Vilniaus universitetas
Tarptautinis žinių ekonomikos ir žinių vadybos centras

Julija Mažuolienė
Informacijos vadybos studijų programos studentė

ES ĮTAKA LIETUVOS INFORMACIJOS SAUGUMO POLITIKAI

MAGISTRO DARBAS

Vadovas: Prof. R.Gudauskas

Vilnius, 2007

Magistro darbo lydraštis

_Julijos Mažuolienės_____magistro darbas
(magistranto (-ės) vardas, pavardė)

tema __ES įtaka Lietuvos informacijos saugumo politikai_____

parengtas gynimui.

_____ _____
(data) (vadovo parašas)

Darbas įregistruotas _____ centre

_____
(data) (administratorės parašas)

Magistro darbą ginti leidžiu

_____ (centro direktoriaus parašas) _____
(data)

Recenzentu skiriu _____

_____ _____
(data) (Direktoriaus parašas)

Darbą recenzavimui gavau

_____ _____
(data) (recenzento parašas)

Mažuolienė, Julija

Ma 742

Europos Sąjungos įtaka Lietuvos informacijos saugumo politikai: magistro darbas / Julija Mažuolienė; mokslinis vadovas prof. R.Gudauskas; Vilniaus universitetas. Tarptautinis žinių ekonomikos ir žinių vadybos centras. – Vilnius, 2007. – 73, [2] lap. – Santr. angl. The ompact of the EU on Lithuanian information security policy – Bibliogr.: p. 67-69 (41 pavad.).

UDK 004.056 (474.5)

Informacijos ir komunikacijos mokslas, informatikos mokslas, ES mokslas

Magistro *darbo objektas* – Lietuvos informacinės erdvės saugumo politika prieš ir po įstojimo į Europos Sąjungą. *Darbo tikslas* – įvertinti Lietuvos informacijos saugumo politiką iki įstojimo į ES ir išanalizuoti esamą informacijos saugumo politikos būklę, apimant informacinius, teisinius, ekonominius, socialinius aspektus. Pagrindiniai *darbo uždaviniai*: apibrėžti informacijos saugumo problematiką ir jos prielaidas Lietuvoje; nustatyti pagrindines informacijos saugumo spragas bei jų atsiradimo priežastis; išanalizuoti elektroninės erdvės galimybes ir grėsmes, tarp jų - teisinį el. ryšio reguliavimą ir kitus aspektus; apibendrinti pagrindinius sprendimus ir priemonės, kurios buvo ir yra taikomos informacijos ir elektroninės erdvės saugumui užtikrinti Lietuvoje ir ES; apibendrinti pagrindinius pokyčius, įvykusius šioje srityje po įstojimo į ES, t.y. informacinius, teisinius, socialinius ir ekonominius aspektus; įvertinti informacijos saugumo užtikrinimo galimybes ir grėsmes ateityje.

Naudojantis dokumentų analizės, bibliografiniu ir lyginamuoju *metodais* bei kokybiniu tyrimu, prieita *išvados*, kad Lietuvos informacijos saugumo politika yra įtakojama daugelio faktorių, kurie priklauso ne tik nuo Lietuvos stojimo į ES, bet ir nuo kitų stambių šalių, kaip JAV, Japonija, įtakos. Lietuvos, kaip ir kitų mažų valstybių informacijos saugumo politika priklauso nuo ekonomikos lygio, teisinio reguliavimo, informacijos ir interneto vartotojų budrumo ir sąmoningumo, IT specialistų kvalifikacijos, tarptautinio bendradarbiavimo ir finansinių galimybių įgyvendinti saugesnio elektroninio ryšio, tinklų ir informacijos saugumo programas, diegti naujausią įrangą ir prižiūrėti informacines sistemas.

Magistro darbas *gali būti naudingas* informacinių technologijų specialistams, informologijos, informacijos, komunikacijos disciplinų dėstytojams ir studentas, visoms institucijoms ir organizacijoms.

TURINYS

SANTRUMPŲ SĄRAŠAS

API – Atvira programų sąsaja

BIAC - Business and Industry Advisory Committee (Verslo ir pramonės patariamasis komitetas)

“BITE” – Telekomunikacijų bendrovė “Bite Lietuva”

BVP – Bendras vidaus produktas

CEN – European Committee of Standartization (Europos standartų komitetas)

CENELEC - European Committee for Electrotechnical Standardization (Europos Elektroninių standartų komitetas)

EBPO - Ekonominio bendradarbiavimo ir plėtros organizacija

EK – Europos Komisija

ENISA - European Network and Information Security Agency (Europos tinklų ir informacijos saugumo agentūra)

ES – Europos Sąjunga

ETSI - European Telecommunications Standards Institute (Europos telekominikacijų standartų institutas)

GATT - General Agreement on Trade and Tariffs (Bendras susitarimas dėl prekybos ir tarifų)

IDS – Intrusion Detection System (Įsibrovimų nustatymo sistema)

IRT – Informacinės ir ryšio technologijos

ITU - International Telecommunications Unijon (Tarptautinė telekomunikacijų sąjunga)

JAV – Jungtinės Amerikos Valstijos

OECD - Organisation for Economic cooperation and development (Ekonominio bendradarbiavimo ir plėtros organizacija)

RRT – Lietuvos Respublikos ryšių reguliavimo tarnyba

VRM – Lietuvos Respublikos vidaus reikalų ministerija

SVĮ – Saugos ir sveikatos vadovas

WPISP - Working Party on Information Security and Privacy (Informacijos saugumo ir privatumo darbo grupė)

ĮVADAS

Šiuolaikinių informacinių technologijų dėka informacija gali būti efektyviai apdorojama, saugoma ir perduodama greitais kompiuteriniais tinklais patogiausiu mums metu ir iš bet kurios pasaulio vietos. Tačiau svarbu yra užtikrinti saugų informacijos ir duomenų perdavimą, apsaugoti informaciją, kuri gali tapti kompiuterinių nusikaltimų įrankiu, siekiant moralinės bei materialinės žalos informacijos vartotojui, informacijos ir elektroninio ryšio paslaugų tiekėjams ar valstybei. Tai turi ypatingą svarbą Europos Sąjungai ir jos narėms, kurios bendradarbiauja ir veikia tarptautiniu lygmeniu. Visos operacijos, kurios vykdomos elektroninio ryšio ir informacinių technologijų pagalba turi būti patikimos ir tinkamai apsaugotos.

Saugus informacijos perdavimas tarp Europos Sąjungos šalių ir tų šalių viduje priklauso nuo daugelio principų, susijusiu su kompiuterio ir informacijos tinklų saugumu, vartotojų, elektroninio ryšio tiekėjų. Tačiau technologijos nuolat tobulėja ir Europos Sąjungos šalys privalo tai įvertinti bei kurti šiuolaikines strategijas informacijos bei elektroninio ryšio apsaugai. Todėl šio darbo tikslas yra išanalizuoti Europos Sąjungoje vyraujančią informacijos saugumo politiką, jos principus ir įgyvendinimo problemas.

Darbo objektas. Šio mokslo tiriamojo darbo *objektas* yra Lietuvos informacinės erdvės saugumo politika prieš ir po įstojimo į ES. Darbo *tikslas* - išanalizuoti Lietuvos informacijos saugumo politiką iki įstojimo į ES ir įvertinti esamą informacijos saugumo politikos būklę, apimant informacinius, teisinius, ekonominius, socialinius aspektus. Darbo *uždaviniai*: apibrėžti informacijos saugumo problematiką ir jos prielaidas Lietuvoje; nustatyti pagrindines informacijos saugumo spragas bei jų atsiradimo priežastis; išanalizuoti elektroninės erdvės galimybes ir grėsmes, apimant teisinį el. ryšio reguliavimą ir kitus aspektus; apibendrinti pagrindinius sprendimus ir priemonės, kurios buvo ir yra taikomos informacijos ir elektroninės erdvės saugumui užtikrinti Lietuvoje ir ES; išanalizuoti pagrindinius pokyčius, įvykusius šioje srityje po įstojimo į ES; informacinius, teisinius, socialinius ir ekonominius aspektus; įvertinti informacijos saugumo užtikrinimo galimybes ir grėsmes ateityje.

Iki šiol nebuvo vertinama kaip pasikeitė situacija po įstojimo į ES, kokias galimybes informacijos saugumo plėtrai atvėrė ES, kas pasikeitė per tris narystės metus, todėl tyrimas yra aktualus ir savalaikis. Tyrimai informacijos saugumo srityje atliekami nuo 2005 metų, tačiau jie apima tik statistinius duomenis ir atspindi interneto pavojus, nusikaltimų skaičių ir apsaugos priemonių naudojimą. Svarbu išanalizuoti

tai, kaip patys darbuotojai atsakingi už informaciją ir tinklų saugumą, todėl interviu yra tinkamas tyrimo metodas situacijai įvertinti.

Kokybinio tyrimo metu buvo apklausti valstybinių institucijų, kurios atsako už informacijos, tinklų, ryšio saugumą, asmens duomenų apsaugą, konfidencialios informacijos saugojimą, darbuotojai, taip pat ir privačios institucijos, kurios teikia paslaugas ir dirba informacinių technologijų, telekomunikacijų srityje.

Šalies informacijos vartotojų ir tiekėjų poreikis disponuoti saugia informacija nustatomas šio darbo pirmojoje dalyje, remiantis Lietuvoje atliktų tyrimų duomenimis. Kadangi naujos informacijos technologijos yra viena sparčiausiai besivystančių sričių, informacijos saugumu besirūpinančių institucijų ir organizacijų skaičius taip pat auga. Todėl nagrinėjant šią problemą, remiamasi kelių organizacijų, dirbančių informacijos saugumo srityje, atliktų tyrimų rezultatais. Tikimasi, kad tai sudarys platesnes gaires šios temos nagrinėjimui. Šioje dalyje taip pat analizuojamos asmens duomenų apsaugos problemos, intelektualios nuosavybės apsauga ir pateikiama su informacijos saugumu susijusi teisės aktų apžvalga, rekomendacijos, skirtos įstatymų įgyvendinimui užtikrinti ir informacijos apsaugai sustiprinti.

Antroje darbo dalyje analizuojamos elektroninės paslaugos, kuriomis vis plačiau ir dažniau naudojasi informacinės visuomenės dalyviai, jos lyginamos su tokių paslaugų naudojimusi kitose Europos Sąjungos šalyse. Šioje dalyje taip pat nagrinėjama ir elektroninių paslaugų saugumo kokybė, elektroninio pašto ir parašo pagrindiniai pavojai bei apsaugos priemonės.

Socialinės atsakomybės ugdymas yra vienas iš svarbiausių aspektų efektyvaus verslo, kompiuterinių nusikaltimų prevencijos, saugaus ir sąmoningo informacijos ir elektroninių paslaugų vartotojo link, todėl svarbu nustatyti šios atsakomybės ribas, mokėti atskirti nuo teisinių šios srities reglamentavimo normų ir nustatyti šio principo gaires. Darbe nurodomos šios gairės ir bandoma nustatyti, koks elgesys elektroninėje terpėje yra priimtinas ir vartotojams ir visuomenei.

Trečioje darbo dalyje analizuojama Europos Sąjungos informacinės visuomenės saugumo politika ir jos pasiekimai, Europos Komisijos veikla ir jos gairės šioje srityje. Šioje dalyje taip pat nagrinėjami Europos Sąjungos tikslai ir uždaviniai, kurių ji siekia ir tikslams pasiekti būtinos sąlygos bei priemonės, teisinė bazė, reglamentuojanti informacijos naudojimą, elektroninio ryšio apsaugos sistemą, duomenų srautus, telekomunikacijų naudojimą, informacinių technologijų plėtrą, asmens duomenų apsaugą, informacinių technologijų tiekimą bei informacijos perdavimą.

Tyrimo, kurio metu bandoma vertinti Lietuvos informacijos saugumo politiką po įstojimo į ES, rezultatai, jų interpretacija ir vertinimas pateikiami ketvirtoje darbo dalyje. Prieduose skelbiamas pavojingiausių interneto pažeidimų sąrašas ir pateikiami interviu metu užduoti klausimai.

Tema yra aktuali kiekvienam interneto vartotojui norint saugiai naudotis visomis globalaus tinklo galimybėmis, siekiant išvengti asmens duomenų vagystės, virusų atakų, nepageidaujamų laiškų. Ypatingą dėmesį informacijos ir tinklų saugumui turėtų skirti tos valstybinės ir privačios organizacijos, kurios renka konfidencialią informaciją, atlieka finansines operacijas, saugo duomenis.

Atliktas darbas gali būti naudingas informacijos ir elektroninio ryšio specialistams rengiant Lietuvos ir ES informacijos saugumo strategiją, vykdant tyrimus, nagrinėjant informacijos teisę, įgyvendinant informacinės visuomenės plėtros strategiją ir ES patvirtintus veiklos planus. Darbe pateiktos gaires ir rekomendacijos gali būti naudojamos kaip pagalbinė priemonė informacijos ir elektroninio ryšio tiekėjams bei vartotojams sprendžiant informacijos naudojimo, saugojimo, perdavimo ir kitus susijusius klausimus.

1. Informacijos saugumas šiuolaikinėje visuomenėje

Šiuolaikinė visuomenė suvokiama kaip modernių technologijų ir inovacijų visuomenė. Ji taip pat laikoma ir informacine visuomene[1], žinių, kompetencijos bei išminties visuomene[2]. Informacinės visuomenės plėtra jau tapo prioritetinė sritis Lietuvoje ir kitose Europos Sąjungos šalyse. Tai sąlygoja žmonijos poreikis turėti kokybišką informaciją reikiamu laiku ir patogiausiu būdu.

1.1. Informacijos saugumo problema

Informacinės visuomenės amžiuje, kai stengiamasi patenkinti informacinį žmogaus poreikį ir sukurti palankią informacijos gavimo, perdavimo bei saugojimo aplinką, didžiausias dėmesys tenka informacinėms technologijoms, sparčiai plėtojamoms informacinėms sistemoms, kompiuterių tinklams. Tačiau atsiranda ir rizikos faktoriai, tokie kaip informacijos bei asmens duomenų panaudojimas, atskleidimas ir platinimas. Ši problema yra aktuali tiek valstybiniam tiek privačiam sektoriui teikiant paslaugas, vykdant finansines operacijas, saugant privačių asmenų ir valstybės teises bei paslaptis.

Už teisinės bazės kūrimą atsakingi valstybės valdymo organai. Tačiau neretai sutinkami neatitikimai tarp teisės aktų ir politinių sprendimų, todėl būtina kurti vieningą nacionalinę informacijos saugumo politiką, kuri apimtų asmens duomenų apsaugą, kompiuterinių nusikaltimų prevenciją, valstybinės informacijos apsaugą, intelektualios informacijos apsaugą ir kitus aspektus.

Kiekviena valstybė, siekdama užtikrinti aukštą teikiamų paslaugų kokybę, ugdo informacijos ir tinklų saugumo kultūrą. Lietuvoje tai numato 2005 metų lapkričio mėnesį Lietuvos Respublikos ryšių reguliavimo tarnybos, Lietuvos bankų asociacijos ir asociacijos "Infobalt" pasirašytas Pažangos informacijos ir tinklų saugumo srityje memorandumas, kurio pagrindu kuriama saugi Lietuvos informacinė visuomenė. Prie šio memorandumo skatinamos prisijunti ir kitos institucijos bei organizacijos.[3]

Lietuvos informacinės visuomenės plėtros strategijoje, kurią 2005 metų gegužės mėnesį patvirtino Lietuvos Respublikos vyriausybė, pateikiamas Lietuvos informacinės visuomenės plėtros rodiklių netolygumų, palyginti su ES, įvertinimas. Remiantis šiuo įvertinimu Lietuvoje vis dar neišspręstos

[1] Glosienė A. Biblioteka informacijos politiko kontekste// Informacijos mokslai Nr. 15.
[2] Gudauskas R. Informacijos visuomenės kūrimo strategija: Lietuva globalių permainų kontekste// Informacijos mokslai Nr.14.-
[3] Bus ugdoma informacijos saugumo kultūra // TZC. –2005.
http://www.tzc.vu.lt/index.php?cid=1383&new_id=2786&page_nr=5

informacijos ir informacinių technologijų saugumo problemos. Todėl vienas iš strategijos prioritetų yra informacinės technologijos, kurios „suteikia naujas galimybes ne tik apsaugoti, bet ir plačiai skleisti informaciją apie kultūrą, skatina modernias kultūros ir meno iniciatyvas“.[4]

Šiuo metu pagrindiniai darbai informacijos saugumo užtikrinimo srityje yra susiję su viešojo administravimo sektoriumi, siekiant įgyvendinti informacijos technologijų saugos valstybinę strategiją ir šios strategijos įgyvendinimą. Tačiau to nepakanka norint užtikrinti informacijos saugumą tuose sektoriuose, kuriuose taip pat egzistuoja ši problema, ypač asmens duomenų apsaugos srityje.

Sparčiai augant naujoms technologijoms didėja ir informacijos saugumo pažeidimų pavojus. Informacija internete laisvai cirkuliuoja ir yra pateikiama visiems informacinio proceso dalyviams, tačiau tokios informacijos saugumą gali pažeisti tiek asmenys, tiek aplinkos ir gamtos keliami pavojai tokie, kaip informacinės sistemos gedimas, žaibas ir kiti. Auga ir kompiuterinių nusikaltėlių skaičius. Tai kelia grėsmę ne tik pavieniams informacijos vartotojams, bet ir valstybinių bei privačių informacinių sistemų saugumui.

Prieš sprendžiant šiuolaikinėje visuomenėje iškilusias problemas, svarbu veikti šiuolaikiškai ir apgalvotai. Kiekvienos problemos sprendimas turėtų priklausyti nuo išsamių tyrimų atliktų toje srityje. Informacijos saugumo srityje dirbančios valstybinės ir privačios institucijos, siekdamos patobulinti savo veiklą ir pagerinti informacijos apsaugos kokybę, nuolat atlieka tyrimus ir nagrinėja iškilusias problemas bei jų atsiradimo šaltinius.

