ISSN 1392-6195

JURISPRUDENCIJA
Mokslo darbai
2006 5(83); 82–89

ELEKTRONINĖS INFORMACIJOS SAUGOS TARPTAUTINIO TEISINIO REGULIAVIMO ANALIZĖ: LIETUVOS PADĖTIS

Doktorantas Žydrūnas Paškauskas

Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Informatikos ir statistikos katedra
Ateities g. 20, LT-08303 Vilnius
Telefonas 271 45 71
Elektroninis paštas zydriusp@mruni.lt

Pateikta 2006 m. balandžio 24 d., parengta spausdinti 2006 m. gegužės 5 d.

Santrauka. Informacinių technologijų sauga yra pagrindinis veiksnys, leidžiantis koordinuoti informacinių technologijų naudojimą Lietuvos viešajame bei privačiajame sektoriuose. Šiandien, kai didžioji visuomenės dalis daugiau ar mažiau priklauso nuo sklandaus informacinių sistemų darbo bei jomis teikiamų paslaugų, saugos reikalavimai iškyla į pirmąją vietą. Sparti naujos kartos technologijų plėtra lėmė nemažai pasikeitimų mus supančiame „daiktiniame" pasaulyje. Nematerialios formos informacija tapo savarankiška vertybe. Tokios vertybės apsaugai skiriama vis daugiau dėmesio tiek techniniu, tiek ir teisiniu požiūriu visame pasaulyje. Aktyvi naujų informacinių technologijų plėtra informacinėje srityje ne tik gerina informacinių procesų ir veiklos kokybę, bet sukelia ir neigiamų pasekmių, tokių kaip nusikaltimai informatikai. Informacijos apsauga, ypač ekonominėje sferoje, – labai svarbi ir specifinė veiklos rūšis, kurią taip pat privalu nuosekliai ir išsamiai teisiškai reglamentuoti.

Efektyvios informacijos saugos politikos ir teisės sukūrimas neįmanomas be technikų profesionalų ir teisininkų glaudaus tarpusavio bendradarbiavimo, kadangi taikant kompiuterines technologijas atsiranda socialinių santykių, susijusių su asmens prigimtinėmis teisėmis, apsauga. Informacinių sistemų sauga turi būti suderinta su informacijos teisėto naudojimo ir laisvo duomenų judėjimo principais demokratinėje visuomenėje. Sauga turi būti užtikrinama taip, kad ji atitiktų demokratinėje visuomenėje pripažintas vertybes. Pabrėžtina, kad egzistuojantys teisės aktai neturi varžyti teisių turėtojų teisėtų interesų arba trikdyti normalių tokios sistemos darbą. Kiekviena valstybė yra atsakinga už tokių sąlygų sukūrimą ir tinkamą jų taikymą. Darbe nagrinėjamos tarptautinio (regioninio) koordinavimo dokumentų, Europos Sąjungos ir kitų išsivysčiusių valstybių, taip pat Europos bendradarbiavimo ir plėtros organizacijos, kurios iki šios dienos priimti teisės aktai suformavo pagrindines vertybines kryptis šioje visuomeninių santykių srityje, teisės aktų nuostatos, tiesiogiai veikiančios informacinių sistemų ir informacijos saugos teisinio reguliavimo klausimus. Straipsnyje taip pat analizuojama šios srities teisinė bazė Lietuvos Respublikoje bei praktinio pritaikymo klausimai. Straipsnis baigiamas išvadomis ir apibendrinimais, suformuluotais taikant loginės analizės, taip pat ir sisteminius metodus.

Pagrindinės sąvokos: saugos teisinis reguliavimas, saugos reguliavimo principai, saugos politika, saugos strategija.

ĮVADAS

Vienas iš pagrindinių įvairių visuomeninio gyvenimo sferų efektyvaus valdymo veiksnių yra teisingas informacijos tvarkymas. Be šiuolaikinių moderniai administruojamų informacinių sistemų nebeįsivaizduojamas kasdieninis kiekvieno iš mūsų gyvenimas.

Informacijos sauga suprantama kaip trijų pagrindinių informacijos savybių – konfidencialumo, vientisumo ir prieinamumo – vienybė. Kad visuomenėje, valstybėje vyrautų įstatymo leidėjo pageidaujamas elgesys, būtina, kad saugos naudą suvoktų dalyvaujančios šalys. Pagrindinė sąlyga – atitinkamos informacinių sistemų plėtros ir keitimosi informacija saugos kultūros sukūrimas Lietuvoje. Informacinių sistemų informacijos ir procesų konfidencialumas, vientisumas bei prieinamumas yra ypatingai svarbios daugelio didelių organizacijų veiklos savybės, kurias lemia teisinio ir kitokio reguliacinio pobūdžio poveikio priemonės. Teisės normos šiandien dar nepakankamai aiškiai atspindi specifinius terminus, sampratas, pasigendama šios srities reglamentavimo pamatinėmis teisės normomis. Todėl efektyvi informacinėse sistemose tvarkomos informacijos sauga turėtų būti vienas iš svarbiausių valstybės informacinės politikos prioritetų. Kuriant Lietuvos Respublikos teisės

aktus, reguliuojančius visuomeninius santykius informacinių sistemų ir informacijos saugos srityje, būtina atlikti tarptautinio koordinavimo dokumentų analizę, nustatyti pagrindinius informacinių sistemų ir informacijos saugos teisinio reguliavimo principus bei nuostatas. Toks valstybės teisinės sistemos sutvarkymas, teisinio reglamentavimo suvienodinimas yra pagrindinis uždavinys, kurį dabar sau turi kelti mūsų valstybė. Todėl šio straipsnio tikslas – pasitelkus aprašomąjį, lyginamąjį, sisteminį dokumentų analizės metodus išanalizuoti ir įvertinti informacijos ir informacinių sistemų saugos nuostatas įvairių valstybių teisės sistemose ir įstatymų leidyboje bei suformuluoti ir pateikti pasiūlymų mūsų valstybės informacinių sistemų ir jose tvarkomos informacijos saugai gerinti.

