai gali būti padaroma, kad ir perdėm apkraunant kompiuterinio tinklo darbą (masiškai siuntinėjami elektroniniai laiškai ir pan. Su tokia problema buvo susidūrę tinklapio www.yahoo.com administratoriai).

Tiesioginis šio nusikaltimo objektas yra visuomeniniai santykiai, susiję su saugiu kompiuterių programinės įrangos naudojimu, bei informacijos apsauga. Dalykas – kompiuterinė programa, kompiuterinis tinklas, duomenų bankas, informacinė sistema.

Nusikalstamos veikos baigimo momentas yra veikiančiojo subjekto veiksmas, kuriuo jis duoda neteisėtai naudojamam kompiuteriui komandą sunaikinti, pakeisti (ir t.t.) kompiuterinę programą/jos dalį, nepriklausomai nuo dėl tokio veiksmo atsirasiančių pasekmių. Tačiau tam, kad tokią veiką būtų galima pripažinti nusikaltimu, reikalingos

pasekmės – didelė žala.

Negatyvus poveikis kompiuterinei programai (sunaikinimas, pakeitimas, ir pan.) – tai toks jos būvio pakeitimas, kai ji netenka visų/dalies savo charakteristikų, kokybinių požymių. Tas faktas, jog teisėtas kompiuterinės programos vartotojas turi galimybę tokią negatyviai paveiktą programą atstatyti, nusikaltimo subjekto neatleidžia nuo baudžiamosios atsakomybės.

Kalbant apie subjektyviąją tokio nusikaltimo pusę, reikia pabrėžti, jog kaltės forma galima tik tyčia. Santykyje su veika, nusikaltimo subjektas gali veikti tik tiesiogine tyčia, ką liudija ir įstatymo leidėjo naudojama sąvoka „neteisėtai“. Tačiau santykyje su nusikalstamos veikos sąlygotomis pasekmėmis nusikaltimo subjektas gali veikti tiek tiesiogine, tiek netiesiogine tyčia.

Nusikaltimo subjektu gali būti bet koks fizinis asmuo, sulaukęs 16 metų amžiaus ir atitinkantis subjektyviosios nusikaltimo sudėties pusės pakaltinamumo požymį. Subjektu gali būti ir teisėtas kompiuterinės informacijos vartotojas, neturintis teisės dirbti su tam tikro lygio informacija bei programomis. Subjektas gali būti tiek bendrinis, tiek specialusis. Kaip minėta aukščiau, dėl šios nusikalstamos veikos baudžiamojon atsakomybėn gali būti traukiamas ir juridinis asmuo.

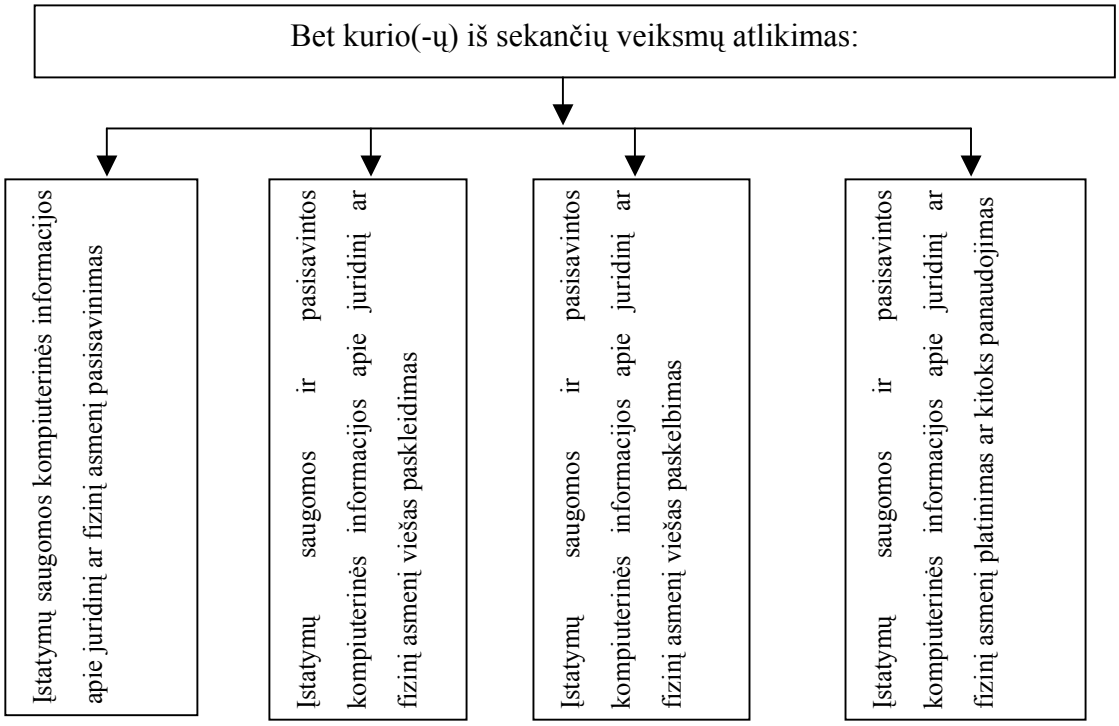
Manau, jog BK 197 straipsnio 1 dalies redakcija ne visiškai atitinka Konvencijos dėl elektroninių nusikaltimų nuostatas. Pagal BK 197 straipsnį reikalaujama, kad veika būtų padaroma didelė žala, tačiau Konvencijos dėl elektroninių nusikaltimų 5 straipsnis, numatantis įpareigojimą nustatyti baudžiamąją atsakomybę už tyčinį pavojingą kompiuterinės sistemos darbo trukdymą, nenumato galimybės apriboti šių nuostatų taikymą tik esant „didelės žalos“ požymiui.