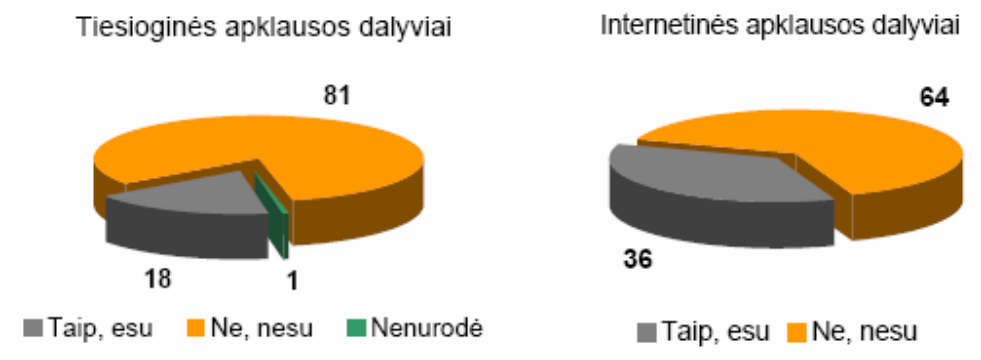
Lietuvos Respublikos ryšių reguliavimo tarnyba (RRT) 2005 metų pabaigoje atliko pirmąjį išsamų tinklų ir informacijos saugumo padėties Lietuvoje tyrimą, kuris parodė, kad tinklų ir informacijos saugumo incidentai – dažnas reiškinys, su kuriuo susiduria Lietuvos interneto paslaugų vartotojai. Net 78 procentai interneto vartotojų susiduria su kompiuterinių virusų daroma žala. Nepageidaujami elektroniniai laiškai (spam) kelia problemų 63 procentams interneto vartotojų, o 11 procentų vartotojų susiduria su neteisėto turinio informacija internete. Tinklų ir informacijos saugumo valdymo politiką savo įmonėse turi, ją prižiūri ir nuolat atnaujina 29 procentai tyrimo metu apklaustų Lietuvos įmonių ir 45 procentų interneto paslaugų teikėjų. Net penktadalis apklausos dalyvių – 22 procentai įmonių ir 23 procentai interneto paslaugų teikėjų teigia, kad jų įmonėje nėra saugumo valdymo politikos[5].

Šio tyrimo metu buvo siekiama išsiaiškinti, kiek ir su kokiais tinklų ir informacijos saugumo pažeidimais susiduria Lietuvos interneto vartotojai, kokiu mastu naudojamos įvairios apsaugos nuo šių

[4] Nutarimas dėl Lietuvos Informacinės visuomenės Pletros strategijos patvirtinimo //Lietuvos Respublikos Vyriausybė 2005 m http://www.ivpk.lt/teises_aktai/files/102.pdf

[5] Tinklų ir informacijos saugumo buklės Lietuvoje tyrimas. Vartotojų apklausa// RRT.- 2005.- http://www.rrt.lt/index.php?-348873977

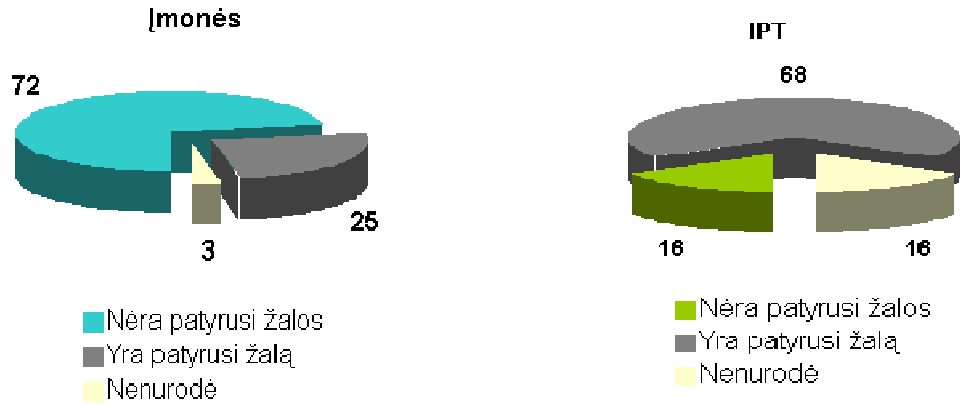
incidentų pažeidimų priemonės bei kokia žala dėl jų patiriama. Informacijos saugumo temos aktualumą puikiai atspindi RRT tyrimo tiesioginėje ir internetinėje apklausoje dalyvavusių vartotojų apklausa:



1. piešinys. Vartotojai, patyrę žalos dėl tinklų ir informacijos saugumo incidentų (procentais)[6]

1 piešinyje vartotojų, kurie patyrė žalą dėl tinklų ir informacijos saugumo incidentų, procentas yra mažesnis nei tų, kurie tokios žalos nepatyrė. Tačiau žalą patyrusių vartotojų skaičius yra pakankamai didelis ir galima teigti, kad informacijos saugumo trūkumą patiria net ketvirtadalis Lietuvos informacijos vartotojų.

RRT tyrimo metu buvo siekiama išsiaiškinti tinklų ir informacijos saugumo valdymo politikos naudojimo Lietuvos įmonėse ir Interneto paslaugų tiekėjų mastą, kiek ir su kokiais tinklų ir informacijos saugumo incidentais susiduriama, kaip dažnai naudojamos įvairios apsaugos nuo šių incidentų priemonės bei kokia žala dėl jų yra patiriama. Tyrimo rezultatai, pateikti 2 piešinyje, rodo kiek tokių įmonių patyrė žalą dėl tinklų ir informacijos saugumo incidentų:



[6] Tinklų ir informacijos saugumo buklės Lietuvoje tyrimas. Vartotojų apklausa// RRT.- 2005.- http://www.rrt.lt/index.php?-348873977

2. *piešinis.* Įmonės ir IPT, patyrusios žalos dėl tinklų ir informacijos saugumo incidentų (procentais)[7]

Remiantis 2 piešinio duomenimis, galima teigti, kad daugelis Interneto paslaugų tiekėjų ir ketvirtadalis Lietuvos įmonių yra patyrę žalos dėl tinklų ir informacijos saugumo incidentų. Tokių incidentų pasekmės gali būti įvairios, pavyzdžiui, įmonės veiklos sutrikimas, slaptos informacijos vagystė, sugadinta programinė įranga, patirta moralinė ir materialinė žala.

Remiantis kitais šio tyrimo duomenimis galima teigti, kad informacijos saugumo politiką savo įmonėse turi ir jos laikosi 29 procentai apklaustų Lietuvos įmonių ir 45 procentai interneto paslaugų teikėjų. Net penktadalis apklausos dalyvių – 22 procentai įmonių ir 23 procentai interneto paslaugų teikėjų - teigia, kad jų įmonėje nėra saugumo valdymo politikos.

RRT atliktas tyrimas parodė, kad tinklų ir informacijos saugumo valdymo politikos įgyvendinimas įmonėse vykdomas dar nepakankamai aktyviai. Tik 29 procentai įmonių ir 45 procentai interneto paslaugų tiekėjų nurodė, jog saugumo valdymo politika jų įmonėje yra įgyvendinama, ir pati įmonė vykdo nuolatinę jos priežiūrą bei atnaujinimą. Tačiau penktadalis apklausos dalyvių teigia, jog jų įmonėje nėra saugumo valdymo politikos[8]

UAB „Ekskomisarų biuras“, siekdamas atkreipti visuomenės dėmesį į informacijos saugumo svarbą verslo sėkmei, atliko tyrimą ir sugriovė keletą klaidingai susiformavusių nuomonių apie esamą situaciją Lietuvos įmonėse. Tyrimu buvo atskleista, kad daugumoje įmonių nėra tinkamos informacinių sistemų ir konfidencialios informacijos apsaugos sistemos, tačiau įmonės nepagrįstai mano, kad jų kompiuteriai yra saugūs (net 64 procentai apklaustųjų įmonių vadovų mano, kad jų sistemos yra saugios[9]).

Ekskomisarų biuro atlikto tyrimo rezultatai yra netikėti ir parodo šalies nepakankamą dėmesį informacijos saugumo politikai. Lietuvos įmonių kompiuteriai, kuriuose yra konfidenciali strateginė, marketingo, finansinė informacija, nėra pakankamai apsaugoti, nors vadovai klaidingai mano priešingai. Tyrimo autoriai taip pat teigia, kad daugumos įsilaužimų į sistemas įmonių atsakingi asmenys nepastebi ir įsilaužėliai nekliudomi naudojasi sistemų resursais, kopijuoja ir koreguoja vidinius įmonės dokumentus ir informaciją[10]. Tačiau tinklų ir informacijos saugumas yra gyvybiškai svarbus verslo sėkmei. Duomenis apie asmenis, finansinę įmonės padėtį, produktų gamybą ir kitą informaciją ypač svarbu patikimai saugoti.

[7] Tinklų ir informacijos saugumo buklės Lietuvoje tyrimas. Įmonių ir IPT apklausa// RRT.- 2005.- http://www.rrt.lt/index.php?174255322
[8] Ten pat
[9] Informacijos apsauga: Kodėl reikia saugotis? 2004 http://www.apsauga.lt/?m1=item20040801234651
[10] Ten pat

Ši problema yra viena iš aktualiausių informacinės visuomenės problemų, kuri, nepaisant didelių šioje srityje dirbančių organizacijų pastangų, nėra galutinai išspręsta.

1.2. Informacijos saugumo spragos

Atsiradus globaliam tinklui ir šiuolaikinėms informacijos technologijoms, informacijos saugojimo ir perdavimo procesai pagreitėjo ir tapo neišvengiama kasdienio gyvenimo dalimi. Dirbant kompiuteriu internete galima naudotis neišsenkančiu informacijos kiekiu, tačiau kompiuteris tampa pasiekiamas iš bet kurio kito kompiuterio, dirbančio internete. Todėl iškyla grėsmė tapti piktų kėslų turinčių asmenų aukomis. Jeigu nebus imtasi visų saugumo priemonių, galimi tokie pavojai, kaip duomenų arba jų privatumo praradimas, informacija iš kompiuterio gali būti sugadinta arba paviešinta internete, kompiuteris gali tapti apkrėstas virusu, kuris sugadina sistemines bylas.

Dažniausiai pasitaikančius tinklo ir informacijos saugumo pažeidimus tyrinėjo SANS Institutas (The Trusted Source for Computer Security Training, Certification and Research) ir Nacionalinis infrastruktūros apsaugos centras (National Infrastructure Protection Center - NIPC). Remdamasis šiais tyrimais SANS Institutas priėmė ekspertų susitarimą[11], kuriame apibrėžiamos pagrindinės interneto saugumo spragos ir galimybės bei priemonės nuo jų apsisaugoti.

SANS Instituto parengtame dokumente „SANS Top 20“ apibrėžta 20 spragų, kurias dažniausiai pasirenka kompiuteriniai įsilaužėliai bei interneto kirminai, tokie kaip Nimda, CodeRed, Blaster ir kiti.[12] Šį Top 20 spragų sąrašą sudaro du Top 10 sąrašai: 10 pavojingiausių Windows ir 10 pavojingiausių Unix pažeidžiamumų sąrašai. Šį sąrašą sudarė SANS institutas bendradarbiaudamas su FTB darbuotojais bei daugeliu kitų saugumo srities profesionalų iš viso pasaulio. Jis yra reguliariai atnaujinamas, pridedant naujas pavojingas interneto paslaugų spragas bei naujus būdus, kaip jas užtaisyti.

Nors informacinės visuomenės plėtros strategijoje informacijos saugumas yra viena iš prioritetinių sričių, tačiau šioje srityje dirbančių organizacijų atlikti tyrimai rodo, kad informacijos saugumui skiriama nepakankamai dėmesio ir tai vis dar rimta ir neišspręsta problema. Šios temos aktualumą patvirtina faktai, kad didelis procentas interneto vartotojų ir įmonių yra patyrę žalą dėl tinklų ir informacijos saugumo incidentų. Kita rimta problema yra ta, kad daugelis Lietuvos įmonių vadovų nepakankamai įsigilina į šios problemos egzistavimą ir teigia, jog jų informacija ir kompiuteriai yra saugūs. Tačiau esanti situacija nėra tokia optimistinė.

---

[11] The Twenty Most Critical Internet Security Vulnerabilities// SANS Institute.- 2005.- http://www.sans.org/top20/
[12] The Twenty Most Critical Internet Security Vulnerabilities// SANS Institute.- 2005.- http://www.sans.org/top20/

1.3. Priemonės informacijos saugumui užtikrinti

Naujos informacijos technologijos suteikia patogesnę ir greitesnę prieigą prie informacijos, tačiau suteikia daugiau galimybių ir norintiems panaudoti lengvai prieinamą informaciją savanaudiškiems tikslams, nusikalstamai veiklai ar kitaip disponuoti gauta informacija. Galimi asmens privatumo pažeidimai, neskelbtinos informacijos ar valstybės paslapčių paviešinimas. Todėl informacijos vartotojams būtina vadovautis rekomendacijomis, kurias pateikia valstybinės ir privačios institucijos bei organizacijos, dirbančios informacijos apsaugos srityje ir siekiančios apsaugoti savo klientus ir šalies piliečius nuo nepageidaujamų incidentų bei žalos patyrimo.

Kaip rodo tyrimų rezultatai, pavyzdžiui, Ryšių reguliavimo tarnybos atliktas Tinklų ir informacijos saugumo būklės Lietuvoje tyrimas, internetas nėra saugus, tačiau nepaisant to egzistuoja ir yra kuriamos įvairios priemonės, kurios leidžia pagerinti asmens duomenų ir kitos Internetu prieinamos informacijos apsaugą. Pavyzdžiui, Lietuvos Respublikos vidaus reikalų ministerijos (VRM) informacinės politikos departamentas rekomenduoja naudoti patikimas informacinių technologijų saugos priemones: [13]

- naudoti antivirusines programas,
- nuolat atnaujinti programinę įrangą,
- saugotis neaiškios kilmės elektroninių laiškų su prikabintais failais,
- naudoti ugniasienes (firewall),
- išsaugoti svarbių failų laikmenų atsargines kopijas,
- naudoti sudėtingus slaptažodžius,
- šifruoti svarbius pranešimus

VRM specialistai taip pat pataria reguliariai atlikti informacinių sistemų saugumo auditą, išanalizuoti įmonės kompiuterinę sistemą, nustatyti saugumo požiūriu netinkamai sutvarkytas darbo vietas, išanalizuoti naudojimosi sistemos resursais ar duomenimis teises, nustatyti, kokios saugumo spragos atviros potencialiam įsilaužėliui. Taip pat svarbu nedelsiant imtis priemonių nustatytiems trūkumams šalinti ar įdiegti papildomas informacines sistemas saugumui užtikrinti. Kitas žingsnis tinklų ir informacijos technologijų saugumo link – darbuotojų mokymai kursuose, kuriuose jie gali pagilinti savo žinias, būtinas saugiam darbui su organizacijos informacija bei kompiuterine technika.

[13] VRM Informacinės politikos departamentas, 2003 http://www2.vrm.lt/nuorodos/ipd/ipd-saugospatarimai.htm

Europos Tarybos ministrų komitetas parengė visoms valstybėms-narėms taikomas rekomendacijas dėl asmens duomenų, naudojamų moksliniams tyrimams ir statistikai, apsaugos, dėl viešųjų elektroninių ryšių paslaugų ir tinklų saugumo užtikrinimo, dėl asmens duomenų, naudojamų įdarbinimo tikslais, apsaugos, dėl asmens duomenų, renkamų ir tvarkomų statistiniais tikslais, apsaugos, dėl privatumo apsaugos internete ir kitas rekomendacijas, susijusia su informacijos saugumu.

Visos Ministrų komiteto priimtos rekomendacijos buvo rengiamos remiantis ES galiojančiais teisės aktais, kurie reglamentuoja informacijos politikos įgyvendinimą, tinklų ir informacijos technologijų saugumą, elektroninių paslaugų naudojimo ir teikimo galimybes, interneto tiekėjų ir vartotojų teises. Šiose rekomendacijose ypatingai saugomi asmens duomenys ir intelektinė nuosavybė, didelis dėmesys skiriamas ir valstybinės informacijos naudojimo bei prieigos klausimams.

Nors minėtos gairės ir pasiūlymai yra rekomendacinio pobūdžio, jų laikymasis gali užtikrinti nusikalstamumo, vykdomo elektroninėje terpėje nelegaliai naudojant informaciją ar duomenis, mažėjimą. Informacijos vartotojai pasijustų saugesni, atsirastų daugiau galimybių naujų elektroninių paslaugų teikimui, sėkmingai būtų įgyvendinami e-valstybės principai sudaryti saugią ir patogią prieigą prie reikalingos informacijos, naudotis viešojo administravimo paslaugomis patogiausiu būdu – elektroninėje terpėje, ir sudaryti palankias sąlygas kiekvienam piliečiui dalyvauti sprendimų priėmimo procese.

2. Lietuvos elektroninės erdvės saugumas

Informacijos saugumo poreikis vis auga ir to priežastis pastaruoju metu vis atsirandančios naujos modernios paslaugos, apimančios elektroninę prekybą, elektroninę bankininkystę, muitines, mokesčių surinkimo ir administravimo sistemas, valstybės informacines sistemas, elektroninį parašą ir kitas. Svarbiausias efektyvumo užtikrinimo rodiklis yra patikimos informacijos perdavimas saugiais informacijos perdavimo tinklais. Tačiau informacinės technologijos nuolat tobulėja, gerinama elektroninio ryšio prieiga, kinta informacijos vartotojų poreikis ir tuo naudojasi kompiuteriniai nusikaltėliai. Todėl tiek informacijos tiekėjas, tiek informacijos vartotojas turi veikti aiškioje teisinėje aplinkoje, esant reikiamoms teisinės apsaugos garantijoms. Informacijos apsaugos garantijos sudaro informacinės visuomenės teisinį pagrindą ir apima ne tik informacijos perdavimą, bet ir saugojimo bei turinio aspektus.

2.1. Informaciniai elektroninės erdvės aspektai

Informacinės visuomenės amžiuje, kai stengiamasi patenkinti informacinį žmogaus poreikį ir sukurti palankią informacijos gavimo, perdavimo bei saugojimo aplinką, didžiausias dėmesys tenka informacinėms technologijoms, sparčiai plėtojamoms informacinėms sistemoms, kompiuterių tinklams. Tačiau atsiranda ir rizikos faktoriai, tokie kaip informacijos bei asmens duomenų panaudojimas, atskleidimas ir platinimas. Ši problema yra aktuali tiek valstybiniam tiek privačiam sektoriui teikiant paslaugas, vykdant finansines operacijas, saugant privačių asmenų ir valstybės teises bei paslaptis.