1. TARPTAUTINIS ELEKTRONINĖS INFORMACIJOS SAUGOS KLAUSIMŲ REGLAMENTAVIMAS

1.1. Europos bendradarbiavimo ir plėtros organizacijos teisinio reguliavimo analizė

Tarptautiniu mastu reglamentuoti informacinių sistemų ir jose tvarkomos informacijos saugos klausimus viena iš pirmųjų pradėjo Europos bendradarbiavimo ir plėtros organizacija (toliau – OECD). OECD priimtos direktyvos vertintinos kaip specifinę reikšmę turintys teisės aktai, kurie nurodo valstybėms narėms pagrindines veiklos kryptis. Daugelį metų OECD priimti teisės aktai formavo bendrą tarptautinių organizacijų tolimesnio bendradarbiavimo pagrindą. 1980 m. OECD tarybos rekomendacija dėl privatumo ir asmens duomenų laisvo judėjimo buvo pirmoji šioje srityje [1]. Ji paskatino tolesnę kitų OECD rekomendacijų ir dokumentų leidybą, tolesnę šioje rekomendacijoje pateiktų principų plėtrą. Tarp pastarųjų reikėtų paminėti 1997 metų OECD tarybos rekomendaciją *Dėl OECD kriptografijos politikos gairių* [2]. Pripažindama, kad kriptografija gali būti efektyvus įrankis užtikrinant informacinių technologijų, taip pat kompiuterių tinklų ir sistemų konfidencialumą, vientisumą ir prieinamumą, Taryba rekomendavo valstybėms narėms atsižvelgti į 1997 m. OECD kriptografijos politikos direktyvą ir į 2002 m. OECD rekomendaciją *Dėl informacinių sistemų saugos gairių* [3]. Jungtinių Tautų Organizacijos Generalinė asamblėja, vadovaudamasi 2002 m. liepos 25 d. OECD tarybos 1037 sesijoje patvirtinta rekomendacija, 2002 m. gruodį priėmė rezoliuciją A/RES/57/239 *Dėl visuotinės kibernetinės saugos kultūros* [4]. Reikia pažymėti, kad 2002 m. OECD rekomendaciją taip pat buvo pripažino Azijos ir Ramiojo vandenyno ekonominio bendradarbiavimo forumas bei Europos Sąjungos Taryba.

Rekomendacija nustato pagrindinius tolimesnės informacinių sistemų plėtros principus. Rekomendacijoje taip pat pateikiami penki „kertiniai akmenys“, kurie reikalauja iš valstybių narių imtis tam tikrų veiksmų, procedūrų, kad būtų įgyvendinti duomenų (informacinių sistemų) saugos principai; bendradarbiauti plėtojant atitinkamus standartus, priemones, procedūras ir užtikrinti informacinių sistemų saugą bei prireikus nedelsiant įgyvendinti rekomendacijose įtvirtintas priemones; plačiai skleisti rekomendacijoje pateiktus principus ir atnaujinti ją kas penkeri metai. Rekomendacija taikytina tiek privačiajam, tiek ir viešajam sektoriams bei visoms informacinėms sistemoms.

Rekomendacijoje pateikiami pagrindiniai principai:

- **Atsakomybės**. Įpareigojimai, privalomi savininkui, paslaugų teikėjui ir informacinių sistemų vartotojams ir kitoms susijusioms šalims, bei jų atsakomybė turi būti aiškūs. Tarpusavyje susiję lokalūs ir globalieji tinklai ir informacinės sistemos labai svarbūs sklandžiam bet kokios institucijos, įmonės, įstaigos, organizacijos darbui užtikrinti. Todėl besinaudojantys šiais produktais asmenys privalo suprasti savo atsakomybę už šių sistemų ir tinklų saugą. Jie privalo atsakyti už savo veiksmus priklausomai nuo savo funkcijų ir vaidmens; nuolat analizuoti saugos politiką, praktiką, priemones ir procedūras bei įvertinti jas atsižvelgdami į esamą padėtį.

- **Supratimo**. Rizikos veiksnių ir egzistuojančių saugos priemonių suvokimas yra pirmas „gynybos“ etapas. Informacinėms sistemoms bei tinklams poveikį gali daryti tiek išorinės, tiek ir vidinės grėsmės. Šalys turi suprasti, kad sistemos darbo sutrikimai gali sukelti didžiulę žalą, taip pat kad žala gali kilti ir dėl sistemų globalumo ir tarpusavio priklausomybės. Šalys privalo valdyti savo sistemos sąranką, sistemos atnaujinimo procesus, suprasti sistemos vietą tinkluose, nustatyti tinkamas darbų priėmimo procedūras, kurias jie gali panaudoti saugos lygiui padidinti, taip pat kitų asmenų ir šalių poreikiams ir interesams užtikrinti.

- **Etikos**. Asmens teisės ir teisėti interesai turi būti gerbiami ir ginami. Kadangi informacinės sistemos ir tinklai plačiai naudojami mūsų visuomenėje, šalys turi suvokti, kad jų aktyvūs veiksmai arba neveikimas gali sukelti žalą kitiems asmenims arba organizacijoms. Todėl labai svarbu elgtis etiškai, šalys turi naudoti darbo metodus, sukursiančius tokią aplinką, kurioje asmeniui naudinga gerbti kitų asmenų interesus, kad nebūtų pažeistos jo paties teisės.

- **Saugos valdymo.** Priemonės, procedūros ir informacinių sistemų saugos praktika turi būti įvertinta ir aptarta įvairiais požiūriais. Saugos valdymas turi remtis rizikos veiksnių įvertinimu. Šis įvertinimas turi būti dinamiškas, apimti visas organizacijos veiklos sferas. Jis turi numatyti galimas grėsmes, jų išvengimo, avarinio atstatymo priemones, nepertraukiamą techninį aptarnavimą, analizę ir auditą. Informacinių sistemų ir tinklų saugos politika, praktika, priemonės ir procedūros turi būti koordinuojamos ir integruotos, kad sukurtų logišką ir struktūriškai vientisą saugos valdymo sistemą. Saugos valdymo reikalavimai priklauso nuo šalių lygio, vaidmens ir funkcijų, rizikos veiksnių bei reikalavimų, keliamų pačiai sistemai.