Kadangi, kaip jau minėta, BK 196 ir 197 straipsnių dispozicijos yra labai panašios, nebesileisime į gilesnę šio straipsnio analizę.

2.4.5. LR BK 198 str. „Kompiuterinės informacijos pasisavinimas ir skleidimas“ baudžiamoji teisinė analizė

Šis straipsnis tokiame būvyje, koks yra ir šiandien, galioja nuo 2003-05-01 d. (t.y. nuo naujojo LR Baudžiamojo Kodekso įsigaliojimo dienos). LR BK 198 straipsnyje teigiama, jog nusikalstamai veikia tas, kas, „1. pasisavino įstatymų saugomą kompiuterinę informaciją apie juridinį ar fizinį asmenį; 2 viešai paskleidė, paskelbė, platino ar kitaip panaudojo informaciją, kurią gavo darydamas šio straipsnio 1 dalyje numatytą veiką“. Trečiojoje straipsnio dalyje nustatyta, jog už tokią nusikalstamą veiką atsako ir juridinis asmuo.

Nusikaltimo, numatyto LR BK 198 straipsnyje, objektyviosios pusės grafinė išraiška.



Kaip matyti iš straipsnio dispozicijos, tokio pobūdžio veika pripažįstama nusikalstama, jeigu ją realizuojant įvykdomos dvi esminės sąlygos: pasikėsinama ne į bet kokią kompiuterinę informaciją, bet tik į tą, kurią saugo įstatymas; informacijos į kurią pasikėsinta turinys savyje talpina duomenis apie juridinį ar fizinį asmenį. Manytina, jog kompiuterinė informacija apie šunų veisles, saugoma kinologo mėgėjo kompiuteryje, nebus laikytina šio nusikaltimo dalyku.

Kaip matyti iš straipsnio dispozicijos, tai blanketinė teisės norma. Įstatymų saugoma kompiuterinė informacija apie juridinį ar fizinį asmenį – tai teisinių gėrių daugėtas, kurio apsaugą reglamentuoja tokie LR įstatymai kaip: „Konstitucija“, „Asmens duomenų teisinės

apsaugos įstatymas“, „Elektroninio parašo įstatymas“, „Valstybės ir tarnybos paslapčių įstatymas“, „Visuomenės informavimo įstatymas“, „Autorių teisių ir gretutinių teisių įstatymas“, „Civilinis kodeksas (informacija susijusi su profesine, komercine ar banko paslaptimi, privati informacija)“ ir kt.

Įstatymo saugomos kompiuterinės informacijos pasisavinimas – tai tokia nusikaltimo subjekto veika, kai minėta informacija yra perimama, ko pasėkoje gali būti naudojama veikiančiojo subjekto nuožiūra. Ar veikiantysis subjektas tokią informaciją panaudos siekdamas kokių nors neteisėtų tikslų, ne tiek ir svarbu – jis atsakys už patį informacijos pasisavinimą. Tokios informacijos platinimas ar kitoks panaudojimas sudaro kvalifikuotą šio nusikaltimo sudėtį (BK 198 str. 2 d.).

Nusikaltimo subjektas gali būti bendrasis – kai asmuo neturi prieigos teisės prie tokios informacijos arba specialusis – kai asmuo turi teisę susipažinti su tokia informacija, tačiau jis tai daro viršydamas savo įgaliojimus. Taigi pati prieiga prie tokio pobūdžio kompiuterinės informacijos gali būti tiek teisėta, tiek ne, tačiau tokios informacijos naudojimas kaip savo visada bus neteisėtas. Nusikalstamai veikai kvalifikuoti užtenka fakto, jog veikiantysis subjektas tokią informaciją pasisavino (arba dar papildomai atliko veiksmus, numatytus BK 198 str. 2 d.).

Fizinio daikto pasisavinimas suponuoja mintį, jog teisėtas daikto savininkas ar valdytojas nebegalės tuo daiktu naudotis, nes neteisėto pasisavinimo pasėkoje daikto paprasčiausiai nebelieka.

Informacijos pasisavinimas paprastai nesusijęs su jos sunaikinimu. Ją, kaip nematerialų objektą įmanoma pasisavinti, kartu paliekant ir teisėtam savininkui ar valdytojui galimybę naudoti pagal paskirtį. Jeigu pasisavinama informacija būtų dar ir sunaikinama, veiką papildomai tektų kvalifikuoti ir pagal LR BK 196 straipsnį.

Kadangi LR BK 198 straipsnyje numatyto nusikaltimo sudėtis yra formalioji, tam, kad būtų konstatuotas nusikalstamos veikos baigtumas, nereikalingos neigiamos pasekmės, priežastiniais ryšiais susijusios su veika – pakanka atlikti straipsnio dispozicijoje išvardintus veiksmus(-ą). Nusikaltimas bus baigtas, uždavus kompiuteriui komandą kopijuoti įstatymų saugomą kompiuterinę informaciją ir ją išsaugojus nusikaltimo subjektui prieinamoje ir teisėtai valdomoje informacijos laikmenoje. Pagal BK 198 str. 2 d. nusikaltimas bus baigtas, kai aukščiau aprašytu būdu pasisavinta įstatymo saugoma kompiuterinė informacija bus viešai paskleidžiama, paskelbiama, platinama ar kitokiu būdu panaudojama. „Viešai“ šiuo atveju

reiškia būdu, kai tokios informacijos turinys tampa prieinamas tretiesiems asmenims (ne nusikaltimo subjektui ir ne teisėtiems informacijos naudotojams).