Informacijos saugumo poreikis vis auga ir to priežastis pastaruoju metu atsirandančios e-pasaulio (elektroninio pasaulio) sąvokos – e-valdžia, e-vyriausybė, e-demokratija. Šios naujos sritys apima elektroninę prekybą, elektroninę bankininkystę, muitines, mokesčių surinkimo ir administravimo sistemas, valstybės informacines sistemas.

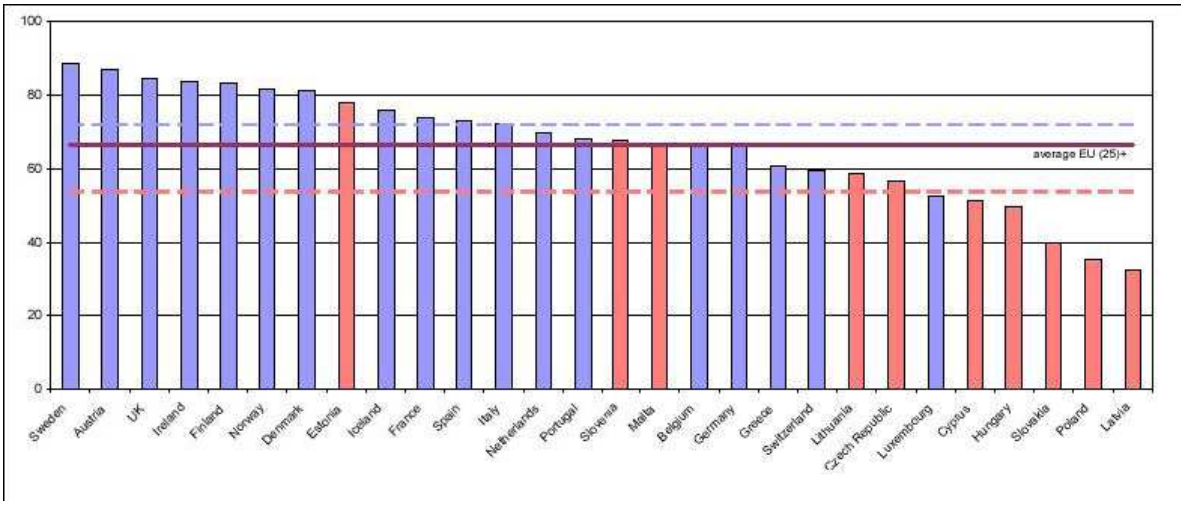
Šiuo metu pagrindiniai darbai informacijos saugumo užtikrinimo srityje yra susiję su viešojo administravimo sektoriumi, siekiant įgyvendinti informacijos technologijų saugos valstybinę strategiją ir šios strategijos įgyvendinimą. Tačiau to nepakanka norint užtikrinti informacijos saugumą tuose sektoriuose, kuriuose taip pat egzistuoja ši problema, ypač asmens duomenų apsaugos srityje.

2.2. Perėjimas prie e-valstybės

Valstybės institucijos ir verslo subjektai jau teikia trečio brandos lygio elektronines viešąsias paslaugas. Prie tokių priskiriami bilietų į renginius užsakymai ir apmokėjimai už juos, lėktuvų bilietų užsakymas ir apmokėjimas už juos, statistinių duomenų pateikimas Statistikos departamentui elektroniniu būdu. Galima pažymėti, jog pajamų deklaravimo paslauga jau yra teikiama IV lygiu. Taip pat, paminėtinos ir šios paslaugos, kurios jau yra teikiamos III-IV lygiu :

- Pajamų mokesčio deklaravimas;
- PVM deklaracija;
- Pelno mokesčio deklaravimas;
- Viešųjų bibliotekų paslaugos (leidinių paieška, užsakymas ir kt.);
- Darbo paieška;
- Su sveikatos apsauga susijusios paslaugos;
- Socialinės įmokos už darbuotojus;
- Muitinės deklaracijos;
- Statistinių duomenų pateikimas Statistikos departamentui;
- Viešieji pirkimai.

1. ***Grafikas.*** *Viešųjų paslaugų teikiama internetu (%[14]).*



[14] *DG for Information and Media , 2005.*

Vertinant Lietuvos situaciją Europos Sąjungos kontekste bei remiantis Europos Komisijos pateikiamais duomenimis, galima teigti, jog viešųjų paslaugų teikimo požiūriu Lietuva dar net nėra pasiekusi vidutinio lygio lyginant su kitomis Europos Sąjungos šalimis. Tokia situacija rodo, jog būtina imtis veiksmų skatinant viešųjų paslaugų plėtrą Internete. Tačiau pastaraisiais metais Lietuva per kelis metus padarė didelę pažangą e-paslaugų teikime.

2003-2004 m. vykdant investicinį projektą „Valdžios elektroninių vartų sukūrimas“ yra sukurtas valstybės ir savivaldos institucijų teikiamų e-paslaugų portalas (www.evaldzia.lt, www.epaslaugos.lt ir www.govonline.lt). Portalas pateikia informaciją gyventojams ir verslui apie viešojo administravimo institucijų (centrinės valdžios institucijų ir savivaldos) teikiamas paslaugas. Viešosios paslaugos suskirstytos pagal vartotojų grupes, gyvenimo įvykius, viešųjų paslaugų temas ir valstybinių institucijų sąrašą. Informaciją apie paslaugas sudaro internetinės nuorodos į paslaugas teikiančių institucijų tinklapių konkrečias vietas. Tačiau pats e-valdžios portalas nevykdo paslaugų transakcijų ir nepalaiko abipusio piliečių, norinčių gauti viešąsias paslaugas ir valstybinių institucijų, teikiančių viešąsias paslaugas, sąveikavimo internetu.

Saugus naudojimasis elektroninėmis paslaugomis

Kartu su elektroninės komercijos atsiradimu gimė ir visa eilė poreikių. Tai ir elektroninio parašo problema, ir telekomunikaciniais kanalais perduodamų duomenų apsaugos problemos. Iš nemažo elektroninės komercijos paslaugų rato galima išskirti elektroninę prekybą, kaip vieną iš sričių, reikalaujančių ypatingos priežiūros saugumo atžvilgiu.

Elektroninėje komercijoje, kuri yra daugiau nei vien tik prekių ir paslaugų pirkimas bei pardavimas internetu, duomenų apsaugos problemos yra aktualios visiems e-prekybos veikėjams, nes nuo to priklauso ir pelnas, įvaizdis ir klientų saugumas. Interneto prekyvietėse yra renkami ir automatiškai apdorojami klientų duomenys, kuriuos pirkėjai pateikia patys. Kaip rodo Lietuvos kompiuterininkų sąjungos šiais metais atlikti privatumo ir saugumo internete tyrimai, informacijos kiekis, kurį prašoma pateikti perkant produktą, dažniausiai yra perteklinis ir nebūtinas šiai paslaugai. Todėl svarbu yra nustatyti duomenų pateikimo kriterijus.

Duomenų rinkimo taisykles nustato Europos Sąjungos duomenų apsaugos direktyva 95/46/EC priimta 1995 spalio 24 dieną. Ji užtikrina laisvą informacijos judėjimą Europos Sąjungos bendrijos viduje, išsaugant pagrindines asmenų teises ir laisves. Garantuojamas elektroninių žinučių slaptumas ir draudžiamas bet koks trečiųjų asmenų įsikišimas ar stebėjimas. Pagal šios direktyvos nuostatas valstybės narės turi sudaryti sąlygas, kurioms esant asmeninių duomenų naudojimas yra teisėtas. Bet kokiu atveju

duomenys gali būti renkami tik teisėtais tikslais. Renkant tokius duomenis turi būti atkreiptas dėmesys į žemiau vardinamus kriterijus.

- **Privatumas.** Asmeniniai duomenys gali būti renkami, apdorojami ir panaudojami tik tokiu atveju, jeigu tai leidžia įstatymas arba asmuo davė savo sutikimą. Bet kurioje elektroninėje prekyvietėje pirkėjas, norėdamas nusipirkti prekę, privalės pateikti savo duomenis, reikalingus tam, kad prekės būtų pristatytos reikiamu adresu. Tačiau pirkdamas prekes duomenų subjektas jas pateikia savo noru, o elektroninė prekyvietė įsipareigoja nenaudoti duomenų kitais negu nustato įstatymas tikslais, taip užtikrinant duomenų subjekto teisę į privatumą.
- **Naudojimas.** Panaudoti duomenis galima tik tokiais tikslais, kuriais jie buvo renkami. Duomenis draudžiama perleisti tretiesiems asmenims, duomenų subjektui nesutikus. Tam, kad duomenys nebūtų atsitiktinai ar neteisėtai sugadinti arba prarasti, jie turi būti atitinkamai apsaugoti. Kitaip tariant, turi būti naudojamos atitinkamos saugumo priemonės. Duomenų naudojimo terminas taip pat yra apibrėžtas. “Asmens duomenys saugomi ne ilgiau, nei to reikalauja duomenų tvarkymo tikslai. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie turi būti sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti valstybiniams archyvams.”
- **Prieinamumas.** Žinome, kad duomenų aktualumas yra labai svarbus veiksnys. Todėl jie turi būti tikslūs ir nuolatos atnaujinami. Pagal LR asmens duomenų teisinės apsaugos įstatymo 17 str. p. 1, p.2 ir p.3 nustato asmens duomenų teisę į žinojimą apie jo duomenų tvarkymą, galimybę susipažinti su duomenimis, bei teisę reikalauti ištaisyti arba ištrinti duomenis. Kaip matome, šios įstatymo nuostatos duomenų subjektui sukuria teisę prieiti prie savo duomenų. Vartotojas taipogi turi turėti galimybę uždrausti jo duomenų kaupimą ir naudojimą, ypač tiesioginės rinkodaros tikslais.
- **Saugumas.** Svarbi problema, susijusi su kompiuteriniu informacijos apdorojimu, yra didelis tokios informacijos pažeidžiamumas bei didesnės galimybės pažeisti informacijos saugumą, pavogti, sunaikinti arba pakeisti duomenis.

Įvairiuose informacijos ar duomenų apsaugos žinynuose, bei vadovuose duomenų apsauga įvardinama įvairiai, tačiau juose visuose pabrėžiami trys pagrindiniai duomenų apsaugą reglamentuojantys lygiai:

1. Administracinis – techninis saugumas
2. Fizinis saugumas
3. Teisinis reglamentavimas

Administracinis - techninis saugumas. Šis lygis daug kur dar vadinamas administraciniu ir organizaciniu saugumu. Administracinis-techninis saugumas traktuojamas kaip techninių priemonių

organizavimas, siekiant užtikrinti kompiuterinėse laikmenose saugomą informaciją. Šiam lygiui galime priskirti tokias priemones, kaip saugumo politikos nuostatas, kurios aiškiai apibrėžia, kokia informacija yra saugoma, o kokia ne. Pagaliau yra nustatomi apsaugos lygiai, t.y. informacijai priskiriami taip vadinami “jautrumo” lygiai.

Šiam lygiui priklauso ir apsaugos organizavimas techninėmis priemonėmis. Tai ugniasienių įdiegimas bei jų taisyklių nustatymas. Antivirusinės programinės įrangos įdiegimas įmonės kompiuterinėse sistemose ir jos nustatymas. Įsilaužimo nustatymo sistemų įdiegimas kompiuterinėse sistemose. Duomenų šifravimo priemonės taip pat yra svarbi duomenų apsaugos priemonė.

Labiausiai pažeidžiama bet kokios kompiuterių sistemos vieta ir didžiausia grėsmė kompiuterių saugumui yra žmonės. Kai kurie žmonės gali būti tiesiog nemokšos ir net nenorėdami gali sunaikinti svarbią informaciją, esančią kompiuterių sistemose. Kiti žmonės gali piktavališkai pažeisti nustatytas taisykles. Nemažiau svarbus yra vartotojų teisių nustatymas kompiuterinėse sistemose. Didesnėse įmonėse ne kiekvienam darbuotojui leidžiama susipažinti su tam tikra informacija, o ir ne kiekvienam leidžiama tokią informaciją administruoti, ją koreguoti. Todėl čia svarbų vaidmenį vaidina vartotojų teisių sistema įmonės kompiuterinėje sistemoje. Tikslus vidinio įmonės kompiuterinio tinklo vartotojų teisių nustatymas labai daug prisideda prie kompiuterinėse sistemose saugomų duomenų apsaugos.

Fizinis saugumas. Jam priskiriami metodai, skirti apsaugoti aparatines ir kompiuterinės technikos ryšių priemones nuo nelaukiamo fizinio pašalinių jėgų poveikio. Tokioms jėgoms galime priskirti stichines nelaimes, techninius gedimus, dėl kurių galimas svarbių duomenų sugadinimas ar sunaikinimas. Tokiais gedimais gali būti trūkę vandentiekio vamzdžiai, elektros įtampos šuolis, kuris neatstatomai gali sugadinti kietajame kompiuterio diske saugomus duomenis, kondicionavimo sistemos gedimas tarnybinių stočių patalpoje, galintis sukelti kompiuterinių sistemų gedimą ir svarbių duomenų praradimą. Tokioms grėsmėms mažinti yra taikomos taip vadinamos aparatinės apsaugos priemonės nepertraukiamo maitinimo šaltiniai ir kitos priemonės.

Teisinis reglamentavimas. Šiam apsaugos lygiui priskiriamas norminių dokumentų paketo įmonėje įvedimas, kuris reglamentuotų tos įmonės darbuotojų elgesį su svarbiais duomenimis bei duomenimis sudarančiais įmonės komercinę paslaptį.

Dažnai šis vaidmuo įmonėse tenka taip vadinamiems saugumo nuostatams. Tačiau tenka pastebėti, kad dažnai šie reikalavimai sprendžiami taisyklių kūrimu ir jų patvirtinimu bendrovių vadovų įsakymais. Svarbu, kad jose būtų apibrėžta, kokia informacija patenka į saugomų duomenų ratą, o kokia ne. Tokių norminių aktų buvimas įmonėse vėliau leidžia juos pažeidusius darbuotojus traukti administracinėn, o padarius didelę žalą, ir baudžiamojon atsakomybėn.

Duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytiniame ar jam prilygintos formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan." Aukščiau minėtų tyrimų duomenys atspindi realią šių dienų situaciją Lietuvos elektroninėje prekyboje.

Lietuvos kompiuterininkų sąjungos atliktų tyrimų metu "iš viso ištirtos 44 svetainės, siūlančios prekes ar paslaugas internetu. Iš jų 8 buvo neveikiančios arba rekonstruojamos. Naudojant bankų korteles galima apsipirkti 8 svetainėse, iš kurių 5 naudoja saugius prisijungimo mechanizmus." Tokia situacija akivaizdžiai rodo, kad Lietuvos elektroninių prekyviečių savininkai nepakankamai užtikrina pirkėjų duomenų apsaugą. Net ir tokios nebrangios technologijos kaip SSL (angl. Secure Sockets Layers) nėra diegiamos, o tai rodo, kad esamų Lietuvos elektroninių prekyviečių savininkai mažai kreipia dėmesio saugumo problemoms spręsti.

Elektroninio pašto saugumas

Viena labiausiai paplitusių interneto paslaugų yra elektroninis paštas. Tai pigi, greita ir paprasta naudoti elektroninė paslauga, kuri pakeitė žmonių bendravimo įpročius ir tapo kasdieninio gyvenimo dalimi. Elektroninis paštas puikiai įsitvirtino šalia įprastinio pašto, telefoninio ir faksimilinio ryšio. Naudojimasis elektroninių paštu yra labai paprastas, tačiau elektroninio laiško siuntėjais ir gavėjas turi turėti kompiuterinę prieiga prie interneto, įdiegtą elektroninio pašto programą ir pašto dėžutę su adresu.

Atsiradus elektroniniam paštui ir pradėjus ji plačiai naudoti ne tik darbo, bet ir kitais tikslais, atsirado ir tam tikros grėsmės, pavojai, kurie gali neigiamai paveikti siunčiamą tekstą, pašto dėžutę arba kompiuterį. Elektroninis paštas yra viešai prieinamas ir galima paveikti įvairiais būdais tuomet, kai laiškas keliauja nuo siuntėjo iki gavėjo. Elektroniniame laiške esanti informacija gali būti perskaityta, iškraipyta ar kitaip paveikta trečiųjų šalių.

Charles ir Shari Pfleeger, nagrinėdami kompiuterinių tinklų ir informacijos saugumą, išskyrė pavojus, susijusius su elektroniniu paštu naudojimu: [15]

- Elektroninių pranešimų slaptumo praradimas jo priėmimo metu;
- Elektroninių pranešimų turinio pasikeitimas (modifikacija);
- Elektroninių pranešimų turinio klastojimas, įsikišant trečiosioms šalims;

[15] Charles P.Pfleeger, Shari Lawrence Pfleeger, Security in Computing, Third Edition, 2002

- Elektroninių pranešimų šaltinio iškraipymas;
- Elektroninių pranešimų nepatekimas į gavėjo pašto dėžutę;

Elektroninių paštu siunčiami duomenys nėra šimtu procentu apsaugoti ir rizikuojama, jog informacija gali būti perskaityta, iškraipyta arba kitaip panaudota įvairiuose tarpiniuose perdavimo etapuose: ryšio linijose, interneto paslaugų tiekėjo prieigose, elektroninio pašto tarnybinėse stotyse. Informacija gali būti prieinama trečiosioms šalims, siuntėjui ir gavėjui net nežinant, todėl reikia vadovautis saugumo ir konfidencialumo principais.