- **Rizikos įvertinimo.** Saugos lygis, kaina, praktika ir procedūros turi atitikti informacinės sistemos reikšmę ir galimos žalos riziką. Šalys turi įvertinti galimus rizikos veiksnius. Vertinant išaiškinamos grėsmės ir pažeidžiamos vietos, be to, vertinimas turi apimti visą sistemą. Tokio įvertinimo metu sudaryta trūkumų ataskaita leis nustatyti vadinamąjį „priimtinos rizikos“ lygį ir padės pasirinkti tinkamas priemones ir metodus, gebančius valdyti kritines situacijas. Be abejo, būtina atsižvelgti į saugomos informacijos pobūdį ir svarbą. Jungiant informacines sistemas, vertinant riziką, privalu numatyti ir galimą žalą, kuri gali kilti iš

kitų asmenų, organizacijų arba gali būti sukelta pastariesiems.

• **Sistemų ir tinklų kūrimo bei projektavimo atsižvelgiant į saugos valdymą**. Šalių naudojamos priemonės, procedūros ir informacinių sistemų saugos praktika turi būti derinama ir koordinuojama. Šalys saugą privalo vertinti kaip vieną iš svarbiausių informacinių sistemų ir tinklų elementų. Norint užtikrinti tinkamą saugos lygį, būtina atitinkamai koordinuoti sistemų bei tinklų kūrimo ir eksploatavimo darbus. Vienas iš galimų sprendimų – įdiegti į sistemą atitinkamas saugos priemones, skirtas eliminuoti arba apriboti potencialios žalos grėsmę arba padarinius, galinčius kilti dėl neišaiškintų grėsmių ar pažeidimų. Šiuo tikslu būtini atskiri techninio, organizacinio bei teisinio pobūdžio sprendimai. Pastarieji turi priklausyti nuo sistemose ar tinkluose saugomos informacijos vertės. Saugos valdymas turi būti pagrindinė visų produktų, paslaugų, sistemų ir tinklų savybė, taip pat neatskiriama sudėtinė visų projektų ir sistemų architektūros dalis.

• **Reagavimo laiku**. Keliamas reikalavimas derinti viešojo ir privačiojo sektoriaus interesus, siekiant tinkamai reaguoti į informacinių sistemų saugos pažeidimus. Būtina skatinti suvokimą, kad informacinėms sistemoms ir tinklams dėl jų tarpusavio sąryšių ir priklausomybės per labai trumpą laiką gali būti padaryti dideli pažeidimai. Todėl šalys turi gebėti laiku reaguoti į tokius saugos pažeidimus. Jos turi keistis žiniomis apie grėsmes ir pažeidžiamas vietas, taip pat sukurti procedūras, numatančias greitą ir veiksmingą ryšio valdymą aptikus tokius pažeidimus bei juos užkardant. Šioje srityje rekomenduojamas tarpvalstybinis bendradarbiavimas.

• **Peržiūros (įvertinimo).** Šalys privalo analizuoti ir pakartotinai vertinti informacinių sistemų ir tinklų saugą, taip pat keisti saugos politiką, praktiką, priemones ir procedūras priklausomai nuo gyvenimo realijų, kadangi nuolat atsiranda naujos grėsmės ir pažeidžiamos vietos. Šalys privalo nuolat nagrinėti, pakartotinai įvertinti ir keisti saugos valdymo priemones.

• **Demokratijos.** Informacinių sistemų sauga turi būti suderinama su informacijos teisėto naudojimo ir laisvo duomenų judėjimo principais demokratinėje visuomenėje. Sauga turi būti užtikrinama taip, kad ji atitiktų demokratinėje visuomenėje pripažintas vertybes.

Šiems principams įgyvendinti turi būti kuriama valstybinė strategija, tvirtinama organizacijos (institucijos) saugos politika, priimamos naujos teisės normos dėl:

1) techninių standartų, metodų ir praktikos taisyklių suderinimo;
2) kompetencijos ir geriausios praktikos kūrimo;
3) sutarčių ir kitų dokumentų, susijusių su informacinių sistemų atsiradimu ir jų teisėtumu;
4) rizikos ir atsakomybės dėl informacinių sistemų saugos susilpnėjimo pasiskirstymo;
5) baudžiamosios, administracinės ar kitokios atsakomybės neišvengiamumo už neteisėtą, neteisingą informacinių sistemų naudojimą;
6) teismų jurisdikcijos ir kompetencijos;
7) savitarpio pagalbos ir ekstradicijos priemonių tarptautiniuose santykiuose;
8) įrodymų rinkimo informacinėse sistemose ir tokių įrodymų leistinumo teisminiuose ginčuose.

OECD rekomendacija siekia paaiškinti dažnai besikeičiančius saugos reikalavimus, ugdyti visuomenės kultūrą saugos srityje, o taip pat naujovišką mąstymą ir elgesį kuriant ir eksploatuojant informacines sistemas. Sauga būtina pasirūpinti dar tik kuriant tinklus ir informacines sistemas. Siūloma keisti požiūrį, kada saugos problemas bandyta spręsti tik įvykus pažeidimo faktui. Šiandien, kai didžioji visuomenės dalis daugiau ar mažiau priklauso nuo sklandaus informacinių sistemų darbo bei jų teikiamų paslaugų, saugos reikalavimai iškyla į pirmąją vietą. Sauga privalo būti įgyvendinama tiktai atsižvelgus į šalių teises ir laisves bei pagrindines sistemos savybes ir teikiamas paslaugas. Šalys, priklausomai nuo savo vaidmens ir funkcijų, turi būti informuotos apie atitinkamus rizikos veiksnius ir taikomas prevencines priemones, jos turi atsakyti ir imtis priemonių informacinių sistemų saugai užtikrinti. Tam, kad visuomenėje, valstybėje vyrautų rekomendacijos leidėjo pageidaujamas elgesys, būtina, kad saugos naudą suvoktų dalyvaujančios šalys. Šiuo atveju labai svarbus yra ir šalių tarpusavio bendradarbiavimas saugos planavimo ir tinkamo koordinavimo klausimais. Šiais klausimais privalo domėtis ir viešasis, ir privatusis sektoriai. Reikia pabrėžti, kad rekomendacija tik sudaro prielaidas, o jos pagrindu turi būti kuriama saugos kultūra visuomenėje. Rekomendacijos įgyvendinimo plane, patvirtintame 2003 m. liepos 2 d. OECD darbo grupės posėdyje [5], vienareikšmiškai apibrėžiami ir nustatomi Vyriausybės ir jos institucijų vaidmuo bei įgaliojimai informacijos ir informacinių sistemų saugos valdymo ir įgyvendinimo srityje. Reikia pastebėti, kad Lietuvos Respublika nėra OECD narė, todėl šios rekomendacijos nuostatos nėra įgyvendintos mūsų valstybės teisinėje sistemoje. Autoriaus nuomone, atsižvelgiant į šios rekomendacijos reikšmę ir svarbą, pabrėžiamą įvairių tarptautinio koordinavimo dokumentų turinyje, tikslinga priimti Lietuvos Respublikos informacijos ir tinklų saugos įstatymą, kuriame būtų įgyvendintos šioje rekomendacijoje įtvirtintos pamatinės nuostatos.