Tiesioginis šio nusikaltimo objektas yra visuomeniniai santykiai, susiję su saugiu įstatymų saugomos kompiuterinės informacijos naudojimu. Dalykas – įstatymų saugoma kompiuterinė informacija apie juridinį ar fizinį asmenį.

Kalbant apie subjektyviąją tokio nusikaltimo pusę, reikia pabrėžti, jog kaltės forma galima tik tyčia. Santykyje su veika, nusikaltimo subjektas gali veikti tik tiesiogine tyčia. Preziumuojama, jog asmuo žino įstatymų reikalavimus ir suvokia, jog tam tikra informacija, liečianti konkretų fizinį ar juridinį asmenį, yra saugoma įstatymų. Pagaliau pasisavinti tiek fizinį, tiek nematerialų daiktą netyčia turbūt neįmanoma.

Nusikaltimo subjektu gali būti bet koks fizinis asmuo, sulaukęs 16 metų amžiaus ir atitinkantis subjektyviosios pusės pakaltinamumo požymį. Kaip minėta aukščiau, dėl šios nusikalstamos veikos baudžiamojon atsakomybėn gali būti traukiamas ir juridinis asmuo.

3. Praktiniai nusikaltimų informatikai tyrimo aspektai

Informatikos ir ryšių departamento prie VRM duomenimis, 2003 metų 5-12 mėnesiais Lietuvos Respublikoje buvo užregistruoti 3 nusikaltimai informatikai (dvi veikos kvalifikuotos pagal LR BK 196 str. 1 d., viena – pagal 198 str. 2 d.). 2004 metais (iki lapkričio 10 d.) užregistruota 12 nusikaltimų informatikai (trys veikos kvalifikuotos pagal 196 str. 1 d., dvi – pagal 197 str. 1 d., keturios – pagal 198 str. 1 d., viena – pagal 198 str. 2 d., viena – pagal $198^{(1)}$ str. 1 d., viena – pagal $198^{(1)}$ str. 2 d.).

2004-11-10 dienai ikiteisminis tyrimas yra baigtas ir procesiniai sprendimai yra priimti 4 baudžiamosiose bylose (iš 15). Tik dviejose iš šių bylų prokuroras pasinaudojo teise užbaigti procesą baudžiamuoju įsakymu, vadovaujantis LR BPK 418 str. (šie ikiteisminiai tyrimai buvo pradėti pagal LR BK 196 str. 1 d. ir 197 str. 1 d.) – t.y. tik dviejose bylose kalti asmenys buvo realiai nubausti piniginėmis baudomis. Beje, įtariamaisiais buvo patraukti jauni, neteisti žmonės (nors ir pilnamečiai), kurie dėl „patirties stokos“ prisipažino padarę nusikalstamas veikas ir sutiko, kad procesas būtų baigtas baudžiamuoju įsakymu. Sunku pasakyti kokia būtų šias bylas ištikusi baigtis, jeigu įtariamieji būtų neigę savo kaltę. Juolab, kad procesiniuose dokumentuose tik grynai formaliai buvo “konstatuota” didelė žala. Dar dvi iš paminėtų bylų buvo nutrauktos LR BPK 3 str. 1 d. 1 p. numatytu pagrindu – buvo konstatuota, jog nepadaryta veika, turinti nusikaltimo ar baudžiamojo nusižengimo požymių. Pabendravus su ikiteisminio tyrimo tyrėjais, kurių žinioje yra minėtų baudžiamųjų bylų tyrimas, paaiškėjo, jog likusios 11 bylų yra taip pat mažai perspektyvios (vėluoja teisinės pagalbos pavedimų įvykdymas iš užsienio valstybių, kai bandoma surinkti srauto duomenis; trūksta aiškumo dėl „didelės žalos“ sampratos, kalbant apie BK 196 ir 197 straipsnius; trūksta žinių, kokius procesinius veiksmus apskritai reikėtų atlikti, tiriant nusikaltimus informatikai).

Kaip žinia, įsigaliojus naujajam Baudžiamojo proceso Kodeksui, ikiteisminis tyrimas yra pradedamas beveik dėl visų pareiškimų (nutarimai nepradėti ikiteisminį tyrimą arba atsisakyti pradėti ikiteisminį tyrimą yra sąlygiškai reti, nes įstatymų leidėjas sąmoningai yra suvaržęs tokią galimybę). Taigi ikiteisminis tyrimas paprastai yra pradedamas, o pradėtas, surinkus pirminius duomenis, dažnu atveju yra paprasčiausiai nutraukiamas. Reikia pripažinti, jog tokia baigtis, matomai, laukia ir daugelio šiai dienai iškeltų bylų dėl nusikaltimų informatikai.

Kartais tokią bylos baigtį nulemia pati ikiteisminio tyrimo sistema: tam tikri sprendimai priimami dėl to, kad nepablogėtu ikiteisminio tyrimo statistiniai rezultatai.

Tokioje situacijoje ypatingai „bijomasi“ išteisinimo teisme.

Taigi, jeigu ikiteisminis tyrimas, kad ir pagal LR BK 196 str. 1 d. yra pradedamas, pavyzdžiui, dėl to, jog buvo gautas vienos Lietuvos Respublikoje registruotos įmonės vadovo pareiškimas apie tai, jog tam tikrą dieną ir valandą „nežinomi asmenys per interneto tinklą įsilaužė į įmonės serverį kur sunaikino keletą failų“, arba „interneto skelbimų puslapyje „www.nesvarbu.lt“ buvo iškraipytas pareiškėjo skelbimų turinys“, tikėtina, jog tokiose bylose procesinis sprendimas bus vienas – nutraukti.