Konfidencialumo užtikrinimo galima pasiekti naudojant šifravimo techniką. Informacijos siuntėjas pagal tam tikras taisykles (susitarimą, naudojant programinę įrangą) persiunčiamus duomenis užšifruoja, o gavėjas – iššifruoja (vėl paverčia ja į suprantamą ir suvokiamą tekstą, vaizdą ar garsą). Tačiau čia taip pat svarbu yra tinkamai laikytis visų reikalavimų. Charles ir Shari Pfleeger suformulavo keletą svarbiausių elektroninių pranešimų saugumo reikalavimų, kurių laikymasis pranešimų siuntėjui ir gavėjui gali turėti lemiamą poveikį[16]:

- Pranešimų slaptumas (siunčiamas pranešimas neturi būti prieinamas trečiosioms šalims, su žinutės turiniu neturi susipažinti pašaliniai asmenys);
- Pranešimų integralumas (žinutė turi pasiekti nurodytą gavėją);
- Pranešimų autentiškumas, tikrumas (persiunčiant žinutė neturi būti tyčia ar netyčia pakeista);
- Pranešimų neišsižadėjimas (siuntėjas turi prisiimti atsakomybę už tą informaciją, kurią siunčia).

Ne visi šie reikalavimai yra privalomi kiekvienam pranešimui, tačiau jie sudaro tinkamą apsaugos kompleksą ir atitinka pagrindinius informacijos konfidencialumo, pasiekiamumo ir vientisumo apsaugos principus.

Elektroninis laiškas, keliaudamas nuo siuntėjo iki gavėjo, pereina per per daugelį tarpinių mazgų ir ryšio linijų, kurios gali priklausyti skirtingiems interneto paslaugų tiekėjams ir telekomunikacijų operatoriams. Laiškas gali kirsti kelių šalių sienas, kur galioja skirtingos elektroninį susirašinėjimą reglamentuojančios teisinės normos. Todėl galima teigti, kad norint pasinaudoti elektroniniu būdu perduodama informacija, tai įmanoma padaryti. Tačiau, jei informacija yra labai svarbi, ir nenorima, kad ji pakliūtų trečiosioms šalims, reikia imtis papildomų apsaugos priemonių.

[16] Charles P.Pfleeger, Shari Lawrence Pfleeger, Security in Computing, Third Edition, 2002

Elektroninio pašto apsaugai yra naudojamas ir elektroninis parašas, kuriuo naudojančios sistemos leidžia užšifruoti perduodamą informaciją ir apsaugoti ją nuo tyčinio ar atsitiktinio pakeitimo, įsitikinti žinutės siuntėjo tapatybės tikrumu. Elektroninio pašto žinutės siuntėjo tapatybę galima nustatyti pagal jo pašto adresą arba prierašą laiško apačioje, tačiau šis prierašas gali būti suklastotas ir išsiustas kito asmens vardu. Siuntėjo tapatybę taip pat gali padėti nustatyti elektroninio parašo sistemos, kurias prižiūri įstaigos informacinių sistemų specialistai. Tokių laiškų turinį taip pat galima apsaugoti tiesiog nesiunčiant labai svarbios ir neplatintinos informacijos tokios, kaip asmens duomenų, slaptažodžių ir kreditinių kortelių numerių.

Virusai yra vienas iš rimtesnių elektroninio pašto pavojų, kuris gali sugadinti kompiuterinę sistemą, ištrinti operatyviąją atmintį ar kitaip paveikti kompiuterį ir jame esančią informaciją. Kompiuteriniai virusai turi savybę plisti ir „užkrėsti“ įvairias kompiuterinės sistemos dalis. Jie plinta per elektronines laikmenas ir elektroniniais tinklais.

Vidaus reikalų ministerijos 2005 metų ataskaitoje pažymėta, kad virusus galima būtų suskirstyti į[17]:

- **Kirminus,** kurie gali daugintis patys, be kitų pagalbinių programų, todėl jie greitai plinta tinklais ir trikdo didelių kompiuterių sistemų veiklą. Dažniausiai kirminai plinta elektroniniu paštu ir yra aktyvuojami, atidarius prie žinutės prisegtą bylą, sulaukiama kenksmingų padarinių.
- **Trojos arklius**, kurie yra ypač pavojingi, nes gali įsibrovėliui suteikti slaptą prieigą prie kompiuteryje saugomos informacijos arba nurodyti kompiuteriui atlikti kenksmingą veiklą.
- **Makrovirusus,** kurie pažeidžia dokumentus, parengtus taikomosiomis programomis, turinčiomis priemones savaime vykdyti komandų sekas. Makrovirusas yra aktyvuojamas atidarius užkrėstą dokumentą. Dažniausi makrovirusų taikiniai yra *Microsoft Word* ir *Excel* dokumentai

Pagal padarytą žalą virusai gali būti suskirstyti į nepavojingus, pavojingus ir labai pavojingus. Aktyvuoti nepavojingi virusai nesutrikdo kompiuterio veiklos, o tik parodo ekrane kokį nors pranešimą arba sugroja melodiją. Pavojingi virusai gali sutrikdyti kompiuterio veiklą: programos gali pradėti veikti neįprastai ir daug lėčiau, kai kurie dokumentai gali tapti nebepasiekiami, kompiuteris gali pradėti dažnai pakartotinai pasileisti. Labai pavojingi virusai gali pakeisti arba ištrinti kompiuteryje saugomus duomenis, persiųsti duomenis pašaliniams asmenims arba sudaryti prieigą įsibrovėliams prie kompiuteryje saugomų duomenų.

Nuo kompiuterinių virusų galima apsisaugoti, pritaikant antivirusines programas, kurios apsaugo į kompiuterius patenkančią informaciją, blokuoja nepageidaujama informaciją ir pašalina ją iš kompiuterio.

[17] Informacijos apsauga valstybės institucijų ir įstaių darbuotojams, 2005

Nepageidaujami elektroniniai pranešimai, dar kitaip vadinami šiukšlėmis arba „spam“, pastaruoju metu kelia vis daugiau problemų juos gaunantiems abonentams. Tokių laiškų mastai yra įspūdingi ir daugelis elektroninio pašto abonentų gauna bent po kelis tokius laiškus per dieną. Interneto paslaugų tiekėjai teigia, kad apie 50 procentų per jų sistemas pereinančio duomenų srauto yra šiukšlės. Nepageidaujamos žinutės dažniausiai yra naudojamos komerciniais ir reklamos tikslais: bandoma įsiūlyti vaistų, programinės įrangos ir kitokių prekių arba paslaugų.

Lietuvos Respublikos ryšių reguliavimo tarnybos (RRT) 2005 metų pabaigoje atlikto išsamaus tinklų ir informacijos saugumo padėties Lietuvoje tyrimo duomenimis, net nepageidaujami elektroniniai laiškai kelia problemų 63 procentų interneto vartotojų[18]. Nepageidaujami elektroniniai laiškai užkemša pašto dėžutes ir lėtina kompiuterių darbą. Dalis tokių laiškų nešioja kompiuterinius virusus, kurie pažeidžia kompiuterinę sistemą arba sunaikina informaciją, esančią kietajame diske.

Norint apsisaugoti nuo nepageidaujamo pobūdžio žinučių, reikia stengtis be reikalo neskelbti savo elektroninio pašto adreso. Daugelis elektroninio pašto programų turi apsaugos nuo nepageidaujamų žinučių priemones: blokuojančius filtrus ir „juodųjų“ siuntėjų sąrašų sudarymo galimybes. Šios priemonės gali padėti sumažinti gaunamų nepageidaujamų žinučių kiekį.

Elektroninis parašas

Elektroninis parašas suprantamas kaip duomenys, kurie susiejami su kitais pasirašomais elektroniniais duomenimis ir atlieka pasirašiusio asmens autentifikavimo (arba identifikavimo) funkciją. Tačiau elektroninio parašo, atliekančio vien identifikavimo funkciją, juridinė galia kelia abejones. Aiškesnę, teisės aktais įtvirtintą galią turi saugus elektroninis parašas, atitinkantis keturis Europos Parlamento ir Tarybos Elektroninio parašo pagrindų direktyvos[19] ir Lietuvos Respublikos Elektroninio parašo įstatymo reikalavimus, pripažintus tarptautiniu mastu, tai:

- **unikalumas** (parašas vienareikšmiškai susietas su pasirašančiu asmeniu);
- **identifikavimas** (leidžia identifikuoti pasirašantį asmenį);
- **saugumas** (parašas sukurtas priemonėmis, kurias gali tvarkyti tik pasirašantis asmuo savo valia);
- **integralumas** (parašas susijęs su pasirašytais duomenimis taip, kad bet koks pasikeitimas yra pastebimas).

[18] Tinklų ir informacijos sauumo Lietuvoje tyrimas: Lietuvos įmonių ir interneto paslaugų tiekėjų apklausa.//RRT, 2005
[19] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013, 19/01/2000 p. 0012 – 0020.

Elektroniniu parašu duomenys pasirašomi, panaudojus elektroninio parašo formavimo duomenis, o patikrinami jais atitinkančiais elektroninio parašo tikrinimo duomenimis. Pažymėtina, kad Lietuvos Respublikos Elektroninio parašo įstatymas atstovauja moderniųjų šios srities įstatymų grupei, įtvirtindamas atvirumo arba technologinio neutralumo principą, reiškiantį, kad įstatymas gali būti naudojamas elektroninių duomenų pasirašymo reglamentavimui, nepriklausomai nuo naudojamos technologijos. Šios technologijos esmė yra privataus rakto, kurie žinomi tik pasirašančiajam, ir viešojo rakto, paskelbiamų viešai, atitikimas ta prasme, kad privačiu raktu sukurtas parašas gali būti patikrintas viešuoju raktu, tačiau iš vieno rakto žinomomis technologinėmis priemonėmis per įmanomą laiką neįmanoma gauti kito rakto. Elektroninį parašą reglamentuojančių įstatymų leidyboje naudojamas ir minimalistinis požiūris – tai yra abstraktus elektroninio parašo pripažinimas ir abstrakčių reikalavimų įtvirtinimas, visa kita paliekant egzistuojančioms technologijoms[20].

Identifikavimo kriterijus užtikrinamas pasitelkiant trečiąjį asmenį – sertifikavimo paslaugų teikėją, kuris per išduodamą sertifikatą (liudijimą) susieja pasirašančio asmens tapatybę su parašo formavimo ir tikrinimo duomenimis bei suteikia galimybę bet kam susipažinti su sertifikatu ir šiame įrašytų tikrinimo duomenų pagalba įsitikinti, jog pasirašęs asmuo yra tas pats, kuris save tokiu nurodo. Siekiant geriau ginti parašo naudotojų teises yra reglamentuojamas kvalifikuotas sertifikatas, kuriame nurodomai informacijai ir kurio išgavėjui (sertifikavimo paslaugų teikėjui) keliami papildomi reikalavimai, tačiau tai, kad parašas neparemtas kvalifikuotu sertifikatu dar automatiškai neatima iš šio parašo juridinės galios.

Juridiniams asmenims ir įmonėms, neturinčioms juridinio asmens teisių naudotis elektroniniu parašu tampa pakankamai sudėtinga dėl dviejų priežasčių – formos reikalavimų ir aiškaus įgaliojimų patvirtinimo trūkumo. Nemažai Lietuvos Respublikos teisės aktų reikalauja, kad juridinio asmens patvirtinimas susidėtų iš įgalioto asmens parašo ir antspaudo. Toks reikalavimas, pavyzdžiui, įtvirtintas Lietuvos Respublikos Civilinio kodekso[21] 70 str., nustatančiame, kad jurtinio asmens įgaliojimas būtų pasirašytas įmonės, įstaigos ar organizacijos vadovo (savininko), fizinio asmens, ir papildomai būtų uždėtas juridinio asmens atspaudas. Atspaudo reikalaujama teikiant dokumentus valstybės institucijoms, atspaudas yra įprastas rekvizitas sudarant sutartis, kai sutarties šalis yra juridinis asmuo. (Elektroninio parašo įstatymo 2 str. 7 d. ir 6 str.).

Ne tik verslo įmonės, bet ir valstybinės institucijos atveria kelius efektyvesniam pasinaudojimui naujomis technologijomis. Šie žingsniai akivaizdžiai parodo, kad elektroninis parašas mūsų gyvenime taps

[20] Internet Law & Policy Forum. Survey of International Electronic and Digital Signature Initiatives // http://www.ilpf.org/digsig/survey.htm.
[21] Lietuvos Respublikos civilinis kodeksas // Žin., 1964, Nr. 19-138.

kasdienybe, todėl jau dabar ypatingai svarbu suprasti kas tai yra, sugebėti tinkamai tai reglamentuoti ir mokėti pasinaudoti atsiveriančiomis galimybėmis.

Naudojant elektroninį parašą, svarbu yra tinkamai ji apsaugoti, kad juo negalima būtų suklastoti ir kad jis saugiai nukeliautų adresatui. Todėl elektroninis parašas turi atitikti dvi svarbiausias sąlygas: elektroninis parašas turi būti nepamirštamas ir autentiškas. Viena geriausių elektroninio parašo apsaugų yra šifravimo naudojimas. Šifravimo sistemos, turinčios atvirą raktą, puikiai tinka elektroniniams parašams.

Lietuvos Respublikos elektroninio parašo įstatymo 8 str., kaip ir Elektroninio parašo pagrindų direktyva, aiškiai nustato, kad saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu, elektroniniams duomenims turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme. Parašas nepraranda teisinės galios dėl to, kad yra elektroninis, nėra paremtas kvalifikuotu sertifikatu ar nėra paremtas kvalifikuotu sertifikatu, išduotu akredituoto sertifikavimo paslaugų teikėjo arba nėra sukurtas saugia parašo formavimo įranga.

2.3. Teisinis elektroninės erdvės reguliavimas

Kiekvienos šalies informacijos saugumo politiką atspindi įstatyminė bazė ir jos įgyvendinimo rodikliai. Didelę įtaką šalies politikai turi ir kultūra bei tradicija, taip pat ir kitų šalių „gera“ patirtis. Tradiciškai įstatymai yra kuriami norint ir siekiant užtikrinti visuomenės gerovę. Tačiau naujos technologijos ir jų pagrindu atsirandančios naujos paslaugos bei verslai skatina keisti egzistuojančius norminius dokumentus, reglamentuojančius tokias sritis kaip elektroninė prekyba, bankininkystė, viešo administravimo paslaugos ir kt.

Atsiradus tokioms sritims, kaip e-vyriausybė, e-valdžia, e-paslaugos, pradėta galvoti apie asmens duomenų apsaugos, valstybinės informacijos saugumo, intelektualinės nuosavybės apsaugos sustiprinimą. Taip pat pradėta daugiau dėmesio skirti ir viešo priėjimo prie įvairaus turinio informacijos. Tai atspinti pastaruoju metų priimti nutarimai, įstatymų pataisos, strategijų atnaujinimai.

Lietuva, būdama Europos Sąjungos nare, privalo suderinti savo prioritetines sritis su ES prioritetais, kurie buvo numatyti 2000 metais priimtoje ir 2004 metais atnaujintoje Lisabonos strategijoje, veiksmų planuose ir kituose visų valstybių-narių patvirtintuose dokumentuose. Lisabonos strategijoje viena iš prioritetinių sričių yra informacinės visuomenės plėtra ir jos neatsiejama dalis – teisinis pagrindas, kuris reglamentuoja asmens duomenų apsaugą, asmeninį individualų gyvenimą, užtikrina ir garantuoja pagrindines žmogaus teises ir laisves.

Lietuvos teisės aktai, reglamentuojantys informacijos saugumą

Lietuvos informacinės informacijos visuomenės teisinis pagrindas yra formuojamas nagrinėjant asmens duomenis ir jų apsaugos užtikrinimą, valstybės informacijos, intelektualios nuosavybės apsaugos aspektais. Tai apima informaciją apie individą, valstybę ar tam tikrą veiklą ir pan., kurios yra sukuriamos, saugomos, tvarkomos ir perduodamos atitinkamais nurodytais būdais. Valstybė taip pat apriboja visuomenę nuo kišimosi į valstybės informaciją, t.y. valstybė nustato tam tikras sritis, kurioms yra suteikiamas valstybinės paslapties statusas. Berno konvencija papildė teisės normas, ginančias intelektinę nuosavybę, nustatė, kas yra laikoma intelektualia nuosavybe, kam ir kada yra suteikiamas autoriaus vardas ir to pasėkoje gaunamos teisės, laisvės bei pareigos[22].

Pagrindiniai Lietuvos Respublikos įstatymai, reglamentuojantys informacijos saugumą yra:

- Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, kuris reguliuoja santykius, atsirandančius tvarkant ir teikiant duomenis apie fizinius asmenis valstybės informacinėmis sistemomis;
- Lietuvos Respublikos visuomenės informavimo įstatymas, nustatantis viešos informacijos gavimo, rengimo, platinimo tvarką ir viešos informacijos rengėjų, platintojų, savininkų ir žurnalistų teises ir pareigas, atsakomybę (1996. liepos 2. Nr.I-1418//Valstybės Žinios. Nr.71-1706.);
- Lietuvos Respublikos valstybės paslapčių ir jų apsaugos įstatymas nustatantis valstybės ir tarnybines paslaptis, jų slaptumą, slaptumo laipsnį;
- Lietuvos Respublikos registrų įstatymas nustatantis valstybės registrų steigimo, tvarkymo, naudojimo, reorganizavimo ir likvidavimo tvarką, taip pat valstybės registrų tvarkymo įstaigų, joms vadovaujančių ir jų priežiūrą atliekančių institucijų, valstybės registrams duomenis teikiančių bei valstybės registrų duomenis naudojančių juridinių bei fizinių asmenų pareigas ir teises, šių teisių apsaugą; taip pat juridinių ir fizinių asmenų, kurių duomenys yra registro objektas, pareigas bei teises, jų apsaugą;
- Lietuvos Respublikos archyvų įstatymas, reglamentuojantis Lietuvos archyvų fondo sudėtį, organizavimą, saugojimą, naudojimą, valstybės ir visuomenės poreikiams tenkinti bei piliečių teisėms realizuoti;
- Lietuvos Respublikos bibliotekų įstatymas nustatantis Lietuvos Respublikos bibliotekų sistemą, ryšius tarp bibliotekų, bibliotekų finansavimą ir valstybinį reguliavimą, apibūdinantis

[22] Informacijos visuomenės teisinio pamato raida Lietuvoje ir pasaulyje. 2004. http://www.infovi.vu.lt/ivs/biblioteka/temos/teisinis.htm

Lietuvos bibliotekų fondą ir jo apsaugą. (1995. Birželio 6. Nr.I-920//Valstybės Žinios. Nr.51. P.10-16.);

- Lietuvos Respublikos muziejų įstatymas, apibūdinantis Lietuvos Respublikos muziejų fondą, nustatantis Lietuvos muziejų sistemą, jų steigimo bei likvidavimo tvarką, muziejinių vertybių apskaitą ir apsaugą, valdymą bei finansavimą.