1.2. Europos Sąjungos teisinio reguliavimo analizė

Gerai subalansuotos informacijos saugos politikos realizavimas yra viena iš priemonių pasiekti Europos Sąjungos (toliau – ES) numatytus informacinės visuomenės plėtros tikslus. ES informacinės visuomenės vizija – visuomenė, kurioje nėra kliūčių laisvam informacijos plitimui ir vieningos rinkos egzistavimui, todėl būtina užtikrinti pasitikėjimą sistema, o informacijos saugos priemonės padeda siekti šių tikslų.

ES institucijos priėmė keletą dokumentų, iš kurių reikėtų išskirti 1997 m. Ministrų konferencijos deklaraciją [6], pabrėžiančią būtinumą plėtoti saugos priemones. Šioje deklaracijoje kaip svarbiausios saugos priemonės pažymimos šifravimo priemonės. Pasak deklaracijos, būtina sukurti techninę ir teisinę aplinką, tinkamą naudoti elektroninį parašą ir kitas priemones. Deklaracijoje akcentuojama, kad:

a) įvairių asmenų atsakomybė, susijusi su duomenų sukūrimu ir panaudojimu, turi būti aiškiai atskirta;

b) tarpininkai, tokie kaip tinklo operatoriai ir prieigos suteikėjai, bendruoju atveju neturėtų būti atsakingi už duomenų turinį;
c) atsakomybės samprata turėtų būti siejama su laisvės reikšti savo įsitikinimus principu, viešų ir privačiųjų interesų gerbimu ir neturėtų sukelti papildomų nepagrįstų sunkumų dalyviams.

Taip pat pažymėtinas 1992 m. kovo 31 d. Tarybos sprendimas *Dėl informacinių sistemų apsaugos* (92/242/EEB), kuriuo priimtas veiksmų planas informacinių sistemų apsaugos srityje.

Vienas iš svarbiausių dokumentų, numatantis duomenų saugos nuostatas ES, yra 1995 m. spalio 24 d. Europos Tarybos ir Europos Parlamento direktyva 95/46/EB *Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo* [7]. Šio dokumento tikslas – užtikrinti asmens duomenų tvarkymą, kartu skiriant nemažai dėmesio duomenų saugos suderinimui. Numatomi tokie pagrindiniai duomenų saugos principai:

1. Duomenų saugos optimizavimo ir tikslų bei priemonių proporcingumo. Direktyvos 17 str. teigiama, kad „atsižvelgus į technologijų lygį ir jų įdiegimo išlaidas, minėtos priemonės turi užtikrinti tokį saugos lygį, kuris atitiktų tvarkymo keliamą riziką ir saugotinų duomenų pobūdį“;

2. Duomenų sauga turi būti užtikrinta nepriklausomai nuo to, kur ir kieno duomenys yra saugomi ir apdorojami viso proceso, taip pat ir jų perdavimo metu;

3. Aiškios atsakomybės nustatymo ir kontrolieriaus galutinės duomenų saugos atsakomybės. Turi būti aiškiai atskirtos kontrolieriaus ir informacijos apdorojimą atliekančių atsakomybės ribos ir sąlygos. Kontrolierius turi atsakyti už darbo trūkumus, nes jis turi įgaliojimus tikrinti duomenų apdorojimo proceso eigoje dalyvaujančius asmenis ir priemones ir įsitikinti jų kvalifikacija.

4. Bene svarbiausias principas teigia, jog valstybės narės administraciniais aktais turi užtikrinti efektyvų duomenų saugos įpareigojimų vykdymą ir kontroliuoti, kaip jų teritorijoje taikomos pagal šią direktyvą valstybių narių priimtos nuostatos.

Žalioji informacinių sistemų saugos knyga įtvirtina nuostatas, į kurias reikia atsižvelgti kuriant informacinių sistemų saugos teisinę aplinką, kuri apima teisinių įpareigojimų (teisių, pareigų), atsakomybės, elektroninių duomenų saugos prievolių sukūrimą. Šis dokumentas numato, jog turi būti kuriamos naujos ir analizuojamos egzistuojančios teisės normos ir taisyklės, kuriami nauji teisiniai santykiai, kad galima būtų valdyti situaciją ateityje. Žalioji knyga reikalauja aktyviai kurti informacijos saugos teisės normas, susijusias su sparčiais technologiniais pasikeitimais. Teigiama, kad informacijos saugos reglamentavimas negali būti kuriamas reaguojant į įvykius (t. y. kuriamas taisant problemas, kurios įvyko praeityje). Pasak Žaliosios knygos, privalu aplenkti technologijų pokyčius. Žalioji knyga nepateikia kokių nors konkrečių patarimų dėl informacijos saugos formos ar turinio, tačiau ji pabrėžia, kad OECD direktyva *Dėl informacinių sistemų saugos* yra pamatas, ant kurio gali būti kuriama tolimesnė teisinė aplinka [8, p. 108].

Europos Parlamentas ir Taryba 2004 kovo 10 d. reglamentu įsteigė Europos tinklų ir informacijos saugumo agentūrą (ENISA) [9], kuri padės Europos Komisijai ir valstybėms narėms atitikti tinklų ir informacijos saugos teisinio reguliavimo reikalavimus [10]. Agentūra bus atsakinga už Europos Parlamento ir Tarybos direktyvos *Dėl elektroninių komunikacijų ir paslaugų erdvės reikalavimų* įgyvendinimą, už bendravimą su privačiu sektoriumi bei užsiims Europos Bendrijos ateities teisinio reguliavimo suvienodinimo klausimais vieningoje Europos Sąjungos rinkoje.