Tiriant nusikaltimus kibernetinėje erdvėje, ikiteisminį tyrimą apsunkina ne tik, mano nuomone, nekokybiškai suformuluotos BK atitinkamų straipsnių dispozicijos, bet ir grynai praktiniai tyrimo aspektai. Visų pirma, nusikaltimai informatikai išeina už vienos valstybės jurisdikcijos. Srauto duomenys (IP adresas ir pan.), kurių pagalba įmanoma nustatyti elektroninių komunikacijų kelią, gali būti taip pat sėkmingai sunaikinti, kaip ir bet kuri kita kompiuterinė informacija. Net jeigu tarptautinio bendradarbiavimo dėka operatyviai pavyktų nustatyti, kurio kompiuterio pagalba buvo padarytas vienas ar kitas nusikaltimas kibernetinėje erdvėje, kiltų kitas klausimas – kas uždavė vieną ar kitą kompiuterinę komandą, ko pasėkoje ir buvo padarytas nusikaltimas (nusikaltimas gali būti padarytas, kad ir Interneto kavinėje, kur vartotojų registracija kelia daug abejonių – paprastai jos iš viso nėra). Taigi nusikaltimų informatikai pėdsakai gali būti nustatomi tik kompiuterinių technologijų dėka, tačiau net didžiausios tyrimo sėkmės atveju, bus nustatytas tik konkretus kompiuteris – nusikaltimo įrankis. Vien tas faktas, kad konkretus asmuo naudoja šį kompiuterį, nebus pakankamas pagrindas jį traukti baudžiamojon atsakomybėn.

Nusikaltimai virtualioje erdvėje neturi jokių sienų, jokių ribų - tiek nusikaltimo organizatoriai tarpusavyje, tiek nusikaltimo dalykai gali būti skirtingose pasaulio dalyse. Internetas ir elektroninės finansinės paslaugos keičia verslo ir kitokio pobūdžio veiklos praktikas ir jomis gali būti labai sėkmingai pasinaudota atliekant nusikaltimus. Atsižvelgiant į tai, būtinybė imtis naujų priemonių nusikaltimų prevencijos ir kontrolės srityje yra akivaizdi. Šiuo metu jau daugelyje pasaulio šalių (ypatingai išsivysčiusiose šalyse, kur kompiuterizacijos lygis yra sąlygiškai aukštas) skiriama daug dėmesio ir pastangų kovai su nusikaltimais kibernetinėje erdvėje. Lietuvoje taip pat 2001-10-01 Lietuvos kriminalinės policijos biure nusikaltimų tyrimo vyriausioje valdyboje buvo įkurtas Nusikaltimų elektroninėje erdvėje tyrimo skyrius (NEETS), kurio misija yra užtikrinti Konvencijos dėl elektroninių nusikaltimų reikalavimų įgyvendinimą, užkardyti, tirti, ir atskleisti ruošiamus,

daromus ar padarytus nusikaltimus elektroninėje erdvėje - pasauliniame interneto tinkle bei korporatyvinėse informacinėse sistemose - intranete, užtikrinti Lietuvos visuomenės ir informacinių technologijų saugumą šioje srityje. Tikėtina, jog specializuotų teisėsaugos padalinių kūrimas pagerins nusikaltimų informatikos srityje tyrimo situaciją.

Išvados ir pasiūlymai

1. Šiandien informacija traktuojama ne tik kaip naujienos/žinios apie įvykius pasaulyje, pranešamos masinės informacijos priemonių pagalba, bet ir kaip komunikacinė struktūra, apimanti žinių kūrimo, sisteminimo, saugojimo, perdavimo, interpretavimo sandus. Informacija tapo žmogiškosios egzistencijos esminiu komponentu, esančiu šalia materialinių bei energetinių resursų. Kadangi informacinis resursas (išteklius) padeda taupyti daugelį kitų visuomenės resursų, tolimesnis visuomenės progresas didžia dalimi priklauso nuo informacinės infrastruktūros tobulėjimo, nuo informacinių produktų formavimo, saugojimo, platinimo bei naudojimo efektyvumo. Kita vertus, sociumo vystymasis naujojoje nuolat tobulėjančioje komunikacinėje erdvėje yra tiesiogiai proporcingas informacinio resurso apsaugos nuo neteisėto naudojimosi juo efektyvumui. Šioje vietoje iškyla teisės ir komunikacijų sąveikos vaidmuo sociumo vystymosi procesams. Teisės vaidmuo reiškiasi tada, kai techninės informacijos apsaugos priemonės nebegali užtikrinti šio socialinio resurso saugos nuo nesankcionuoto poveikio.

Globaliųjų tinklų, Interneto sklaidos epochoje, įstatymų leidėjas, kurdamas baudžiamosios teisės normas, susidūrė su naujomis nusikalstamomis veikomis, su naujomis "senųjų/tradicinių" nusikalstamų veikų raiškos formomis, su moderniųjų/pomoderno laikų teisiniais gėriais, kuriuos ir turi apsaugoti laikmečiui adaptuotos baudžiamosios teisės normos.

Šios naujosios nusikalstamos veikos ypatingos tuo, kad jos daromos visiškai naujoje ir vienai valstybei nepavaldžioje virtualioje - elektroninėje erdvėje. Mūsų epochos svarbiausiu fenomenu tapo Internetas. Tačiau būtent ši virtuali erdvė atvėrė naujas galimybes ir nusikaltėliams. Komunikacijos Internetu metu vyrauja beasmeniškumas, savęs “sukonstravimo” galimybė (tai virtualių įvaizdžių bendravimas), kas dažnu atveju kalbant apie nusikaltimus, “išplauna” veikos ir atsakomybės santykį.