Tai pat svarbūs yra ir Lietuvos Respublikos Vyriausybės nutarimai bei kiti norminiai dokumentai, reglamentuojantys teisinius informacijos aspektus. Tai - nutarimai „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“, „Dėl valstybės registrų steigimo, projektavimo, reguliavimo ir naudojimo“.

Pažymėtini yra Lietuvos Respublikos Ryšių ir informatikos ministerijos įsakymas dėl asmens duomenų valdytojų registravimo, Lietuvos Respublikos Valdymo reformų ir savivaldybių reikalų ministerijos įsakymai, Lietuvos Respublikos Valstybinės duomenų apsaugos inspekcijos įsakymai „Dėl asmens duomenų teikimo sutarties“ ir „Dėl duomenų teikimo sutarties“.[23] Išskirtinas yra Lietuvos žurnalistų ir leidėjų etikos kodeksas, kuriame yra numatomi pagrindiniai žurnalistų ir leidėjų elgesio etikos principai.

Naujų informacinių technologijų ir naujų paslaugų atsiradimas skatina peržiūrėti esamus įstatymus ir priimti šių įstatymų pataisas arba išleisti naujus įstatymus. Taip atsiradus elektroninei prekybai ir kitoms paslaugoms elektroninėje terpėje buvo priimti „Elektroninių ryšių“, „Elektroninio parašo“, „Visuomenės informavimo“, „Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio“ įstatymai. Šie įstatymai buvo papildyti Lietuvos Respublikos Vyriausybės nutarimais „Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarka“, „Dėl neigiamą poveikį nepilnamečių vystimuisi darančios informacijos“, bei Lietuvos Respublikos ūkio ministro įsakymu „Dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teikimo vidaus rinkoje reglamento patvirtinimo“.

Informacijos tiekėjai ir vartotojai turėtų atsižvelgti į Lietuvos Respublikoje galiojančius teisės aktus ir neskelbti žalingo turinio ir neigiamą poveikį nepilnamečiams darančios informacijos, viešinti ar platinti įstatymais apibrėžtą neskelbtiną informaciją. Viešųjų elektroninių ryšių paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų paslaugų saugumui užtikrinti, o prireikus - kartu su viešųjų ryšių tinklų teikėjais imtis tokių pat priemonių viešųjų ryšių tinklų saugumui užtikrinti. Šios priemonės turi užtikrinti iškilusią grėsmę atitinkantį saugumo lygį.

[23] Informacijos visuomenės teisinio pamato raida Lietuvoje ir pasaulyje. 2004. http://www.infovi.vu.lt/ivs/biblioteka/temos/teisinis.htm

Lietuvoje veikiantys teisės aktai, reglamentuojantys asmens duomenų pasaugą, suteikia asmeniui teisę susipažinti su savo duomenimis. Tačiau įstatymas numato ir galimybę negauti tokios informacijos, jei tai gali pakenkti valstybės saugumui arba tokie duomenys gali pakenkti pačiam subjektui ir pan. LR teisės aktais bandoma apsaugoti ir valstybinę informaciją[24], kuri yra vienas svarbiausių ir slapčiausių kiekvienos šalies resursų. Informacijos rinkimas, kaupimas, apdorojimas, saugojimas, analizė, valstybės informacinės infrastruktūros kūrimas yra prioritetiniai kiekvienos valstybės informacijos politikos objektai. Nagrinėjant šį aspektą, svarbu pažymėti, kad Lietuvos teisės aktai reglamentuoja piliečių teises ir prieigą prie viešos ir įslaptintos valstybinės informacijos.

Informacinėje visuomenėje, kur didžiausią reikšmę turi informacijos sukūrimas, jos apdorojimas, saugojimas, perdavimas, svarbu užtikrinti individo, valstybės, organizacijos veikloje sukurtą informacijos produktą. Todėl įstatymais ginama intelektuali nuosavybė, apimanti teises, kurios yra susijusios su literatūros, meno ir mokslo kūriniais, kūrybine veikla, garso ir vaizdo įrašais, išradimais, prekių ir paslaugų ženklais. Pagrindinis teisės aktas, reglamentuojantis intelektinę nuosavybę yra Autorinių ir gretutinių teisių įstatymas ir Berno konvencija, prie kurios Lietuva prisijungė 1994 m.[25]

Lietuvos valstybinės institucijos, atsakingos už informacijos saugumą, norėdamos užtikrinti teisės aktų įgyvendinimą ir efektyvumą, bendradarbiauja tarpusavyje. Tai tokios institucijos, kaip Policijos departamentas prie VRM, Informacinės visuomenės plėtros komitetas, Lietuvos kriminalinės policijos biuras, Žurnalistų leidėjų etikos komisija, Lietuvos radijo ir televizijos komisija ir kitos organizacijos. Prie jų prisijungia ir privačios įmonės, pavyzdžiui, UAB „Ekskomisarų biuras“.

Privatumo ir asmens duomenų apsauga

Viena iš pagrindinių žmogaus teisių yra teisė į privatų gyvenimą, kuri yra reglamentuojama ne tik nacionalinėje konstitucijoje, bet tarptautiniais teisės aktais. Ši teisė apima privatų, šeimos ir namų gyvenimą, asmens fizinę ir psichinę neliečiamybę, garbę ir reputaciją, asmeninių faktų slaptumą, draudimą skelbti gautą ar surinktą konfidencialią informaciją ir kitus aspektus.[26] Informacijos slaptumas yra sudedamoji asmens privataus gyvenimo dalis taip garantuodamas galimybę laisvai keistis informacija, neatskleidžiant jos tretiesiems šalims.

Asmens duomenų apsaugos poreikis atsirado kartu su vis platesniu kompiuterinių technologijų naudojimu ir naujomis galimybėmis manipuliuoti duomenimis. Europos Sąjungos lygmeniu asmens

[24] Ten pat. Valstybinė informacija - politinės, ekonominės, karinės, mokslo ir technikos bei kitos žinios ir / ar duomenys, kurie yra svarbūs ar gali daryti (daro) įtaką valstybės veiklai ar valstybiniam gyvenimui, atitinkamos veiklos sričiai ir pan..
[25] Informacijos visuomenės teisinio pamato raida Lietuvoje ir pasaulyje.
http://www.infovi.vu.lt/ivs/biblioteka/temos/teisinis.htm
[26] Jarukaitis, I. Elektroninių ryšių teisė. – 2005. – p.333

duomenų apsaugą reglamentuoja 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių dokumentų judėjimo. Lietuvos Respublikoje asmens duomenis saugo Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, priimtas 1996 m. birželio 11 d.

Elektroninio ryšio paslaugas ir tinklus teikiantys ūkio subjektai kiekvieną dieną tvarko didelius informacijos kiekius, todėl šiame sektoriuje asmens duomenų teisinės apsaugos normos daro tiesioginę įtaką dideliu mastu. Asmens duomenų apsaugos reglamentavimą pritaikytą būtent elektroninio ryšio sektoriui nusako 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje. Lietuvos mastu šias nuostatas reglamentuoja Lietuvos Respublikos Elektroninių ryšių įstatymas.

LR Elektroninių ryšių įstatyme nustatyti tik patys bendriausi apsaugos principai, apimantys elektroninio ryšio tinklų ir paslaugų tiekėjus, naudojamą techninę programinę įrangą, operatyvinę sistemą, informacijos turinio perdavimą, elektroninių ryšių operatorius ir kitus principus. Tačiau daugiausiai klausimų šiame kontekste kyla dėl teisėsaugos institucijų veiklos ir jų veiksmų ribų tiek turinio, tiek srauto duomenis perimant/kontroliuojant teisės pažeidimų užkardymo ir tyrimo tikslais, tačiau išimčių, nustatytų aukščiau aptartoms privatumo ir asmens duomenų apsaugos normoms, yra ir daugiau. Pagal ribojimo tikslus galima išskirti tokius privatumo ir informacijos apsaugos ribojimo elektroninių ryšių tinkluose pagrindus:

1) Privatumo ir informacijos apsaugos ribojimas, susijęs su nusikalstamų veikų užkardimu ir tyrimu;
2) Privatumo ir informacijos apsaugos ribojimas, susijęs su pagalbos tarnybų veikla;
3) Privatumo ir informacijos apsaugos ribojimas, susijęs su kitais žalingais veiksniais.

Teisėsaugos institucijų veikloje, skirtoje nusikaltimų užkardimui ir jų tyrimui, elektroninių ryšių tinklais perduodama informacija gali būti itin vertinga. Viena vertus, būtinybė kai kuriais atvejais perimti tinklais perduodamą informaciją yra akivaizdi, kita vertus, būtina įtvirtinti tam tikras garantijas, kad tokia teise nebus piktnaudžiaujama.

Perėmimo apibrėžimas elektroninių ryšių kontekste gali būti apibrėžtas kaip trečiosios šalies veiksmas, kuriuo įgyjamos žinios apie tarp dviejų ar daugiau subjektų ryšių tinklais siunčiamą turinio arba su ja susijusią informaciją, įskaitant ir su elektroninių ryšių paslaugų naudojimu susijusius srauto duomenis[27].

[27] Jarukaitis, I. Elektroninių ryšių teisė., 2005., p.369

Be elektroniniais ryšių tinklais perduodamos turinio informacijos, teisėsaugos institucijos pastaraisiais metais vis labiau domisi ir srauto duomenimis. Atsiradus naujoms elektroninių ryšių paslaugoms, itin išsiplėtė šių duomenų apimtis, jie tampa vis informatyvesni ir naudingesni tiriant nusikaltimus. Išsiplėtė ir technologinės galimybės tokią informaciją rinkti, kaupti ir kitaip naudoti.

2004 m. balandžio 28 d. Airija, Jungtinė Karalystė, Prancūzija ir Švedija pateikė Pagrindų sprendimo dėl viešosioms paslaugoms teikti tvarkomų ir kaupiamų arba esančių viešųjų ryšių tinkluose duomenų išsaugojimo siekiant užkardyti, tirti ir nustatyti baudžiamąsias veikas, įskaitant terorizmą, bei patraukti baudžiamojon atsakomybėn, projektą[28]. Šiuo projektu siekiama suderinti Europos Sąjungos valstybių narių vidaus teisės normas dėl elektroninių ryšių tinkluose tvarkomų ir kaupiamų duomenų ir užtikrinti veiksmingą tarpvalstybinį bendradarbiavimą.

Šiai iniciatyvai buvo pritarta, tačiau kai kurios nuostatos sulaukė nemažai kritikos dėl kai kurių dalių. Viena iš jų nusako plataus išsaugojimų duomenų rato įtvirtinimą:

1. Pranešimo šaltiniui susekti ir nustatyti būtiną informaciją, apimančią asmens duomenis, susisiekimo informaciją bei informaciją, nurodančią užsakytas paslaugas;
2. Pranešimo nukreipimui ir paskirties vietai nustatyti būtinus duomenis;
3. Pranešimo išsiuntimo datai, laikui ir trukmei nustatyti būtinus duomenis;
4. Duomenis, būtinus telekomunikacijoms nustatyti;
5. Duomenis, būtinus ryšių priemonei arba tam, kas ją atstoja, nustatyti;
6. Duomenis, būtinus pranešimo buvimo vietai nustatyti inicijavimo/išsiuntimo pradžioje ir siuntimo metu.

Šiame projekte duomenys apimtų informaciją, sukuriama paslaugų, teikiamų šiomis nurodytomis ryšių infrastruktūromis, struktūromis ir protokolais:

1. Telefonijos, neįskaitant trumpųjų pranešimų, daugialypės terpės pranešimų, elektroninės žiniasklaidos;
2. Trumpųjų pranešimų, elektroninės žiniasklaidos, daugialypės terpės pranešimus;
3. Interneto protokolus, elektroninį paštą, balso perdavimą, plačiajuostį ryšį ir kt.

Svarbu nustatyti tinkamą pusiausvyrą tarp privačių asmenų ir ūkio subjektų interesų ir visuomeninių interesų, užtikrinant tinkamą pagrindą veiksmingai kovai su nusikaltimais ir elektroniniame sektoriuje veikiantiems subjektams.

[28] Jarukaitis, I. Elektroninių ryšių teisė., 2005., p.363

Autorinių teisių apsauga

Jungtinių Amerikos Valstijų teisės aktai autorines teises apibrėžia kaip „įvairiai išreikštų apčiuopiamų originalių kurinių autorystę, ... kurie gali būti suvokti, atkurti ar kitaip tiesiogiai panaudoti...[29]“. Lietuvoje kūrinys, kurio autorinės teisės gali būti saugomos apibrėžiamas Lietuvos Respublikos autorinių ir gretutinių teisių įstatyme (priimtas 1999 m. gegužės 18 d.) kaip „originalus kūrybinės veiklos rezultatas literatūros, mokslo ar meno srityje, nepaisant jo meninės vertės, išraiškos budo ar formos[30]“. Tačiau šie įstatymai negarantuoja idėjų raiškos apsaugos, tik kūrinio.

Tik kūrėjas turi autorines teises į savo kūrinį ir ir gali jomis disponuoti, kita vertus jeigu kūrinio autoriaus neįmanoma nustatyti, tuomet šis kūrinys negali būti saugomas autorinių teisių. Tam tikri kūriniai yra laikomi valstybinės reikšmės kūriniais ir autorinės teisės į tą kūrinį priklauso tik valstybei.

Autorinės teisės į kūrinį yra saugomos ribotą laiką. Lietuvos Respublikoje autorių turtinės teisės galioja visą autoriaus gyvenimą ir 70 metų po autoriaus mirties, neatsižvelgiant į kūrinio teisėto padarymo viešai prieinamu datą.

Kūriniai, kurių autorinės teisės yra saugomos įstatymų, turi būti realios (apčiuopiamos) vertės. Lietuvoje autorinių teisių objektais nelaikomi:

1) idėjos, procedūros, procesai, sistemos, veiklos metodai, koncepcijos, principai, atradimai ar atskiri duomenys;

2) teisės aktai, oficialūs administracinio, teisinio ar norminio pobūdžio dokumentai (sprendimai, nuosprendžiai, nuostatai, normos, teritorijų planavimo ir kiti oficialūs dokumentai), taip pat jų oficialūs vertimai;

3) oficialūs valstybės simboliai ir ženklai (vėliavos, herbai, himnai, piniginiai ženklai ir kiti valstybės simboliai bei ženklai), kurių apsaugą reglamentuoja kiti teisės aktai;

4) oficialiai įregistruoti teisės aktų projektai;

5) įprastinio pobūdžio informaciniai pranešimai apie įvykius;

6) folkloro kūriniai.

Teisės normos, reglamentuojančios autorines teises nurodo autorinių teisių objektą ir saugo jį nuo neteisėto naudojimosi: kopijavimo, plagijavimo, pardavimo ir kitų veiksmų.

Nors informacinės visuomenės plėtros strategijoje informacijos saugumas yra viena iš prioritetinių sričių, tačiau šioje srityje dirbančių organizacijų atlikti tyrimai rodo, kad informacijos saugumui skiriama

[29] Charles P.Pfleeger, Shari Lawrence Pfleeger. Security in Computing, Third Edition, 2002
[30] Lietuvos Respublikos autorinių ir gretutinių teisių įstatymas// LRS,. 1999 m. gegužės 18 d.

nepakankamai dėmesio ir tai vis dar rimta ir neišspręsta problema. Šios temos aktualumą patvirtina faktai, kad didelis procentas interneto vartotojų ir įmonių yra patyrę žalą dėl tinklų ir informacijos saugumo incidentų. Kita rimta problema yra ta, kad daugelis Lietuvos įmonių vadovų nepakankamai įsigilina į šios problemos egzistavimą ir teigia, jog jų informacija ir kompiuteriai yra saugūs. Tačiau esanti situacija nėra tokia optimistinė.

2.3. Socialiniai aspektai elektroninio ryšio saugumo politikoje

Kiekviena organizacija turėtų aiškiai apibrėžti atsakomybę už informacijos panaudojimą tam tikruose valdymo dokumentuose, nustatydama pagrindinius vartotojų vaidmenis ir atsakomybes už pažeidimus.

Socialinė atsakomybė elektroninio ryšio srityje nėra apibrėžta įstatymų, tačiau jos pagrindas yra etikos normos, kuriomis turėtų vadovautis kiekvienas elektroninės visuomenės vartotojas. Charles ir Shari Pfleeger išskyrė keletą aspektų, kuomet socialinės atsakomybės užtikrinimas gali padėti apsaugoti kompiuterius ir informaciją nuo nepageidaujamų pažeidimų ar kitų atvejų.

Socialiai atsakingi elektroninės erdvės vartotojai turėtų būti sąmoningi ir šiais principais[31]:

- Saugoti kompiuterius nuo kompiuterinių nusikaltėlių, kurie pažeidžia konfidencialumo, integralumo ir kompiuterinių sistemų tinkamumo principus, ir užkirsti jiems kelia;
- Laikytis autorinių teisių įstatymo;
- Gerbti programuotojų ir darbdavių intelektinės nuosavybės teises, nekopijuoti, neperparduoti pirktos programinės įrangos;
- Saugoti asmens duomenis, gerbti kiekvieno individo teisę į privatumą.

Socialinės atsakomybės stoka Lietuvoje ryškiai matoma, tai liudija daugybė internete vykdomų nusikaltimų, neteisėtas disponavimas autorinėmis teisėmis, duomenų vagystė ir kiti. Verslo sektoriuje, kaip ir valstybiniame, tokių nusikaltimų padariniai gali būti lemiami.