Išanalizavus egzistuojančias ES iniciatyvas informacijos saugos srityje, autoriaus nuomone, galima teigti, kad šiandien didžioji jų dalis yra neprivalomo pobūdžio ir pagrindinį dėmesį skiria tokiems klausimams, kaip programinės įrangos autorystės teisė, asmens duomenų apsauga. Dar daugiau, didžiosios dalies šalių narių įstatymų leidėjai daugiausia dėmesio skiria atsakomybės už neteisėtą informacijos ir duomenų panaudojimą klausimams, užuot skatinusi ir diegusi prevencines, profilaktines priemones [11, p. 20].

2. JUNGTINIŲ AMERIKOS VALSTIJŲ TEISINIO REGULIAVIMO ANALIZĖ

Teisinis reguliavimas, susijęs su Jungtinių Amerikos Valstijų (JAV) viešajame sektoriuje tvarkomos informacijos konfidencialumu, labai įvairus. Nustatyta daug įpareigojimų tiesiogiai su informacija dirbantiems asmenims arba institucijoms pagal tvarkomos informacijos saugos lygį bei nuostatos, kad tokia informacija turi būti apdorota pagal jos turinio klasifikavimo taisykles. Tačiau šiuo metu tokių taisyklių arba iš viso nėra, arba jos neapima visos valstybiniame sektoriuje tvarkomos informacijos [12]. Kuriant, derinant informacijos saugos branduolį sudarančias funkcijas, užduotis, būtina atlikti ekonominį grėsmių, rizikos veiksnių ir išlaidų, prevencijos priemonių įvertinimą. Šiuo atveju taip pat būtina pabrėžti, kad nepagrįstos, neduodančios atitinkamų rezultatų sąnaudos yra nepageidaujamos.

JAV praktika, susijusi su kompiuterinio saugumo įstatymo nuostatų įgyvendinimu, rodo, kad praktiniame gyvenime nėra taip lengva įgyvendinti privatumo ir nacionalinio saugumo sektorių reikalavimus. Šiame teisės akte numatyta, kad Nacionalinis standartų ir technologijų institutas (toliau – NIST) padės „kiek sugeba“ Nacionalinei saugos agentūrai (toliau – NSA) sukurti standartus ir direktyvas, būtinas užtikrinti „jautrios“ informacijos saugą ir privatumą Federalinėse kompiuterinėse sistemose [13]. Šiuo metu jau žinoma, kad kurdamos šiuos standartus NIST ir NSA labai retai sutaria dėl nagrinėjamų klausimų. Problemų kyla dėl to, kad NIST yra civilinė įstaiga, besiorientuojanti į kaštais pagrįstus saugos valdymo kriterijus, o NSA yra karinė įstaiga, siekiant besąlyginio saugos valdymo [14, p. 208].

JAV gynybos departamentas daugybę metų stengiasi rasti būdų užtikrinti klasifikuotų duomenų saugą. Ypatingas dėmesys skiriamas vienai iš saugos savybių – t. y. duomenų konfidencialumui [15; p. 74]. Vykdydamas šią veiklą Gynybos departamentas priėmė *Patikimų kompiuterinių sistemų plėtros kriterijus*, alternatyviai vadinamus „Oranžine knyga“ [16]. Šie dokumentai, ko gero, – vieni iš pagrindinių teisės aktų, kuriais vadovaujamasi JAV, užtik-

rindama automatizuotų informacinių sistemų duomenų konfidencialumą.

Toliau nagrinėjant informacijos saugos reguliavimo ypatumus JAV, būtina atkreipti dėmesį į tai, kad JAV vyrauja *informacijos laisvės* principas, o Europoje – *informacijos ribojimo* (*draudimo*). Iš tiesų sunku palyginti skirtingus požiūrius ir sistemas. Minėta direktyva 95/46/EC numato asmens duomenų, saugomų Europos Sąjungos valstybių kompiuterinėse sistemose, kontrolę. Vienas iš svarbiausių yra apribojimas tarpvalstybinio duomenų perdavimo į valstybę, kurioje nėra tinkamo asmens duomenų teisinės apsaugos lygio, t. y. lygio, kuris atitinka Europos Sąjungos standartus. Šiuo atveju Europoje galioja visa apimantis (*holistinis*) principas, kad „vienas taikomas viskam“. JAV požiūris apibūdintinas kaip „sektorinis“, ten situacija yra daug įvairesnė: reglamentavimas teisės aktais, neteisinis reguliavimas ir savireguliacija [17, p. 430]. Dėl tokio griežto reguliavimo Europos direktyvų nuostatos labai dažnai tiesiog ignoruojamos JAV.

3. ELEKTRONINĖS INFORMACIJOS SAUGOS NUOSTATŲ ĮGYVENDINIMAS LIETUVOJE

Lietuvos Respublika ilgai neturėjo ilgalaikės informacinių technologijų plėtros strategijos. 1990–2000 m. ne kartą keitėsi institucijos, atsakingos už šios srities politikos įgyvendinimą mūsų valstybėje, dėl to valstybės politika šioje srityje tapo išbalansuota ir silpnai koordinuojama. Galima sakyti, kad pirmą kartą šiuo klausimu rimtai susidomėta tik 2000 m., kai buvo atliktas pirmas valstybės informacinės infrastruktūros situacijos įvertinimas. Viena iš pagrindinių šio vertinimo sričių buvo informacijos saugos suvokimo lygis, šios srities politika ir tuometinis vyriausybinių įstaigų apsaugos laipsnis. Įvertinimas nurodė esamos informacinės infrastruktūros trūkumus, o būtent – kad daugumoje vyriausybinių įstaigų apskritai informacijos apsauga yra prasta. Informacijos saugos kontrolė tuo metu buvo labai silpna. Beveik visų sričių saugą reikėjo tobulinti, norint apsaugoti informacijos infrastruktūrą nuo išpuolių, galinčių pakenkti Vyriausybės įstaigų veiklai. Viena iš svarbiausių blogos apsaugos priežasčių buvo nesuvokimas, kad rūpintis sauga yra būtina. Galima paminėti ir kitų priežasčių, pvz., nepatyrusius saugos srityje dirbančius specialistus bei finansavimo trūkumą – saugai užtikrinti reikalingos lėšos.