2. Egzistuoja dvi pagrindinės mokslinės minties srovės, skirtingai traktuojančios elektroninių nusikaltimų esmę. Viena jų prie nusikaltimų kibernetinėje erdvėje priskiria visus nusikaltimus, kuriuose kompiuteris bei kompiuterinė informacija yra tiek nusikaltimo dalykas, tiek nusikalstamos veikos priemonė. Kita – prie nusikaltimų informatikai priskiria tik priešingas teisei veikas, susijusias su informacijos elektroninio apdorojimo procesais. Pastarieji mokslininkai pagrindiniu kvalifikuojančiu požymiu, leidžiančiu tam tikrus nusikaltimus išskirti į atskirą nusikaltimų informatikos srityje grupę, įvardina specifinių nusikalstamos veikos būdų, priemonių ir dalykų bendrybę. Kitaip tariant, nusikalstamos veikos dalykas yra informacija, apdorojama kompiuterinės technikos pagalba, o kompiuteris tarnauja nusikalstamos veikos priemone. Pastarosios nuomonės laikosi ir šio magistro darbo autorius.

3. Lietuvos Respublikoje informatikos baudžiamąja teisine apsauga susidomėta gerokai atsiliekant nuo telekomunikacinių technologijų vystymosi procesų. 2003-05-01 d. įsigaliojo „naujasis“ Lietuvos Respublikos Baudžiamasis Kodeksas. Būtent šiame kodekse buvo įtrauktas atskiras XXX skyrius - NUSIKALTIMAI INFORMATIKAI, susidedantis iš trijų straipsnių. 2004-01-29 d., įsigaliojus BK pakeitimams, šis skyrius buvo papildytas dar dviem straipsniais. Pirmą kartą nusikaltimai, kurių objektas yra labai specifinis - kompiuterinė informacija - įstatymo leidėjo buvo įvardinti visuomeniškai pavojingomis veikomis.

4. Teisinių instrumentų taikymas nusikaltimų informatikai tyrimo sferoje yra labai problematiškas visų pirma dėl to, kad šių nusikaltimų dalykas yra nematerialus ir gali būti apčiuopiamas tik panaudojus aukštąsias technologijas. Tačiau, turint omenyje, jog Lietuvos Respublikos Baudžiamojo Kodekso XXX skyriaus kai kurių straipsnių dispozicijos yra sukonstruotos vadovaujantis grynai teisės teorijos principais, kartais ignoruojant

kompiuteriuose ir kompiuteriniuose tinkluose vykstančius techninius procesus, darytina išvada, jog šių teisės normų taikymas negali užtikrinti ikiteisminio tyrimo sėkmės.

5. Neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo (arba kompiuterinis „įsilaužimas“), už kurį baudžiamoji atsakomybė numatyta LR BK $198^{(1)}$ straipsnyje, kaip toks, mano galva, nėra savipakankama veika, kad ją būtų galima įvardinti nusikaltimu, nes „grynasis“ kompiuterinis įsilaužimas egzistuoja labai trumpą laiko atkarpą kaip pereinamoji grandis - tai tik priemonė daryti kitus nusikaltimus informatikos sferoje.

Net ir dėl techninių priežasčių „grynojo prisijungimo“ prie kompiuterio ar kompiuterinio tinklo administratorius nepastebės, kol nebus pradėtas daryti poveikis informacijai (pagrindinis informacijos kopijavimo, naikinimo, keitimo ir kitokio poveikio signalas yra tinklo neįprastai aukštas apkrovimo lygis, kas ir paskatina administratorių ieškoti to priežasčių).

Manau, jog $198^{(1)}$ straipsnio sudėtis turėtų būti inkorporuota į kitas nusikaltimų informatikai sudėtis (į 196 – 198 straipsnių dispozicijas, o pastaruosiuose straipsniuose įvardinti nusikalstami veiksmai numatomi kaip materialios pasekmės, ko pasėkoje, “grynąją” neteisėtą prieigą reikėtų vertinti kaip pasikėsinimą padaryti nusikalstamas veikas, numatytas LR BK 196 - 198 straipsniuose).

6. Kalbėdamas apie neteisėtą disponavimą įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti (LR BK $198^{(2)}$ straipsnis), įstatymų leidėjas į šio straipsnio antrojoje dalyje numatyto nusikaltimo kvalifikuotąją sudėtį įtraukia vieną subjektyviosios pusės požymį – tikslo turėjimą daryti nusikaltimus kibernetinėje erdvėje tokių produktų pagalba. Savaime suprantama, jog tyrėjams, atliekantiems ikiteisminį tyrimą, visais atvejais yra nelengva įrodinėti subjektyviųjų požymių egzistavimą nusikalstamos veikos procese. Nusikalstamos veikos subjektas daugeliu atveju ir laikysis versijos, jog jis tik įgijo ir laikė tokio pobūdžio kompiuterines programas, įrenginius ar prisijungimo kodus, nors ir neturėjo tikslo daryti nusikaltimus informatikos srityje. Manau, jog ir taip sudėtingai įrodinėjamų nusikaltimų informatikai sudėtyse neturėtų būti numatyti fakultatyviniai subjektyviosios pusės požymiai – atsakomybė turėtų kilti dėl paties fakto.

7. Kalbant apie kompiuterinės informacijos bei kompiuterinės programos sunaikinimo ar pakeitimo sudėtis (LR BK 196, 197 straipsniai), pažymėtina, jog dispozicijose neturėtų būti neaiškių, vertinamojo pobūdžio sąvokų (arba jos turėtų būti tinkamai paaiškintos).