Nagrinėjant verslo poveikį aplinkai ir visuomenei, formuojasi naujas požiūris į tai, kokia turėtų būti XXI amžiaus verslo formulė. Vis aktualiau yra užtikrinti, jog šalia finansinių tikslų įmonės pradėtų daugiau rūpintis natūralia aplinka ir visuomene. Juk aplinka ir verslas yra tampriai susiję, o verslo ilgalaikė sėkmė priklauso nuo to, kaip įmonės sugeba darniai integruotis į aplinką ir jausti visuomenės socialines nuotaikas. Būtinumas užtikrinti ilgalaikę harmoningą ūkio bei visuomenės plėtrą yra

[31] Charles P.Pfleeger, Shari Lawrence Pfleeger, Security in Computing, Third Edition, 2002

Vyriausybės, pilietinės visuomenės ir verslo atstovų uždaviniai. Jiems spręsti, verslo sferoje vis dažniau kalbama apie verslo etiką , socialiai atsakingą verslą bei bendrą socialinę atsakomybę.

Socialiai atsakingi elektroninio ryšio tiekėjai siekdami būti geru pavyzdžių kitoms įmonėms ir teikdami paslaugas, turėtų:

- suteikti prieigą prie konkrečių tinklo elementų ir (ar) priemonių kitiems ūkio subjektams, įskaitant atsietą prieigą prie vietinės linijos;
- sąžiningai derėtis su ūkio subjektais, prašančiais suteikti prieigą;
- nenutraukti prieigos prie jau suteiktų priemonių;
- teikti nustatytas paslaugas turint tikslą jas perparduoti;
- suteikti atvirą prieigą prie techninių sąsajų, protokolų ar kitų technologijų, kurios yra būtinos paslaugų suderinamumui ar virtualaus tinklo paslaugoms teikti;
- suteikti prieigą prie patalpų ar kitus elektroninių ryšių infrastruktūros bendro naudojimo būdus;
- suteikti konkrečias paslaugas, būtinas užtikrinti paslaugų teikimą paslaugų gavėjams;
- suteikti prieigą prie veiklos palaikymo sistemų ar kitų panašių programinių sistemų, būtinų sąžiningai paslaugų teikimo konkurencijai užtikrinti;
- sujungti tinklus ar tinklų priemones, įskaitant galimybę sujungti tinklus bet kuriame techniškai galimame tinklo taške.

Dabartiniu metu Lietuvoje kaip ir visoje Europoje stiprėja socialinės atsakomybės ugdymo plėtra. Mūsų šalyje taip pat tvirtėja verslo orientacija į veiklą, kurios rezultatai yra nukreipti ne vien į pelno siekimą, bet ir į suinteresuotų veikėjų poreikius bei tokias dimensijas, kaip žmogaus teisės, aplinkos tausojimas, socialinis solidarumas ir sanglauda. Socialinės atsakomybės idėjos ir praktika pasiekia mūsų šalį įvairiais keliais, įtakoja globalizacijos procesus.

Naujos ūkio raidos tendencijos, informacinių technologijų panaudojimas bei pasaulio ekonomikos globalizacija pateikia naujus iššūkius ne tik įvairių šalių verslo visuomenei, vyriausybėms, bet ir visai žmonijai. Tai yra pilietinės visuomenės brandumo rodiklis.

Socialinės atsakomybės ugdymas turi nemažai privalumu, tai palankios verslui ilgalaikės perspektyvos (visos sąlygos verslo plėtrai), visuomenės poreikių ir lūkesčių pasikeitimas, moralinis įsipareigojimas vykdyti socialiai atsakingą veiklą, ir grįsti egzistuojančiomis moralės normomis. Kiti privalumai tai - žmogiškųjų išteklių ir intelektinio kapitalo stiprinimas, inovacijos, kūrybiškumas, intelektualusis kapitalas ir mokymasis yra stiprinami teigiamos KSA strategijos, gero įvaizdžio ir

saugumo užtikrinimas, taip pat ir populiarumas, sukurtas remiantis įmonės reputacija ar jos firminiu ženklu.

Etikos aspektai elektroninėje erdvėje

Bendraudami žmonės turi laikytis tam tikrų taisyklių, tai visiems savaime aišku, tačiau elektroninis bendravimas taip pat turi savo taisykles, kurių reikėtų paisyti. Etiketas yra nerašytos taisyklės, kuriomis priimta vadovautis mūsų visuomenėje, tačiau priimtomis teisės normomis taip pat reikia vadovautis.

Teisės normomis neįmanoma apibrėžti visų formų elgesio, kuris yra būdingas visuomenei. Kita vertus visuomenė vadovaujasi jai priimtinomis etikos ir moralės normomis, kurios nusako tinkama elgesį, nenumatydamos sankcijų. Primityviai kalbant, etika nustato standartus tarp to, kas gera ir bloga daugiausiai idėjiniu požiūriu, vadovaudamasi tam tikrais idealistiniais principais. Nežiūrinti į tai, kad religinės grupės ir organizacijos propaguoja tam tikrus elgesio standartus, kiekvienas individas vis tiek turi savo gero elgesio supratimą ir juo vadovaujasi.

Etika skiriasi nuo teisės keliais svarbiais aspektais. Pirmiausia teisė yra taikoma visiems (jeigu asmuo nesutinka su teisės normomis, jos vis tiek jam galioja). Intravertus, kilus konfliktui, teismai priima teisingą sprendimą, vadovaudamiesi teisės aktais. Ir galiausiai teisės aktuose identifikuojami veiksmai yra arba teisėti arba neteisėti, o etikoje - dori veiksmai ir nedori, prieštaraujantys moralės principams.

Skirtingos etikos taisyklės galioja skirtingose šalyse ir kultūrose, todėl dorą elgesį neįmanoma apibrėžti kaip vienintelį įmanoma ir geriausią. Naudodamasis elektroninėmis paslaugomis vartotojas turėtų vadovautis bendrais principais, kurie būdingi elektroninei erdvei. Todėl, prieš išsiunčiant ar persiunčiant elektroninio pašto žinutę, reikėtų įvertinti, ar gavėjo neįžeis elektroninio laiško turinys ir forma.

Nederamo turinio informacija – tai įžeidžiančios frazės, keiksmažodžiai, žeminančio turinio laiškai, skatinantys diskriminaciją, smurtą ar prievartą. Taip pat reikėtų atminti, kad besaikis informacijos siuntinėjimas to nepageidaujantiems gavėjams gali nereikalingai apkrauti kompiuterių tinklus ir trukdyti kitiems vartotojams normaliai bendrauti ir dirbti. Už kai kurios nederamos informacijos platinimą yra numatyta teisinė atsakomybė.

Kartais elektroninės žinutės gavėjas gali pasakyti, kad ekrane mato ne lietuvišką tekstą, o nesuprantamų simbolių kratinį. Taip nutinka dėl skirtingų teksto kodų lentelių nustatymų gavėjo ir siuntėjo kompiuterių sistemose. Todėl iškyla pavojus, kad perduota informacija bus nesuprasta, taps bevertė. Ganėtinai dažnai kompiuterių vartotojai mano, kad techniškai šių problemų negalima išspręsti, numoja į jas ranka ir pereina prie susirašinėjimo „šveplu“ raidynu, t.y., lietuviškas raides Ą, Č, Ę, Ė, Į, Š,

Ų, Ū ir Ž pakeičia raidėmis A, C, E, I, S, U ir Z. Tobulėjant programinei įrangai daugelis problemų dėl lietuviško raidyno kompiuteriuose yra išspręstos. Todėl elektroninio pašto žinutes derėtų rašyti lietuviškomis raidėmis, o „šveplas“ žinutes rašančiam kolegai pasiūlyti pasitarti su įstaigos kompiuterius prižiūrinčiais specialistais.

Tam, kad išsaugotume savo ir kitų interneto vartotojų privatumą, turėtume laikytis galiojančių teisės aktų, o taip pat ir kai kurių etinių aspektų. Pavyzdžiui:

- Atsakingas darbas (kiekvienas vartotojas turėtų prisiimti atsakomybę už siunčiamo pranešimo turinį);
- Išlaikyti kitų vartotojų (siuntėjo, gavėjo) konfidencialumą;
- Atsakingai naudotis kompiuterinėmis programomis, remtis instrukcijomis;
- Išlaikyti siunčiamos informacijos integralumą;

Etikos kodeksas yra vienas iš instrumentų, stimuliuojančių socialiai atsakingą verslą. Įmonėse ir organizacijose priimami etikos (elgesio) kodeksai, kuriuose įmonės įsipareigoja vykdyti, taip išreikšdami atskirus įsipareigojimus įvairiems socialiai atsakingo verslo kriterijams. Tam kad kodeksai nebūtų tik deklaratyvūs, įmonėse yra kuriamas visas jų palaikymo (įsipareigojimų realizavimo) mechanizmas – ‚Etikos infrastruktūra“. Skirtingose įmonėse jos elementų skaičius, pavadinimai bei funkcijos gali skirtis, o bendrai šią infrastruktūrą sudaro etikos kodeksai, etikos komitetai/komisijos, etikos konsultantai, ekspertai, advokatai, tarnautojai, teikiantys informaciją etikos klausimais, etikos informacijos tarnyba, „karštosios“ telefono linijos įmonių viduje , dalykinės etikos centrai, dalykinės etikos mokslinio tyrimo ir populiarinimo struktūros, jungiančios mokslininkų ir veiklos praktikų pastangas analizuoti bei diegti į dalykinę pozityvias vertybes, etikos mokymo programos, apvalieji stalai ir diskusijos, etinis socialinis auditas, koreliuojantis su etikos kodeksais vyriausybės nutarimas, teisės aktas; vyriausybės įgaliota tarnyba skundams tirti.

Visi šie Etikos infrastruktūros elementai yra vadybos instrumentai. Jie ypač nuosekliai taikomi žmogiškųjų išteklių valdyme ir diegiami tikslingai institucionalizuojant šiuolaikinę etiką į visas praktinės veiklos sferas.

Kiekviena organizacija turėtų aiškiai apibrėžti atsakomybę už informacijos panaudojimą tam tikruose valdymo dokumentuose, nustatydama pagrindinius vartotojų vaidmenis ir atsakomybes už pažeidimus. Taip pat visi informacinės sistemos vartotojai turėtų būti atskaitingi tam tikrai institucijai. Socialinė atsakomybė yra kompleksinis reiškinys ir vartotojas turėtų būti visapusiškai ugdomas šioje srityje pradedant nuo techninių kompiuterio naudojimo įgūdžių, baigiant teisinėmis ir etikos normomis.

3. Informacijos saugumas ES

Saugus informacijos perdavimas tarp Europos Sąjungos šalių ir tų šalių viduje priklauso nuo daugelio tokių principų, kaip kompiuterio, informacijos tinklų saugumas, vartotojo tinkamo elgesio internete ugdymas, elektroninio ryšio tiekėjų socialinė ir teisinė atsakomybė, teisinių aktų laikymasis ir kiti. Tačiau technologijos nuolat tobulėja ir Europos Sąjunga privalo tai įvertinti bei kurti šiuolaikines strategijas informacijos bei elektroninio ryšio apsaugai.

3.1. Informacijos saugumo prielaidos ES

Informacijos ir komunikacijos technologijų kūrimas ir naudojimas sudaro sąlygas techniniam progresui, modernizacijai ir struktūriniams ekonomikos pokyčiams. Atsižvelgiant į šiuos pokyčius ir siekiant 2000 m. kovo mėn. Lisabonos Europos Vadovų Taryboje Europos valstybių ir vyriausybių vadovų priimtos strategijos tikslų[32], kur vienas svarbiausiu aspektų yra konkurencingumas, Europos Sąjunga turėtų skatinti valstybes-nares naudotis visomis informacijos ir komunikacijos technologijų galimybėmis ir užtikrinti informacijos bei elektroninio ryšio saugumą.

Europos informacijos ir informacinių sistemų saugumo politikos tikslas yra apsaugoti informaciją nuo žalingo poveikio, užtikrinti saugią prieigą prie informacijos ir išsaugoti jos vertę išlaikant svarbios informacijos į duomenų konfidencialumą ir autentiškumą. Šie aspektai yra svarbūs visose srityse - darbo rinkoje, švietime, politikoje ir visose kitose srityse kur naudojamos informacinės technologijos.

Atsižvelgdama į Lisabonoje iškeltus tikslus (didesnis augimas, daugiau ir geresnių darbo vietų ir didesnė socialinė integracija), kurių įgyvendinimui neįkainomąją reikšmę turi informacinės technologijos, ir siekdama informacinės visuomenės plėtrai suteikti politinį stimulą, Europos Komisija pradėjo iniciatyvą e-Europa. Ši programa tinkamu laiku sprendė tinkamus klausimus ir skatino debatus dėl informacinės visuomenės politikos visoje Europoje bei už jos ribų. Lisabonos strategijos įgyvendinimo pusiaukelės metu (2004-2005 m.) atlikta apžvalga[33] patvirtino, kad pagrindiniai programos tikslai išliks aktualūs.

Siekdama Lisabonos strategijos tikslų įgyvendinimo bei informacijos saugumo užtikrinimo, Europos Komisija (EK) rengia direktyvas, potvarkius ir kitus dokumentus, į kuriuos, rengiant nacionalinę

[32] The Lisbon Strategy for growth and jobs http://ec.europa.eu/growthandjobs/index_en.htm 2000
[33] A new start of Lisbon Strategy: http://europa.eu/scadplus/leg/en/cha/c11325.htm, 2005

informacijos saugumo strategiją, turi atsižvelgti valstybės-narės. 2004 metais įvertinus Lisabonos strategijos įgyvendinimą, pasiekimus, Europos Komisija nusprendė numatyti politiką busimiems uždaviniams spręsti ir parengė komunikatą, kurio tikslas pradėti plačius politinius debatus dėl ES informacinės visuomenės strategijos po 2005 m. Jame nurodomos pagrindinės sritys, kuriose ES lygmens IRT politika gali atnešti pokyčių.[34]

Šie pokyčiai yra susiję ne tik su technologijomis, bet apima ir socialines bei ekonomines struktūras, naujų vyriausybės formų atsiradimą, naujus bendravimo ir bendradarbiavimo budus, verslo sektorių ir kitas sritis. Atsižvelgusi į šiuos aspektus, EK apibrėžė keletą svarbiausių problemų, kurias labiausiai įtakoja informacijos technologijų plėtra:

- Informacinių technologijų _ir paslaugų sektorius pats savaime yra svarbus sektorius. EK duomenimis jis išaugo nuo 4 procentų ES BVP iki maždaug 8 procentų ir sudarė apie 6 procentus ES užimtumo 2000 m[35]. Tai vienas novatoriškiausių sektorių, kuriam skiriama labia daug ES išlaidų mokslinių tyrimų ir taikomosios veiklos srityje.

- Informacinės technologijos yra svarbios našumui kelti ir konkurencingumui didinti, nes yra susijęs su augimu ir naujovėmis prekių ir paslaugų rinkose. Informacinės technologijos taip pat vis dažniau sudaro neatskiriamą visų pramonės ir paslaugų rinkų dalį.

- Naudojimasis informacinėmis technologijomis skatina pilietiškumą ir kelia gyvenimo kokybę.Jų taikymas dideliam žmonių skaičiui gali suteikti daugiau ir geresnių paslaugų. Naujos informacinės priemonės padeda stiprinti vyriausybės ir piliečių santykių skaidrumą ir atvirumą.

Kelios ES šalys išsiskiria gebėjimu diegti ir išnaudoti informacines technologijas, tačiau bendrus Europos gebėjimus išnaudoti visas šios srities teikiamas galimybes būtina gerokai sustiprinti. Tol, kol Europoje Lisabonos tikslai dar nėra pasiekti, itin svarbu, kad informacinių technologijų teikiamos galimybės būtų visiškai išnaudojamos.[36]

Norint pasiekti Lisabonos tikslų, specialią informacijos ir informacinių technologijų saugumo politiką reikės įgyvendinti dar daug metų. Platesnio jų panaudojimo skatinimas priklauso nuo gebėjimo spręsti daugelį klausimų, kuriuos kelia šių technologijų taikymas.

Plėtojant ir taikant IRT, padaryta daug pasiekimų. Dar daugiau bus pasiekta ateityje. Pavyzdžiui, 2004 m. liepą su maždaug 80 procentų gyventojų 15 ES valstybėse narėse buvo galima užmegzti ryšį plačiajuosčiu tinklu, tačiau vidutiniškai tik 7,7 procento jų buvo abonentai. Kartu su pastaruoju metu

---

[34] "Challenges for European Information Society beyond 2005" [**COM(2004) 757** final - Not yet published in the Official Journal]

[35] „OECD Information Technology Outlook“, 2004 m.

[36] „Komisijos ataskaita pavasario Europos Vadovų Tarybai. Lisabonos strategijos įgyvendinimas. Išsiplėtusios Sąjungos reformos“ KOM(2004) 29

pastebimu trečiosios kartos mobiliojo ryšio paslaugų augimu tai rodo, kad yra didelis būsimo augimo potencialas. Be to, gali būti diegiamos ir naujos alternatyvios technologijos[37]. Todėl dabartinę politiką, pavyzdžiui, reguliavimo arba spektro politiką, reikės pritaikyti prie naujų tendencijų.

Intensyvūs ir platūs moksliniai tyrimai ir taikomoji veikla yra itin svarbi bendram informacinių technologijų sektoriaus stiprumui ir šių technologijų panaudojimui visose ūkio šakose. Vyriausybės ir Europos Sąjunga skatina ir remia Europos bendrovių vykdomą mokslinių tyrimų veiklą, kurdamos palankią mokslinę, finansinę ir verslo aplinką. Europos lygmeniu svarbus vaidmuo teko Pamatinei programai. Tačiau mokslinių tyrimų ir taikomosios veiklos poreikis šiame sektoriuje nuolat auga, kartu su moksliniais tyrimais turėtų būti siekiama skatinti informacinių technologijų ir ryšių naujoves, kaip numatyta siūlomoje pažangos ir konkurencingumo programoje[38]. Taip pat vis didėja poreikis ištirti socialinį ir ekonominį technologijų naudojimo įvairiuose sektoriuose, tarp jų – sektoriuose, kuriuose veikia daug suinteresuotų asmenų, viešojo ir privataus sektorių bendradarbiavimo, geresnio nacionalinių ir regioninių iniciatyvų koordinavimo srityse, poveikį.