Būtina pabrėžti, kad išskirtinis valstybinio sektoriaus informacinių sistemų bruožas – būtinumas griežtai ir centralizuotai nustatyti tiesioginio valdymo ir kontrolės principus. Šiuo atveju būtinas saugos lygis turi būti nustatomas pirmiausia atsižvelgus į valstybės nacionalinio saugumo interesus, o tik po to – į galimas išlaidas. Todėl informacijos technologijų saugos svarbą bene pirmą kartą valstybiniu mastu Lietuvos institucijose nurodė Informacijos technologijų saugos valstybinė strategija, patvirtinta 2001 m. gruodžio 22 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1625 [18]. 2001–2004 m. vykdant patvirtintą šios strategijos įgyvendinimo planą, nauja redakcija buvo išdėstyti Bendrieji duomenų saugos reikalavimai, patvirtinti Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 [19]. Lietuvos Respublikos Vyriausybės nutarimu buvo patvirtintos naujos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės [20], Lietuvos Respublikos vidaus reikalų ministerija parengė ir patvirtino Tipinius duomenų saugos nuostatus [21], Informacijos klasifikavimo pagal duomenų grupes rekomendacijas [22], Saugaus valstybinio duomenų perdavimo tinklo nuostatus bei Saugaus valstybinio duomenų perdavimo tinklo paslaugų teikimo taisykles [23] (Saugaus valstybinio duomenų perdavimo tinklo operatoriaus funkcijos buvo pavestos valstybės įmonei „Infostruktūra“), Informacinių technologijų saugos atitikties vertinimo metodiką [24] bei Interneto tarnybinių stočių apsaugos rekomendacijas [25]. Šiuo laikotarpiu taip pat įsteigtas padalinys saugumo priežiūros tarnybos funkcijoms vykdyti bei patvirtintos Laikinų leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės [26]. Taip pat nagrinėjamu laikotarpiu kiekvienos organizacijos, nusprendusios užtikrinti savo IT saugą, parankine knyga tapo 2002 m. liepos 1 d. įsigaliojęs Lietuvos standartas „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“, tapatus tarptautiniam standartui ISO/IEC 17799:2000, kuris 2004 m. buvo išverstas į valstybinę kalbą ir patvirtintas. Šis standartas nurodo gerąją praktiką, kuria vadovaudamosis organizacijos turi kurti savo informacijos saugos politiką.

Šiandien daug nuostatų iš Informacijos technologijų saugos valstybinės strategijos dar neįgyvendintos:

a) elektroninio verslo saugos klausimus nagrinėja tik privačia iniciatyva įsteigtas interneto portalas eSecurity.lt [27][1], nors Lietuvos Respublikos Vyriausybė 2001 m. birželio 25 d. posėdyje (protokolo Nr. 30, 27 klausimas) patvirtino Elektroninio verslo koncepciją;
b) nesukurta metodologinė ir konsultacinė informacinių technologijų, sistemų ir informacijos saugos sistema;
c) strategijoje kalbama apie duomenų saugos įgaliotinių pareigybės įvedimą ir mokymą. Šiuo metu situacija valstybės įstaigose tokia, kad tokių pareigybių arba iš viso nėra, arba ši pareigybė tik formali, papildoma, pvz., informacinės sistemos administratoriaus funkcija;
d) nesukurta vieninga tokių tarnautojų rengimo sistema.

Šioje srityje vis dar trūksta aiškios, koordinuotos valstybės politikos, informacinių technologijų ir informacijos saugą reglamentuojanti teisinė bazė nenustato vienodų ir aiškių reikalavimų informacinių sistemų valdytojams. Taip pat dėl šiuo metu galiojančių teisinių nuostatų gyvuoja skirtinga praktika atskirose valstybinėse institucijose. Skirtingas teisės normų interpretavimas neleidžia sukurti bendros informacinių technologijų ir informacijos saugos politikos bei užtikrinti efektyvios informacinių sistemų valdytojų kontrolės.

[1] Straipsnį rengiant Ryšių reguliavimo tarnybos, Vidaus reikalų ministerijos ir kitų partnerių pastangomis buvo įvykdytas naujas projektas Esaugumas (www.esaugumas.lt).

Autoriaus nuomone, šiandien visuomeninių santykių sritis nepakankamai reguliuojama pamatinėmis teisės normomis. Be autoriaus siūlomo priimti Lietuvos Respublikos informacijos ir tinklų saugumo įstatymo, kuriame turėtų būti įtvirtinti pagrindiniai tarptautinio koordinavimo dokumentuose nurodyti principai, Lietuvos Respublikai reikalinga nauja Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija, kurioje būtų galima numatyti autoriaus nagrinėtų tarptautinio reguliavimo dokumentų nuostatų praktinį įgyvendinimą mūsų valstybėje. Ši strategija padėtų kurti Lietuvos Respublikoje saugią informacinę visuomenę. Strategija taip pat turėtų skatinti bendradarbiavimą informacinių technologijų saugos klausimais nacionaliniu ir tarptautiniu lygiu, prisidėti prie Lietuvos informacinių technologijų ir telekomunikacijų operatorių potencialo ir kompetencijos ugdymo, gerinti ir užtikrinti informacijos saugos rizikos valdymą, užtikrinti pagrindinių žmogaus ir piliečio teisių, laisvių ir teisėtų interesų bei nacionalinio žinių potencialo apsaugą ir plėtoti visuomenės informacinių technologijų saugos klausimų sampratą. Vienas iš svarbesnių uždavinių – valstybės institucijų informacinių sistemų ir jose tvarkomos informacijos klasifikavimas priklausomai nuo kylančių ir esamų grėsmių bei sistemos ir joje tvarkomos informacijos svarbos asmenims, įstaigai, visai visuomenei ar valstybei. Todėl būtina nuspręsti dėl valstybinės informacijos saugos klausimus koordinuosiančios institucijos paskyrimo, nustatyti konfidencialios informacijos prioritetus, išplėsti kontrolės tarnybos funkcijas bei spręsti klausimą dėl atsakomybės už neteisėtą duomenų tvarkymą ir nusikaltimus informatikai griežtinimo. Autoriaus nuomone, taip pat tikslinga iš esmės peržiūrėti organizacijos informacijos saugos politiką sudarančių dokumentų rengimo tvarką, atsisakant šiuo metu galiojančių Tipinių duomenų saugos nuostatų. Šiuo tikslu reikėtų parengti ir poįstatyminiu teisės aktu patvirtinti naujas Informacijos saugos politiką sudarančių dokumentų rengimo gaires. Jų pagrindu kiekviena valstybinė institucija parengtų savo informacijos saugos politiką sudarančius dokumentus. Atsižvelgiant į informacinių sistemų integruotumą ir tarpusavio priklausomybę bei Europos Komisijos 1994 m. rekomendaciją Nr. 820 [28], kuria patvirtinta Europinė elektroninių duomenų apsikeitimo sutarties forma, autoriaus nuomone, taip pat rekomenduotina patvirtinti naują Saugaus apsikeitimo automatiniu būdu duomenimis tarp valstybinių institucijų sutarties formą, kuri prievolinių santykių tarp institucijų pagrindu gebėtų užtikrinti informacinių sistemų ir duomenų saugos reikalavimų vykdymą perduodant duomenis automatiniu būdu.