Dėl nusikalstamų veikų, numatytų LR BK 196 ir 197 straipsniuose, baudžiamoji atsakomybė kyla tik tuo atveju, jeigu dėl tokios veikos buvo padaryta “didelė žala”. Tačiau kokias aplinkybes, atsiradusias nusikalstamos veikos realizavimo atveju, reikėtų įvardinti kaip „didelę žalą“, lieka neaišku.

Nusikalstamų veikų kibernetinėje erdvėje specifika ir siekis vienodinti teismų praktiką reikalauja įstatyme pateikti abstrakčios sąvokos „didelė žala” išaiškinimą. Būtų tikslinga BK XXX skyrių papildyti dar vienu straipsniu, kuriame būtų atskleisti du šios sąvokos aspektai – turtinės ir neturtinės žalų turiniai. Priešingu atveju, neaiški juridinė definicija įvairių teismų bei ikiteisminio tyrimo institucijų gali būti komentuojama nevienodai. Akivaizdu, kad šią situaciją palikus teismų praktikos formavimosi procesui, didelės žalos samprata kristalizuosis pakankamai ilgą laiką, neišvengiant klaidų, nevienodo veikų kvalifikavimo ikiteisminio tyrimo įstaigose ir teismuose.

Mano manymu, „didelės žalos“ (šią sąvoką tinkamai apibrėžus) atsiradimas turėtų būti vertinamas kaip nusikalstamą veiką kvalifikuojantis požymis ir tokias pasekmes sukėlusi veika išskirta į atskirą straipsnio dalį, tuo tarpu pirmąsias BK 196, 197 straipsnių dalis suformuluojant kaip formaliąsias nusikaltimų sudėtis.

Atsižvelgiant į tai, kad BK 196 ir 197 straipsnių normos savo paskirtimi ir sankcijomis yra panašios, manau, būtų tikslinga šiuos straipsnius apjungti į vieną baudžiamojo kodekso straipsnį, nesureikšminant fakto, jog, iš pirmo žvilgsnio, BK 196 ir 197 straipsniai numato

skirtingą nusikalstamos veikos dalyką: kompiuterinę informaciją (196 str.) ir kompiuterines programas (197 str.). Kompiuterinė programa taip pat yra kompiuterinė informacija, talpinanti savyje papildomas funkcijas – t.y., kompiuterinė programa yra tie kompiuteriniai duomenys, kurie tiesiogiai dalyvauja procesoriaus atliekamose operacijose.

8. Vadovaujantis Lietuvos Respublikos Baudžiamuoju Kodeksu, kompiuterinės informacijos (išskyrus įstatymų saugomą informaciją apie fizinį ar juridinį asmenį) pasisavinimas/kopijavimas/perimtis negalėtų būti priskirtas prie nusikalstamų veikų kibernetikos srityje. Informacijos kopijavimas/perimtis ir yra vienas iš esminių nusikaltimų informatikai aspektų, dėl kurio dažnu atveju praktikoje ir yra "įsilaužinėjama" į kompiuterius ar kompiuterių tinklus. Europos tarybos konvencijoje dėl elektroninių nusikaltimų apie kompiuterinę informaciją/kompiuterinius duomenis kalbama bendrąja prasme - „kompiuteriniai duomenys" – tai bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat programa, pagal kurią kompiuterinė sistema gali vykdyti tam tikrą funkciją". Mano galva, derėtų praplėsti nusikalstamų veiksmų baigtinį sąrašą LR BK 196 straipsnyje (t.y. šalia kompiuterinės informacijos sunaikinimo, pakeitimo ir kt., papildomai kriminalizuoti kompiuterinės informacijos perėmimą/kopijavimą).

9. Kompiuterinės informacijos pasisavinimas ir skleidimas (LR BK 198 straipsnis), pripažįstami nusikalstamomis veikomis, jeigu jas realizuojant įvykdomos dvi esminės sąlygos: pasikėsinama ne į bet kokią kompiuterinę informaciją, bet tik į tą, kurią saugo įstatymas; informacijos į kurią pasikėsinta turinys savyje talpina duomenis apie juridinį ar fizinį asmenį.

Kaip matyti iš straipsnio dispozicijos, tai blanketinė teisės norma. Įstatymų saugoma kompiuterinė informacija apie juridinį ar fizinį asmenį – tai teisinių gėrių daugėtas, kurio apsaugą reglamentuoja tokie LR teisės aktai kaip: „Konstitucija", „Asmens duomenų teisinės apsaugos įstatymas", „Elektroninio parašo įstatymas", „Valstybės ir tarnybos paslapčių įstatymas", „Visuomenės informavimo įstatymas", „Autorių teisių ir gretutinių teisių įstatymas", „Civilinis kodeksas (informacija susijusi su profesine, komercine ar banko paslaptimi, privati informacija)" ir kt. Mano manymu, konstruojant nusikaltimų kibernetinėje erdvėje sudėtis, ir derėtų eiti būtent šia kryptimi – t.y. formuluoti blanketines teisės normas (sukurti kompiuterinės technikos eksploatavimo taisykles ir panašiai).