Elektroninių ryšio priemonių, reguliavimas išliks itin svarbus, kuriant aplinką, kuri būti palanki ir skatintų didesnes investicijas, naujoves, naujesnes paslaugas ir žemesnes kainas. Naujas ES elektroninių ryšio priemonių reguliavimo modelis veikia nuo 2003 m. Būtina užtikrinti, kad jis būtų visiškai ir efektyviai įgyvendintas ir išliktų tinkamu aplinkoje, kurioje technologijos sparčiai vystosi.

Svarbų poveikį informacinių technologijų plėtrai taip pat daro daugelis kitų reguliavimo klausimų. Tarp jų – autorinių teisių apsauga, taisyklės, taikomos mokėjimams mobiliuoju telefonu ir mikromokėjimams, privatumo apsauga, teisėsaugos institucijų poreikis. Reikalingos suderintos pastangos parengti ir įgyvendinti sprendimus, kuriais bus užkirstas kelias teisinėms problemoms, kurias turi spręsti atitinkamos verslo įmonės ir reguliavimo institucijos, tuo pat metu suteikiant galimybę visiškai išnaudoti informacinių technologijų teikiamus privalumus.

Atsižvelgiant į šiandien didėjančią priklausomybę nuo atvirų tinklų ir informacinių technologijų sistemų, šių sistemų trūkumai ir pažeidžiamumas kelia rimtų grėsmių. Tam, kad būtų išspręstos saugumo problemos ir užkirstas kelias elektroniniams nusikaltimams, būtinas glaudus visų rinkos sektorių bendradarbiavimas. Interneto saugumas išliks svarbiu darbotvarkės klausimu, kuriam spręsti reikės imtis priemonių interneto stabilumui ir patikimumui užtikrinti, pavyzdžiui, pasirengti šalinti riziką, užtikrinti atitiktį bei parengti jo naudojimo ir valdymo metodus.

Efektyviai naudoti informacines technologijas laikui bėgant tampa vis sudėtingiau. Sparčiai kintantys standartai ir priemonės bei jų suderinamumas reikalauja nuolatinio specialistų dėmesio. Todėl,

[37] „Price Waterhouse Coopers“, 2004 m. rugpjūtis
[38] „Finansinė 2007–2013 m. perspektyva“ KOM(2004) 487

siekiant efektyviai pasinaudoti informacinių technologijų pažanga, smulkioms įmonėms turėtų būti suteikta galimybė naudotis jų specifiniams poreikiams pritaikytomis kompetentingos, prieinamos ir tikslinės paramos paslaugomis, reikalingomis vidaus ir klientams skirtiems sprendimams.

Didelis skaičius vartotojų dabar turi galimybę naudotis infrastruktūra ir paslaugomis, kurios leidžia skleisti daugelio tipų skaitmeninį turinį. Tai reiškia, kad rinkos turi puikių galimybių plėtoti patrauklų turinį ir paslaugas, kurios bus naudingos ir vartotojams, ir ūkiui. Tačiau pažanga šioje srityje yra lėta. Garso ir vaizdo bei daugialypės terpės turinys – tai raktas į visų naujų technologijų, ypač, plačiajuosčių technologijų, sėkmę. Todėl svarbu, kad Europos Sąjunga prisiimtų labai aktyvų vaidmenį, remdama turinio teikėjus ir skatindama pažangių paslaugų kūrimą.

Kurti naujas paslaugas ir turinį kliudo įvairūs trukdžiai. Kai kurie jų yra reguliavimo kliūtys, pavyzdžiui, neužtikrintumas, susijęs su finansinių paslaugų taisyklių taikymu mokėjimams mobiliuoju telefonu, arba sistemų, kurios sudarytų galimybę teisėtai naudotis turiniu, atitinkančiu esamas intelektinės nuosavybės teises, plėtra ir priimtinumas. Kai kurie jų yra susiję su vieta rinkoje, pavyzdžiui, sunkumai kuriant sistemas arba suderinamumo problemos, patogumo vartotojams trūkumas ir situacijos, kai naujos paslaugos konkuruoja su jau esamomis. Kiti gi susiję su dominavimo rinkoje situacijomis. Naujų paslaugų ir turinio rinkos augimas priklausys nuo gebėjimo surasti reikalingus atsakymus į šį ilgą klausimų, kurie rūpi ir viešąjam ir privačiam sektoriams, sąrašą.

Informacinės ir ryšio technologijos šioje srityje yra naudojamos, siekiant pagerinti teikiamų paslaugų kokybę, sustiprinti demokratiją ir skaidrumą. Šioje srityje yra iškilę keli politiniai uždaviniai. Tai investicijų I informacinių technologijų plėtrą nepakankamumas ir uždaviniai, susiję su daugelio paslaugų suderinamumo trūkumu, administracinėmis teisėmis ir praktikos skirtingumu skirtingose šalyse, identiteto valdymo klausimais ir kartais nepakankamu turimų tinklų patikimumo ir saugumo lygiu. Be to, tobulinimas šioje srityje yra ypač svarbus, kadangi joms tenka neproporcingai didelė administracinė našta. Verslo įmonėms, ypač smulkioms, turi būti suteikta galimybė kaip galima daugiau procedūrų atlikti internetu. Norint tai pasiekti, reikia sukurti galimybę pateikti dokumentus su patvirtintais elektroniniais parašais. Galiausiai, prioritetu išlieka viešųjų paslaugų teikimo tarp sienų aspektas. Svarbiausių visoje Europoje teikiamų paslaugų, kurių būtų galima ypač siekti, pavyzdžiu galėtų būti įmonės registracija ir piliečių judėjimas „vieno sustojimo“ principu.

Didėjant galimybėms naudotis informacinėmis technologijomis ir jų pritaikymo būdais, auga poreikis užtikrinti jų suderinamumą: pavyzdžiui, fiksuoto ryšio ir bevielių tinklų, telekomunikacinių ir garso ir vaizdo paslaugų. Paprastai suderinamumą ir standartus kuria ir pasirenka rinkos operatoriai. Tikimasi, kad siekiant naujų prioritetų, bus tęsiamas Europos standartizavimo organizacijų, CEN, CENELEC ir ETSI darbas, įgyvendinant 2002 m. ir 2005 m. e-europa iniciatyvas. Be to, vyriausybės

privalo atidžiai sekti pažangą šioje srityje. Kai kuriomis aplinkybėmis joms gali tekti paremti suinteresuotus asmenis, šiems ieškant bendrų sprendimų. Kai kuriose srityse, kurios yra itin aktualios viešąjai politikai, gali tekti reikalauti naudoti atvirus standartus.

Internetas vis plačiau naudojamas kasdieniame piliečių gyvenime. Didesnio jo paplitimo prielaida – mūsų pasitikėjimo pateisinimas. Sektoriaus saugumas, privatumo apsauga, turto apsauga ir bendras valdymas yra neatskiriama piliečių pasitikėjimo informacine visuomene kūrimo dalis. Tai itin aktualu, kalbant apie vartotojų susirūpinimą dėl privatumo praradimo, neteisėtos arba nelegalios komercinės praktikos, nepageidaujamų pranešimų bei nelegalaus ir žalingo informacijos turinio bei mažumų apsaugos.

Daug pastangų skiriama tam, kad būtų sukurtas saugesnis vaikams internetas, rizikos valdymo sistemos ir incidentų kontrolės priemonės, priemones prieš elektroniniu paštu siunčiamą nepageidaujamą informaciją. Kiti aspektai yra susiję su sistemų ir tinklų patikimumu. Modernaus gyvenimo infrastruktūros, pavyzdžiui, bankų, finansų, sveikatos apsaugos, energijos, transportavimo ir pan., labai priklauso nuo IRT ir viena nuo kitos, o jų sutrikimai gali turėti ilgalaikių pasekmių.

Tuo pat metu privatumas ir duomenų apsauga tampa vis svarbesniu klausimu, kadangi didelės galimybės leidžia palyginti lengvai pasinaudoti išsamia informacija tiek apie privačius asmenis, tiek apie intelektinę nuosavybę.

Pripažįstama, kad efektyvus IRT naudojimas įmonėse yra vienas pagrindinių sėkmės veiksnių, didinančių Europos konkurencingumą. Tačiau naujus verslo procesus perimti ir įdiegti naujus verslo modelius, išnaudojant IRT teikiamas galimybes, vis dar yra sudėtinga, ypač milijonams Europos SVĮ. Mažesnės ir vangesnės investicijos Europoje į IRT yra aiškus makroekonominis rodiklis, rodantis, kad Europa neinvestuoja į našumą didinančias IRT tiek, kiek JAV. Be to, Europos veiklos rezultatams įtakos turi didelė SVĮ, kurios vis dar atsilieka nuo didesnių įmonių ne tik IRT panaudojimo, bet ir naudojamų IRT sudėtingumo srityje, dalis.

Informacinės ir ryšio technologijos turėtų būti plačiau naudojamos, kad būtų pasiekti visi Lisabonos strategijos kūrimo metu iškelti uždaviniai. Lietuva privalo pasinaudoti didžiuliu darbu, kuris jau atliktas ES informacinės visuomenės politikos srityje. Būtina aiškiai parodyti didžiulį teigiamą informacijos ir komunikacijos technologijų ir bendrai informacinės visuomenės poveikį, siekiant nugalėti naujų technologijų baimę ir išspręsti skaitmeninės atskirties didėjimo klausimą. Ekonominiu požiūriu pagrindinis klausimas yra ne tik kaip užtikrinti, kad informacinės technologijos būtų plačiau pritaikytos, bet ir kaip įgyti patirties tam, kad naudą būtų galima paskleisti plačiau.

3.2. ES informacijos saugumo teisinė bazė

Klestint informacinių technologijų sričiai, Europos Sąjungos šalyse pradėjo formuotis informacijos saugumo politika ir jos reglamentavimas. Jau 1981 metais buvo priimta Europos Tarybos Konvencija dėl asmenų apsaugos automatiškai apdorojant asmens duomenis. Remiantis šia konvencija, 1995 metais buvo priimta bendra nuostata panaikinti laisvo asmens duomenų judėjimo kliūtis ir konkurencijos daromus iškraipymus, sukuriant visoje Europos Sąjungoje vieningą lygiavertę, aukšto lygio apsaugos sistemą[39].

Europos Tarybos priimtuose teisės aktuose daug dėmesio skiriama intelektinės nuosavybės teisiniams aspektams, kurie yra aptariami greta teisinių aspektų, reglamentuojančių prekybą. Bendroji sutartis dėl tarifų ir prekybos (General Agreement on Trade and Tariffs, GATT)[40]. Joje yra nustatomi minimalūs reikalavimai autorių ir gretutinėms teisėms, prekių ženklams, geografinės kilmės nuorodoms, pramoniniam dizainui, patentams ir topografijoms. Intelektinės nuosavybės sąvoka šioje sutartyje apima ir pramoninės bei komercinės nuosavybės sąvokas ir užtikrina žmonių idėjų skatinimą, laiduoja visuomenės galimybę pasinaudoti asmenų kūrybos rezultatais.

Direktyva dėl privatumo ir elektroninių ryšių

Visoms ES valstybėms-narėms Europos Tarybos priimtos direktyvos yra atspirties taškas rengiant nacionalines strategijas ir įstatyminius projektus. Pažymėtina yra Duomenų apsaugos ir elektroninės komunikacijos sektoriaus (Data protection and electronic communication sector) direktyva, priimta 2002 metais ir reglamentuojanti naujų technologijų ir naujų paslaugų elektroninėje terpėje atsiradimą bei naudojimą, vartotojų teises ir pareigas, „spam“ (nepageidaujamų elektroninių laiškų) plitimą Internetu.

Ši Europos Parlamento ir Tarybos Direktyva reikalauja, kad:

- valstybės narės užtikrintų fizinių asmenų teises ir laisves, susijusias su asmens duomenų tvarkymu, ir ypač jų privatumo teisę, siekiant užtikrinti laisvą asmens duomenų srautą Bendrijoje[41].
- Būtų garantuojamas konfidencialumas pagal tarptautinius dokumentus, susijusius su žmogaus teisėms, visų pirma Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, taip pat valstybių narių konstitucijomis. Naujų elektroninių ryšių paslaugų diegimas yra būdingas informacinės visuomenės plėtrai. Plačiajai visuomenei tapo prieinami ir įperkami skaitmeniniai judrieji tinklai. Tokie

[39] Informacijos visuomenės teisinio pamato raida Lietuvoje ir pasaulyje. http://www.infovi.vu.lt/ivs/biblioteka/temos/teisinis.htm
[40] General Agreement on Trade and Tariffs, GATT. 2005
[41] Directive **2002/58/EC** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

skaitmeniniai tinklai turi didžiulius pajėgumus ir galimybes tvarkyti asmens duomenis. Nuo naudotojų pasitikėjimo, kad nėra jokios rizikos jų privatumui, iš dalies priklauso ir šių paslaugų sėkminga tarpvalstybinė plėtra.

- Viešai prieinamos paslaugos būtų apsaugotos. Viešai prieinamų elektroninių ryšių paslaugų teikėjas turi imtis tinkamų techninių ir organizacinių priemonių, kad užtikrintų savo paslaugų saugumą, o tam tikrais atvejais tokių priemonių imasi kartu su viešųjų ryšių tinklo teikėju, kad užtikrintų ir paties tinklo saugumą. Atsižvelgiant į naujausius technikos laimėjimus bei jų įdiegimo kainą, šios priemonės užtikrina saugumo lygį, atitinkantį atsiradusiai rizikai.

- Valstybės narės viešiesiems ryšių tinklams nustatytų specifines teisines, normines ir technines nuostatas, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės bei juridinių asmenų teisėti interesai, visų prima dėl didėjančių automatinio duomenų, susijusių su abonentais ir naudotojais, kaupimo ir tvarkymo pajėgumų.

Valstybės narės, atitinkami paslaugų teikėjai ir naudotojai kartu su kompetentingomis Bendrijos institucijomis turėtų bendradarbiauti diegdami ir plėtodami reikiamas technologijas, jeigu tai būtina taikant šioje direktyvoje numatytas garantijas užtikrinti, ypač atsižvelgdamos į tokius tikslus, kaip asmens duomenų tvarkymo minimizavimas ir, kur įmanoma, anoniminių ir pseudoniminių duomenų naudojimas.

Remiantis šia direktyva, paslaugų teikėjai, jeigu reikia, kartu su tinklo teikėju turėtų imtis tinkamų priemonių savo paslaugų saugumui užtikrinti, ir pranešti abonentams apie kiekvieną tinklo saugumo pažeidimo specifinę riziką. Tokia rizika pirmiausia gali kilti atviruoju tinklu, tokiu kaip internetas, teikiamoms elektroninių ryšių paslaugoms arba analoginei judriajai telefonijai. Itin svarbu, kad tokių paslaugų abonentams ir naudotojams paslaugos teikėjas išsamiai praneštų apie galimą saugumo riziką, kurios pašalinti jis nepajėgia.

Paslaugų teikėjai, siūlantys viešai prieinamų elektroninių ryšių paslaugas internetu, turėtų informuoti naudotojus ir abonentus apie tai, kokias priemones jie galėtų taikyti savo pranešimams apsaugoti, pavyzdžiui, specialią programinę įrangą ar šifravimo technologijas. Reikalavimas pranešti abonentams apie konkrečią riziką saugumui neatleidžia paslaugų teikėjo nuo įsipareigojimo savo lėšomis imtis tinkamų ir skubių priemonių pašalinti bet kokią naują, nenumatytą saugumo riziką ir atkurti normalų paslaugos saugumo lygį. Informacija abonentui apie saugumo riziką turėtų būti teikiama nemokamai, išskyrus nominalias išlaidas, kurias abonentas gali patirti gaudamas ir rinkdamas informaciją, pavyzdžiui, parsisiųsdindamas elektroninio pašto pranešimą.

Elektroninių ryšių sektoriuje ši direktyva taikoma visiems pagrindinių teisių ir laisvių apsaugos klausimams. Ši direktyva, nenagrinėja pagrindinių teisių ir laisvių apsaugos klausimų, susijusių su veiklos rūšimis, kurių nereglamentuoja Bendrijos teisės aktai. Todėl ji nekeičia esamos pusiausvyros tarp fizinio asmens teisės į privatumą ir valstybių narių galimybės imtis šios direktyvos nurodytų priemonių, kurių reikia užtikrinti visuomenės saugumą, gynybą, valstybės saugumą (įskaitant valstybės ekonominę gerovę, kai veiklos rūšys yra susijusios su valstybės saugumo klausimais) ir baudžiamosios teisės vykdymu. Tokiu būdu ši direktyva neturi jokio poveikio valstybių narių galimybėms teisėtu būdu perimti elektroninių ryšių pranešimus arba imtis kitų priemonių, kurių reikia minėtiems tikslams pasiekti laikantis Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos, kaip išaiškinta Europos žmogaus teisių teismo nutarime. Tokios priemonės turi būti tinkamos, griežtai atitinkančios siekiamą tikslą ir būtinos demokratinėje visuomenėje, taip pat joms turi būti taikoma tinkama apsaugos garantija pagal Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją.

Remiantis šia direktyva[42], valstybės narės užtikrina, kad elektroninių ryšių tinklų naudojimas informacijai saugoti ar prieiti prie informacijos, saugomos abonento ar naudotojo galiniame įrenginyje, būtų leidžiamas tik su sąlyga, kad atitinkamam abonentui ar naudotojui yra pateikiama aiški ir išsami informacija apie tokio duomenų tvarkymo tikslus, ir kad jam būtų suteikta teisė atsisakyti tokio duomenų valdytojo vykdomo tvarkymo. Tai nedraudžia techninio saugojimo ar priėjimo prie informacijos, kurio vienintelis tikslas yra vykdyti informacijos perdavimą elektroninių ryšių tinklu ar jį palengvinti, taip pat būtinais atvejais teikti informacinės visuomenės paslaugas, kurių aiškiai paprašo abonentas ar naudotojas.