IŠVADOS

1. Pagrindinis informacinių technologijų ir informacijos saugos tikslas yra apsaugoti ir užtikrinti informacinės sistemos ir joje tvarkomos informacijos konfidencialumą, vientisumą ir prieinamumą. Todėl tikslinga aiškiai atskirti nuostatas, tiesiogiai susijusias su informacijos sauga, nuo tų, kurios tik netiesiogiai su sauga siejasi. Kitas klausimas, kaip išsamiai šiuos klausimus turi reglamentuoti teisė ir kokią vietą valstybės teisinėje sistemoje turėtų užimti tokios normos.

2. Šiuo metu vis dar trūksta aiškios, koordinuotos valstybės politikos šioje srityje. Būtina nuspręsti dėl valstybės informacijos saugos klausimus koordinuojančios institucijos paskyrimo. Informacijos saugos politiką valstybėje turėtų koordinuoti viena nepriklausoma įstaiga prie Lietuvos Respublikos Vyriausybės. Vienas iš svarbesnių uždavinių – valstybės institucijų informacinių sistemų ir jose tvarkomos informacijos klasifikavimas priklausomai nuo kylančių ir esamų grėsmių faktoriaus bei sistemos ir joje tvarkomos informacijos svarbos asmenims, įstaigai, visai visuomenei ar valstybei. Atsižvelgiant į duomenų vientisumui, prieinamumui ir konfidencialumui keliamus didelius reikalavimus, strateginės svarbos ir komercinę naudojamose informacinėse sistemose sukauptos informacijos vertę, būtina atlikti naudojamų informacinių technologijų ir informacinių sistemų saugos peržiūrą.

3. Ši visuomeninių santykių sritis per mažai reguliuojama pamatinėmis teisės normomis, todėl informacijos saugai reguliuoti valstybėje tikslinga priimti Lietuvos Respublikos informacijos ir tinklų saugos įstatymą, kuriame turėtų būti įtvirtinti pagrindiniai tarptautinio koordinavimo dokumentuose nustatyti principai. Lietuvos Respublikai šiandien taip pat reikalinga nauja Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija, kuri numatytų minėtų tarptautinio reguliavimo dokumentų nuostatų praktinį įgyvendinimą mūsų valstybėje, nustatytų konfidencialios informacijos prioritetus. Taip pat būtina išplėsti kontrolės tarnybos funkcijas bei išspręsti klausimą dėl atsakomybės už neteisėtą duomenų tvarkymą ir nusikaltimus informatikai griežtinimo.

4. Autoriaus nuomone, taip pat tikslinga iš esmės pertvarkyti informacijos saugos politiką sudarančių dokumentų rengimą, atsisakant šiuo metu galiojančių Tipinių duomenų saugos nuostatų. Šiuo tikslu reikėtų parengti ir poįstatyminiu teisės aktu patvirtinti naujas Informacijos saugos politiką sudarančių dokumentų rengimo gaires. Jų pagrindu kiekviena valstybinė institucija parengtų savo informacijos saugos politiką sudarančius dokumentus. Atsižvelgiant į informacinių sistemų integruotumą ir tarpusavio priklausomybę bei Europos Komisijos 1994 m. rekomendaciją Nr. 820, kuria patvirtinta Europinė elektroninių duomenų apsikeitimo sutarties forma, autoriaus nuomone, taip pat rekomenduotina patvirtinti naują Saugaus apsikeitimo automatiniu būdu duomenimis tarp valstybinių institucijų sutarties formą, kuri prievolinių santykių tarp institucijų pagrindu gebėtų užtikrinti informacinių sistemų ir duomenų saugos reikalavimų vykdymą perduodant duomenis automatiniu būdu.

LITERATŪRA

1. **Legal Aspects** of Information Security in the Nordic Countries // Nordiske seminar-og Arbejds-rapporter.
2. **The Encyclopedi**a of Computer Security // http://www.itsecurity.com/dictionary/dictionary.htm.
3. **Computer Security** Act,1987, Computer Security Legislation, Law and Crime,USA. // http://nsi.org/Library/Compsec/compact.txt.