10. Nusikaltimų informatikai dispozicijų trūkumai, ikiteisminio tyrimo pareigūnų, prokurorų ir teisėjų menkas kompiuterinis išprusimas, nepakankamos kompiuterinės-techninės žinios, nepakankamas tarptautinis bendradarbiavimas, srauto duomenų (IP adresų), kurių pagalba įmanoma nustatyti elektroninių komunikacijų kelią, nepakankama apsauga (vartotojui priskirtas dinaminis IP adresas, reikalavimas telekomunikacines paslaugas teikiančioms įmonėms srauto duomenis saugoti tik 6 mėnesius ir pan.), „Interneto kavinių" veiklos nepakankamas reglamentavimas stabdo LR BK XXX skyriuje įvardintų nusikalstamų veikų tyrimą. 2004-11-10 dienai ikiteisminis tyrimas yra baigtas ir procesiniai sprendimai yra priimti 4 baudžiamosiose bylose (iš 15). Tik dviejose iš šių bylų prokuroras pasinaudojo teise užbaigti procesą baudžiamuoju įsakymu, vadovaujantis LR BPK 418 str. (šie ikiteisminiai tyrimai buvo pradėti pagal LR BK 196 str. 1 d. ir 197 str. 1 d.) – t.y. tik dviejose bylose kalti asmenys buvo realiai nubausti piniginėmis baudomis. Dar dvi iš paminėtų bylų buvo nutrauktos LR BPK 3 str. 1 d. 1 p. numatytu pagrindu – buvo konstatuota, jog nepadaryta veika, turinti nusikaltimo ar baudžiamojo nusižengimo požymių. Pabendravus su ikiteisminio tyrimo tyrėjais, kurių žinioje yra minėtų baudžiamųjų bylų tyrimas, paaiškėjo, jog likusios 11 bylų yra taip pat mažai perspektyvios. Žinoma, egzistuoja tokios situacijos priežastys, nepriklausančios nei nuo teisės normų kūrėjų, nei nuo teisę taikančių subjektų darbo ir kvalifikacijos. Viena iš tokios situacijos priežasčių – aukštas elektroninių nusikaltimų latentiškumo lygis. Kita vertus, tam tikras kliūtis sukuria ir patys nukentėjusieji: daugelis komercinių struktūrų nesuinteresuotos paviešinti duomenis, galinčius sukelti abejonių dėl jų informacinių sistemų saugumo ir patikimumo.

Santrauka

Magistro baigiamojo darbo objektas – nusikaltimų informatikai baudžiamosios teisinės apsaugos efektyvumo analizė.

Magistro baigiamajame darbe analizuojami socialinio kismo aspektai, susiję su informacinės visuomenės tapsmo procesais, keliamas informacinių technologijų sklaidos ir teisės, kaip vienos stabiliausių socialinių struktūrų santykio klausimas. Siekiant įvertinti kibernetinės erdvės baudžiamosios teisinės apsaugos efektyvumą, darbe pateikiamos pagrindinės sąvokos ir sampratos, susijusios su nusikaltimais informatikai, analizuojamos baudžiamosios teisės normos, nustatančios baudžiamąją atsakomybę už nusikaltimus kibernetinėje erdvėje, bandoma įžvelgti šių teisės normų dispozicijų trūkumus, trukdančius/galinčius trukdyti šias normas taikyti praktikoje, įvardijamos pagrindinės problemos, kylančios tiriant nusikaltimus informatikos srityje.

Įvertinus mokslinėje literatūroje formuluojamos problemos aspektus bei prieinamus empirinius duomenis, magistriniame darbe ginama tokia hipotezė: teisinių instrumentų taikymas nusikaltimų informatikai tyrimo sferoje yra labai problematiškas. Tai ypač pasakytina, turint omenyje, jog Lietuvos Respublikos Baudžiamojo Kodekso XXX skyriaus kai kurių straipsnių dispozicijos yra sukonstruotos tokiu būdu, kad jų taikymas negali užtikrinti ikiteisminio tyrimo sėkmės.

Summary

The object of the graduation paper for Master's degree is analysis of the effectiveness of the security provided by criminal law concerning informational technologies.

The graduation paper analyses social change aspects related to the process of the informational society formation, it raises the question of relation between rights and propagation of informational technologies as an issue of one of the most stabile social structures. Seeking to evaluate the effectiveness of the security provided by criminal law for cyberspace, the paper provides basic notions and conspectus related to crimes to informational property, analyses standards of criminal law, determining criminal liability for crimes in cyberspace, endeavors to perceive the shortcomings of standards dispositions of this law interfering with practical applications of these standards, identifies the main problems arising while investigating crimes in the field by informational technologies.

Evaluating aspects of the problem formulated in the science literature and the available empirical data, the graduation paper defends the following hypotheses: application of legal instruments in the investigation sphere of crimes in the informational field is very problematic. It is especially manifest having in mind that some dispositions of articles in Lithuanian Criminal Code section XXX are construed in such a way that the application of them cannot guarantee the success of pre-trial investigation.

Literatūros sąrašas

1. Augustinaitis A. Informacinės visuomenės mokslo bruožai // Sociologija. Mintis ir veiksmas, 1998/2.
2. Fiske J. Įvadas į komunikacijos studijas.-Vilnius, 1998.
3. Mickunas A., Pilotta J.J. Technocracy vs. democracy. Issues in the politics of communication. New Jersey, 1998.
4. Piesliakas V. Mokymas apie nusikaltimą ir nusikaltimo sudėtį. - Vilnius, 1996.
5. Ramonet I. La Tyrannie de la communication.- Paris, 1999.
6. Rytel T. Japonijos kelias į informacinę visuomenę // Mokslo Lietuva, 1999/5.
7. Sodžiutė L., Sūdžius V. Elektroninė komercija: prielaidos, struktūra ir procesai. – IĮ "Petro ofsetas", 2003 m.
8. Wessels J. Baudžiamoji teisė. Bendroji dalis. – Vilnius, 2003.
9. Baudžiamoji teisė. Bendroji dalis.- Vilnius, Eugrimas, 1996.
10. Baudžiamoji teisė. Specialioji dalis. 1, 2 knygos. - Vilnius, 2000.
11. Informacinių technologijų visuomenė: humanitarinės interpretacijos – monografija. – Vilnius, Lietuvos teisės universiteto leidybos centras, 2002.
12. Šiuolaikinis nusikalstamumas / Autorių kolektyvas. Redaktorius Tadas Klimas. – Kaunas, VDU l-kla, 2002.
13. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. – Москва, 2001.
14. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия – Телеком, 2002.
15. Вартанова Е. Информационное общество в стратегии Европейского Союза (Информационное общество: необходимость государственного подхода) http://www.internews.ru/ZIP/43/europe.html
16. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность //Юридический мир.— 1998.— февраль.
17. Крылов В. Информационные преступления — новый криминалистический объект //Российская юстиция.— 1997.— № 4.
18. Пугачев В.П. Информационная властъ и демократия // Общественные науки и современостъ, 1999/4.
19. Огурцов А.П. Наука: власть и коммуникация (социально-философские аспекты) // Вопросы философии, 1990/11.
20. Ракитов А.И. Философия компъютерной революции. – Москва, 1991.

21. Современный капитализм: критический анализ буржуазных политологических концепций / К.С.Гаджиев, А.К.Гливакщвский, Г.В.Каменская и др.-Москва, 1988.
22. Уголовное право России – Учебник для вузов в 2-х томах. Том 2 Особеная часть. – Издательская група НОРМА-ИНФРА - М, Москва, 1999.
23. Российское уголовное право в 2-х томах - Особеная часть. Под редакцией професора А.И.Рарога, Москва, 2003.
24. Уголовное право. Особенная часть. Учебник. Под ред. д.ю.н. проф. А.С. Михлина, М.: Юриспруденция, 2000.
25. Судебная практика по компьютерным преступлениям (краткий обзор). Протасов П. – http://law.bugtrag.ru

Norminiai teisės aktai

26. Lietuvos Respublikos KONSTITUCIJA // Valstybės žinios, 1992, Nr. 33-1014.
27. Lietuvos Respublikos Baudžiamasis Kodeksas // Valstybės žinios, 2000, Nr. 89-2741.
28. Elektroninio parašo įstatymas // Valstybės žinios, 2000, Nr. 61-1827.
29. Visuomenės informavimo įstatymas // Valstybės žinios, 2000, Nr. 75-2272.
30. Asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios, 1996, Nr. 63-1479.
31. Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose // Valstybės žinios, 2002 Nr. 952.
32. Dėl duomenų apsaugos plėtojimo 2002-2004 metais programos patvirtinimo // Valstybės žinios, 2002 Nr.23-871.
33. Dėl Asmens duomenų valdytojų valstybės registro įsteigimo ir šio registro nuostatų patvirtinimo // Valstybės žinios, 2000, Nr. 27-721.
34. Dėl Asmens duomenų valdytojų valstybės registro reorganizavimo, šio registro nuostatų ir asmens duomenų valdytojų pranešimo apie duomenų tvarkymą automatiniu būdu tvarkos patvirtinimo // Valstybės žinios, 2003 Nr. 18-971.
35. Dėl valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo // Valstybės žinios, 1998 Nr.115-3259.
36. Dėl Tipinių duomenų saugos nuostatų patvirtinimo //Valstybės žinios, 2003 Nr.76-3511.
37. EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EC). // http://www3.lrs.lt/c-bin/eu/preps2?Condition1=7879&Condition2=
38. Valstybės ir tarnybos paslapčių įstatymas // Valstybės žinios, 2004 Nr.

39. Elektroninių ryšių ĮSTATYMAS // Valstybės žinios, 2004 Nr.69-2382.
40. Dėl Lietuvos Respublikos elektroninių ryšių įstatymo koncepcijos patvirtinimo // Valstybės žinios, 2003 Nr.26-1039.
41. Lietuvos Respublikos kompiuterių programų ir duomenų bazių teisinės apsaugos įstatymas – Negalioja de jure //Valstybės žinios, 1996 Nr.18-456.
42. ĮSTATYMAS dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo // Valstybės žinios, 2004 Nr.36-1178.
43. Konvencija dėl elektroninių nusikaltimų // Valstybės žinios, 2004, Nr. 36-1188.
44. Lietuvos Respublikos ryšių įstatymas – *Negalioja* de jure. // Valstybės žinios, 1998 Nr. I-1109.
45. Patentų įstatymas // Valstybės žinios, 2001 Nr. I-372.
46. Europos patentų konvencija. // http://www3.lrs.lt/cgi-bin/preps2?Condition1=226277&Condition2=
47. Autorių teisių ir gretutinių teisių įstatymas // Valstybės žinios, 1999, Nr. 50-1598.
48. Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymo 5 ir 9 straipsnių pakeitimo ir papildymo ĮSTATYMAS // Valstybės žinios,2003 Nr.108-4813.
49. Dėl Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo // Valstybės žinios, 2004 Nr.58-2061.
50. Dėl Viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo // Valstybės žinios, 2004 Nr. 290.
51. Dėl Lietuvos Respublikos Vyriausybės 2003 m. kovo 5 d. nutarimo Nr. 290 "Dėl Viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo" pakeitimo // Valstybės žinios, 2004 Nr.96-3530.
52. Уголовный Кодекс Российской Федерации: Федеральный закон РФ. //http://www.akdi.ru/pravo/kodeks/text_uk2.htm#g1
53. ФЗ "Об информации, информатизации и защите информации." // http://www.akdi.ru/pravo