4. **Bigelow R.** Computer Security, Crime and Privacy, in the USA // Part 8 Computer Law & Security Report.
5. **Joyner C. C., Lotrionte C.** Information Warfare as International Coercion: Elements of a Legal Framework. National Security Studies Program, Georgetown University. // EJIL (2001). Vol. 12. No. 5.
6. **An Advanced** Workshop on Information security law & practices: Regulatory compliance, secure electronic commerce, emerging security liability and litigation best regulations, strategies and litigation. // http://www.lawseminars.com/htmls/seminars/03dataca.
7. **The Frontiers** of Privacy and Security: New Challenges for a New Century // https://cits.gov.bc.ca/popt/Security_Services/ conference/feb2003/default.htm#feb14_information.
8. **Project S2005:** Legislation/Regulation on Information Security – „Harmonisation Proposals".
9. **Data security** and law: Perspectives on the Legal Regulation of Data Security. Saarenpää A., Pöysti T. The Institute of Legal Informatics University of Lapland 1997.
10. **Information** security: recommended practices for United nations organizations. Administrative Committee on Coordination Information Systems Coordination Committee (ISCC). ACC/1994/ISCC/18 4 November 1994**.**
11. **Rasch M. D.** Computer security: Legal Lessons in the Computer Age. Security Management, April, 1996.
12. **Cailloux J. P. and Roquilly C.** Legal Security of Web Sites: Proposal for a Legal Audit Methodology and a Legal Risks Classification // The Journal of Information, Law and Technology (JILT). 2001. 2.
13. **Thomas R.** Mylott III. Computer Law for the Computer Professional. – Prentice Hall, 1984.
14. **Trusted Computer** Systems Evaluation Criteria (Orange Book) // http://nsi.org:16080/Library/Compsec/orangebo.txt.
15. **Cronin K. P., Weikers R. N.** Data Security and Privacy Law: Combating Cyberthreats. – West Group, USA, 2002.
16. **OECD** Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data, 1980.
17. **OECD** Recommendation of the Council concerning guidelines for criptography policy,1997.
18. **OECD** Recommendation of the Council concerning guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002.
19. **United Nations** General Assembly Resolution A/RES/ 57/239 for „Creation of a Global Culture of Cyber Security" established in December of 2002.
20. **Working Party** on Information Security and Privacy Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. 02-Jul-2003 DSTI/ICCP/REG(2003)5/ REV1.
21. **Ministerial Declaration** „Global Information Networks", Ministerial Conference, Bonn 6-8 July 1997.
22. **Green Book,** Draft 4.0. // http://nsi.org/Library/Compsec/ greenbk.txt.
23. **Commission** recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange (Text with EEA relevance) (94/820/EC).
24. **Regulation** (EC) No 460/2004 of the European parliament and of the Council of 10th march 2004 establishing the european network and information security agency.
25. **Directive** 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).
26. **Europos Parlamento** ir Tarybos 1995 m. spalio 24 d direktyva 95/46/EB Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo // OJL Nr. 281, 23.11.1995.
27. **Lietuvos Respublikos** Vyriausybės 2001 m. gruodžio 22 d. nutarimas Nr. 1625 Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo // Valstybės žinios. 2001. Nr. 110-4006; 2002. Nr. 80-3429.
28. **Lietuvos Respublikos** Vyriausybės 1997 m. rugsėjo 4 d. nutarimas Nr. 952 Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose // Valstybės žinios. 1997. Nr. 83-2075; 2003. Nr. 2-45.
29. **Lietuvos Respublikos** Vyriausybės 2004 m. balandžio 19 d. nutarimas Dėl Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo // Valstybės žinios. 2004. Nr. 58-2061.
30. **2003 m. liepos 16 d.** Lietuvos Respublikos vidaus reikalų ministro įsakymas Nr. 1V-272 Dėl Tipinių duomenų saugos nuostatų patvirtinimo // Valstybės žinios. 2003. Nr. 76-3511.
31. **2003 m. sausio 27 d.** Lietuvos Respublikos vidaus reikalų ministro įsakymas Nr. 1V-33 Dėl Informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo // Valstybės žinios. 2003. Nr. 77-3541.
32. **2004 m. gegužės 14 d.** Lietuvos Respublikos vidaus reikalų ministro įsakymas Nr. 1V-167 Dėl Saugaus valstybinio duomenų perdavimo tinklo nuostatų ir Saugaus valstybinio duomenų perdavimo tinklo paslaugų teikimo taisyklių patvirtinimo // Valstybės žinios. 2004. Nr. 83-3025.
33. **2004 m. gegužės 6 d.** Lietuvos Respublikos vidaus reikalų ministro įsakymas Nr. 1V-156 Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo // Žin., 2004, Nr. 80-2855.
34. **2004 m. gegužės 21 d.** Lietuvos Respublikos vidaus reikalų ministro įsakymas Nr. 1V-176 Dėl Interneto tarnybinių stočių apsaugos rekomendacijų patvirtinimo // Valstybės žinios. 2004. Nr. 85-3095.
35. **Laikinų leidimų** automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2002 m. gruodžio 30 d. įsakymu Nr. 604 // Valstybės žinios. 2003. Nr. 9-313.
36. www.esecurity.lt - eSecurity – „Ekskomisarų biuro" projektas, skirtas verslo saugumui užtikrinti.
37. **Волубев С. В.** Безопасность социотехнических систем. – Викинг, 2000.
38. **Черней Г. А., Охрименко С. А., Ляху Ф. С.** Безопасность автоматизированных информационных систем. – Ruanda, 1996.

INTERNATIONAL LEGAL PROVISIONS IN THE AREA OF ELECTRONIC INFORMATION SECURITY: ACCOMMODATION IN LITHUANIA

Doctoral Candidate Žydrūnas Paškauskas
Mykolas Romeris University

S u m m a r y

The confidentiality, authenticity, integrity, obligation and availability of information systems based information and processes are mission-critical for the operation of most large organizations – in many cases, these efforts are imposed by

legal and regulatory requirements. Technological development has multiplied and diversified the vectors for creation, production and exploitation information. The legal protection of technological measures applies without prejudice to public policy or public security. When applying the exceptions and limitations, they should be exercised in accordance with international and national obligations. Such exceptions and limitations may not be applied in a way which prejudices the legitimate interests of the right holder or which conflicts with the normal exploitation of his work or other subject matter. They should ensure, that right holders provide beneficiaries of such exceptions or limitations with appropriate means of benefiting from them, by modifying an implemented technological measure or by other means. Every country should provide effective sanctions and remedies for infringements of information security rights and obligations. The practice of OECD (Organisation for economic co-operation and development) in the field of information systems and information security and introduced the concept of a "culture of security" relating to safe information technology and Internet usage are observed in this article also. The most European countries security strategies are built on these guidelines.

Information technology security shall be a key factor governing information technology use by Lithuanian public sector, businesses and consumers. A culture of security shall be built around the development and deployment of information systems and electronic information exchange in Lithuania. The new national information security strategy will help Lithuania become an information secure society. The Government must designate key targets underpinning information security in society. Strategy must take into account security requirements for the specific type of data, information processing or systems that may be involved. This will, moreover, enhance efforts to safeguard critical infrastructures.

Regulations concerning information security shall be enforced and further developed in a coordinated manner, and made straightforward and easy for users to follow. All parties share responsibility for promoting awareness and understanding of information technology security issues, and for nurturing an emergent "culture of security" within society.

The main purposes of the article – to identify, analyze and evaluate the practise of European Union, USA and other countries for the legal regulation on information systems and information security and adopt that practice for Lithuanian state information systems and information security regulation. Conclusions relating to the legal regulation of information systems and information security are provided. The methods of descriptive, comparative and system analysis are used in this article.

Keywords: security legal standard, principles of security regulation, security policy, security strategy.