Valstybės narės taip pat užtikrina skaidrias procedūras, reglamentuojančias būdus, kuriais viešųjų ryšių tinklų ir (ar) viešai prieinamų elektroninių ryšių paslaugų teikėjas galėtų nepaisyti šių draudimų:

a) laikinai panaikinti galimybę nustatyti liniją, iš kurios skambinama, gavus iš abonento paraišką, kurioje prašoma susekti piktybinius ar erzinančius skambučius. Tokiu atveju, laikantis nacionalinių įstatymų, duomenis, nustatančius skambinantį abonentą, saugos ir leis su jais susipažinti viešųjų ryšių tinklų ir (ar) viešai prieinamų elektroninių ryšių paslaugų teikėjas;

b) panaikinti galimybę nustatyti liniją, iš kurios skambinama, taip pat laikinai nepaisyti naudotojo ar abonento atsisakymo leisti tvarkyti vietos nustatymo duomenis, konkrečios linijos atveju organizacijoms, kurios aptarnauja pagalbos skambučius ir kurias valstybė narė pripažįsta atliekančias tokią funkciją, įskaitant teisėsaugos institucijas, greitosios pagalbos ir priešgaisrinės apsaugos institucijas, kad būtų galima atsakyti į tokius skambučius.

---

[42] Directive **2002/58/EC** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Ši direktyva suderina valstybių narių nuostatas, užtikrinančias vienodą pagrindinių teisių ir laisvių apsaugos lygį, ypač teisę į privatumą, susijusį su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, ir užtikrinančias laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų judėjimą Bendrijoje

Elektroninių ryšių tinklų ir paslaugų reglamentavimas

1997 metais Europos komisija parengė ir publikavo “Europos Elektroninės komercijos iniciatyvą”, kurioje buvo įtvirtinti tokie pagrindiniia uždaviniai, kurių įgyvendinimas užtikrintų tinkamą Europos Sąjungos teisės ir visos ekonominės aplinkos suderinamumą su nauju, modernių technologijų vystymusi:

- Užtikrintų platų ir visaapimantį prieėjimą prie infrastruktūros, produktų ir paslaugų, reikalingų eletroninei komercijai;
- Sukurti palankią reguliacinę aplinką;
- Kurti, skatinti elektroninei komercijai palankią terpę;
- Užtikrinti, kad teisinis reguliavimas šioje srityje atitiktų vartotojų poreikius.

2002 metais Europos Parlamentas ir Europos Taryba priėmė Direktyvą dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos. Ši direktyva yra taikoma elektroninių ryšių paslaugų srityje ir nustato elektroninių ryšių paslaugų, elektroninių ryšių tinklų, susijusių priemonių ir susijusių paslaugų reguliavimo suderintą sistemą. Ji nustato nacionalinių reguliavimo institucijų užduotis ir procedūras, kurios užtikrintų, kad reguliavimo sistema būtų suderintai taikoma visoje Bendrijoje.

Ši direktyva ir specifinės direktyvos nepažeidžia įpareigojimų, susijusių su paslaugomis, teikiamomis naudojant elektroninių ryšių tinklus ir paslaugas, kuriuos nustato nacionalinė teisė, suderinta su Bendrijos teise, arba Bendrijos teisė. Ji taip pat nepažeidžia priemonių, taikomų Bendrijos ar nacionaliniu lygiu laikantis Bendrijos teisės, kuriomis siekiama bendros svarbos tikslų, ypač susijusių su turinio reguliavimu ir audiovizualine politika.

Šios direktyvos priėmimą ir valstybių-narių šios direktyvos perkėlimą į nacionalinę teisinę bazę lėmė keletas aspektų:

- **Dabartinė telekomunikacijų reguliavimo sistema** sėkmingai sukūrė sąlygas veiksmingai konkurencijai telekomunikacijų sektoriuje pereinant nuo monopolio prie visiškos konkurencijos. 2000 m. kovo 23–24 d. Lisabonos Europos Vadovų Taryba pabrėžė, kokias galimybes augimui, konkurencingumui ir naujų darbo vietų kūrimui turi perėjimas prie skaitmeninės žiniomis pagrįstos ekonomikos. Ji ypač pabrėžė, kaip svarbu Europos įmonėms ir piliečiams turėti priėjimą prie nebrangios pasaulinės klasės ryšių infrastruktūros ir plataus asortimento paslaugų.
- **Audiovizualinė politika ir turinio reguliavimas** atliekamas siekiant bendriausių interesų, tokių kaip žodžio laisvė, žiniasklaidos pliuralizmas, nešališkumas, kultūrų ir kalbų įvairovė, socialinė įtrauktis, vartotojų apsauga ir nepilnamečių apsauga.

Šios direktyvos ir specifinės nuostatos nekliudo kiekvienai valstybei narei imtis būtinų priemonių savo esminių saugumo interesų ir valstybės politikos bei visuomenės saugumo apsaugai užtikrinti ir leisti tirti bei atskleisti kriminalinius nusikaltimus ir kelti dėl jų bylas, taip pat nekliudo nacionalinėms reguliavimo institucijoms nustatyti konkrečius proporcingus įpareigojimus, taikomus elektroninių ryšių paslaugų teikėjams.

Kad įmonės galėtų konkuruoti elektroninių ryšių sektoriuje, esminis dalykas – numeracijos sistemos prieiga remiantis skaidriais, objektyviais ir nediskriminaciniais kriterijais. Visus nacionalinių numeracijos planų elementus turėtų valdyti nacionalinės reguliavimo institucijos, įskaitant taškinius kodus, naudojamus tinklo adresams. Kai iškyla reikalas Bendrijoje suderinti numeracijos išteklius, kad būtų galima toliau plėtoti paslaugas visoje Europoje, Komisija gali taikyti technines įgyvendinimo priemones pasinaudodama savo vykdomosios valdžios galiomis. Jei tai gali padėti užtikrinti visišką paslaugų sąveiką pasaulyje, valstybės narės tarptautinėse organizacijose ir forumuose, kur priimami numeracijos sprendimai, turėtų laikydamosi sutarties derinti savo nacionalines pozicijas.

Siekiant garantuoti sąžiningos ir veiksmingos konkurencijos sąlygas, reikėtų užtikrinti, kad egzistuotų savalaikės, nediskriminacinės ir skaidrios teisių įrengti įrenginius suteikimo procedūros. Ši direktyva nepažeidžia nacionalinių nuostatų, reglamentuojančių turto ekspropriavimą ar naudojimą, įprastą naudojimąsi turto teisėmis, įprastą naudojimą to, kas priklauso viešajai sričiai, ar valstybėse narėse galiojančių turto nuosavybės taisyklių neutralumo principo.

Vartotojų lygiu turėtų būti skatinama skaitmeninės interaktyvios televizijos paslaugų sąveika ir patobulinta skaitmeninė televizijos įranga, kad būtų galima užtikrinti laisvą informacijos srautą, žiniasklaidos pliuralizmą ir kultūrų įvairovę. Pageidautina, kad nepriklausomai nuo perdavimo būdo

vartotojai turėtų galimybę priimti visas skaitmeninės interaktyvios televizijos paslaugas atsižvelgiant į technologijų neutralumą, būsimą technologijų pažangą, poreikį skatinti pereiti prie skaitmeninės televizijos ir konkurencijos būklę skaitmeninės televizijos paslaugų rinkose. Skaitmeninės interaktyvios televizijos platformos operatoriai turėtų stengtis įgyvendinti atvirą taikomųjų programų sąsają (API), kuri atitiktų Europos standartų organizacijos priimtus standartus ir specifikacijas.

Perėjimas nuo esamų API prie naujų turėtų būti skatinamas ir organizuojamas, pavyzdžiui, visiems suinteresuotiems rinkos dalyviams pasirašant supratimo memorandumus. Atviros taikomųjų programų sąsajos padeda sąveikai, t. y. interaktyvaus turinio perkeliamumui tarp perdavimo mechanizmų, ir šio turinio visiškam funkcionavimui patobulintoje skaitmeninėje televizijos įrangoje. Tačiau būtina atsižvelgti į poreikį netrukdyti priėmimo įrangos funkcionavimui ir apsaugoti ją nuo, pavyzdžiui, piktybiškų virusų.

Nacionalinės reguliavimo institucijos ir nacionalinės konkurencijos institucijos turėtų vienos kitoms teikti informaciją, būtiną šios direktyvos ir specifinių direktyvų nuostatoms taikyti, kad jos galėtų visapusiškai bendradarbiauti. Keičiantis informacija, gaunančioji institucija turėtų užtikrinti tokį pat konfidencialumo laipsnį, kokį užtikrina informaciją teikiančioji institucija.

Elektroninę terpę ir elgesį joje reglamentuoja ne tik minėtos direktyvos, bet ir Elektroninių paslaugų valdymo gairės (A new framework for electronic communications services, 1999 lapkritis), kurių pagrindu per pirmuosius įgyvendinimo metus buvo priimtos net šešios elektroninės informacijos saugumą reglamentuojančios direktyvos:

- Elektroninės komunikacijos apsaugos direktyva. (Directive on privacy and electronic communications), apimanti duomenų apsaugą ir elektroninės komunikacijos sektorių;
- Tinklų direktyva (Framework Directive), apimanti komunikacijos tinklų ir paslaugų gaires;
- Autorinių teisių direktyva (Authorization Directive);
- Visuotinių paslaugų direktyva (Universal Service Directive), apimanti viešai prieinamas paslaugas, vartotojų teises, elektroninę prekybą.
- Prieigos direktyva (Access Directive), kurioje reglamentuojama prieiga prie informacijos ir komunikacijos tinklų ir įrangos;
- Sprendimas dėl radijo bangų spektro (Radio Spectrum Decision), apimantis radijo bangų spektro politiką ES.

Lietuvoje priimtų informacijos saugumą reglamentuojančių teisės aktų priėmimo laikas leidžia teigti, kad dar prieš tapdama Europos Sąjungos nare, Lietuva pradėjo rūpintis informacijos saugumo politika. Nors tokia politika dar nėra vieninga visiems Lietuvos informacinės visuomenės dalyviams ir dar nepilnai susiformavo, tačiau lemtingi žingsniai jau žengti. Tai - informacijos politikos teisinio pagrindo formavimasis ir informacinės visuomenės plėtros strategijos kūrimas bei įgyvendinimas.

Tapusi Europos Sąjungos nare, Lietuva perkėlė pagrindines Europos Tarybos priimtas direktyvas, skirtas informacijos ir tinklų saugumo užtikrinimui, į nacionalinius teisės aktus, papildė bei pataisė esamus įstatymus. Ši bendra visoms ES valstybėms-narėms teisinė bazė saugo autorines ir gretutines teises, intelektinę nuosavybę, informacijos naudojimą, saugojimą bei perdavimą elektroninėje terpėje, interneto tiekėjų ir vartotojų teises, vaikų teises į žalos nenešančią informaciją ir kitas pagrindines teises informacijos visuomenėje.

3.3. ES iniciatyvos informacijos saugumo srityje

Siekdama visapusiško informacijos ir ryšių apsaugos politikos įgyvendinimo, Europos Komisija ne tik rengia teisės aktus ir rekomendacijos, bet ir koordinuoja programas, projektus, iniciatyvas bei skiria jiems finansavimą. Dažniausiai visos ES šalys palaiko šias iniciatyvas ir įgyvendina jas kaip tarptautiniame lygmenyje, taip ir nacionaliniame.

Prie Europos Sąjungos prisijungus naujoms šalims, tarptautinės organizacijos taip pat pasipildo naujais nariais ir jų veikimo sritis tampa dar platesnė. Valstybių bendradarbiavimas tarptautiniame lygmenyje turi neįkainojamąją reikšme, nes kiekviena valstybė “atsineša” savo patirtį, savo sukaiptas žinias ir panaudoja jas bendram darbui.

Tarptautinės organizacijos ir jų bendradarbiavimas

Tarptautiniams projektams įgyvendinti ir tarptautiniam bendradarbiavimui užtikrinti steigiamos tarptautinės organizacijos, kurių nariais tampa bendradarbiaujančių valstybių atstovai. Tokios organizacijos dažnai įgaliojamos rengti tos srities standartus arba rekomendacijas, įgyvendinti Europos Komisijos programas ir kitaip skatinti Europos Sąjungos piliečius prisidėti prie ekonomikos vystimosi.

Atsižvelgdama į esamą padėtį informacijos ir ryšių saugumo srityje, Europos Taryba, priėmė sprendimą įkurti Europos tinklų ir informacijos saugumo agentūrą[43], kuri stiprintų Bendrijos, valstybių

[43] Europos Parlamento ir Tarybos reglamentas (EB) Nr. 460/2004 2004 m. kovo 10 d.

narių ir verslo bendruomenės pajėgumą užkertant kelią tinklų ir informacijos saugumo problemoms, jas nustatant ir į jas reaguojant.

Agentūra buvo steigiama siekiant užtikrinti pagalbą Komisijai ir valstybėms narėms klausimais, susijusiais su tinklų ir informacijos saugumu.

Agentūros uždaviniai:

- rengti atitinkamą informaciją, skirtą esančiai ir kylančiai rizikai, o visų pirma – Europos lygmeniu, tokiai rizikai, kuri galėtų sukelti poveikį elektroninio ryšio tinklų lankstumui ir pasiekiamumui, bei jais gaunamos ir perduodamos informacijos autentiškumui, vientisumui ir konfidencialumui, analizuoti ir atliktos analizės rezultatus pateikia valstybėms narėms ir Komisijai;
- teikti Europos Parlamentui, Komisijai, Europos institucijoms ar valstybių narių paskirtoms kompetentingoms nacionalinėms institucijoms patarimus, bei pagalbą savo tikslų srityje, kai jos yra paprašoma;
- stiprinti įvairių tinklų ir informacijos saugumo srityje veikiančiųjų asmenų bendradarbiavimą, inter alia, rengiant reguliarias konsultacijas su pramone, universitetais ir kitais suinteresuotais sektoriais bei kurdama valstybių narių, privataus sektoriaus ir vartotojų institucijų paskirtų Bendrijos institucijų bei valstybinio sektoriaus institucijų kontaktinių asmenų tinklą;
- lengvinti Komisijos ir valstybių narių bendradarbiavimą toliau plėtojant bendrąsias metodologijas, skirtas užkirsti kelią tinklo ir informacijos saugumo problemoms, jas nustatyti ir į jas reaguoti;
- prisidėti prie sąmoningumo skatinimo ir, inter alia, skatindama keistis turimu geriausiu praktiniu patyrimu, įskaitant patyrimą apie vartotojų įspėjimo būdus, bei siekdama valstybinio ir privataus sektoriaus iniciatyvų sinergijos, prisideda prie galimybės visiems vartotojams gauti savalaikę, objektyvią ir išsamią informaciją tinklų ir informacijos saugumo klausimais;
- padėti Komisijos ir valstybių narių dialogo su pramone metu sprendžiant techninės kompiuterio įrangos ir programinės įrangos produktų saugumo problemas;
- sekti standartų, skirtų tinklo ir informacijos apsaugos produktams ir paslaugoms, raidą;
- patarti Komisijai mokslinių tyrimų tinklo ir informacijos saugumo srityje bei rizikos prevencijos technologijų veiksmingo naudojimo klausimais;
- skatinti rizikos įvertinimo veiklą, tarpusavyje veikiančius rizikos valdymo sprendimus bei tyrimus, susijusius su prevencija valdymo sprendimais valstybinio ir privataus sektoriaus organizacijose;

- prisidėti prie Bendrijos pastangų bendradarbiaujant su trečiosiomis šalimis ir tam tikrais atvejais su tarptautinėmis organizacijomis, skatinant bendrą visa apimantį požiūrį į tinklo ir informacijos saugumo problemas, tuo būdu prisidedant prie tinklų ir informacijos saugumo kultūros tobulinimo;
- nepriklausomai reikšti savo išvadas, orientaciją ir teikia patarimus klausimais, atitinkančiais jos veiklos sritį ir uždavinius.

Ryšių tinklai ir informacinės sistemos tapo esminiu ekonominės ir socialinės plėtros veiksniu. Kompiuterinės ir ryšių tinklų paslaugos šiuo metu tampa tokiomis plačiai naudojamomis komunalinėmis paslaugomis, kokiomis šiuo metu jau yra elektros energijos ar vandens tiekimas. Todėl ryšių tinklų ir informacinių sistemų saugumas, o ypač – jų pasiekiamumas kelia vis didėjantį visuomenės susirūpinimą dėl problemų atsiradimo pagrindinėse informacinėse sistemose galimybės, kurias sukelia sistemos sudėtingumas, avarijos, klaidos ir įsilaužimai, kas gali turėti pasekmių fizinėms infrastruktūroms, teikiančioms ES piliečių gerovei ypatingai svarbias paslaugas. Todėl tikimąsi, kad Europos tinklų ir informacijos saugumo agentūros įkūrimas padės sustabdyti vis didėjanti nusikaltimų skaičių šioje srityje ir pagerins informacijos saugumo politiką visose Europos Sąjungos šalyse.

Kitos tarptautinės organizacijos veikiančios Europos Sąjungos lygiu yra Ekonominio bendradarbiavimo ir plėtros organizacija (Organisation for Economic cooperation and development, OECD[44]), Tarptautinė telekomunikacijos sąjunga (ITU- International Telecommunication Union[45]), OECD Working Party on Information Security and Privacy (WPISP) ir Verslo ir pramonės patariamasis komitetas (BIAC,Business and Industry Advisory Committee[46]) .

Ekonominio bendradarbiavimo ir plėtros organizacija (EBPO). Ši organizacija įkurta 1961 m. JAV ir Kanadai prisijungus prie Europos ekonominio bendradarbiavimo organizacijos (angl. OEEC – Organisation for European Economic Co-operation), vienijusios Europos šalis bendram tikslui – atstatyti po II-ojo Pasaulinio karo sugriautą ekonomiką.

EBPO svarstomų klausimų spektras yra labai platus – nuo makroekonominių iki aplinkosauginių, švietimo, mokslo, technologijų, inovacinių. Kitos tarptautinės ekonominės organizacijos ir finansinės institucijos aukštai vertina EBPO ruošiamas tyrimais bei analizėmis pagrįstas studijas, kurios įvertina atskirų valstybių vykdomą politiką konkrečioje srityje. EBPO yra sukaupusi vieną išsamiausių statistikos bazių.

---

[44] Organisation for economic co-operation and development
http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html
[45] http://www.itu.int/aboutitu/ International telecommunication union
[46] The business and Industry Advisory Cometee to the OECD http://www.biac.org/

EBPO išskyrė devynis svarbiausius principus, kuriais remiasi kurdama savo veiklos strategiją informacijos apsaugos srityje[47]:

- problemos nustatymas ir suvokimas;
- atsakomybės skatinimas;
- reagavimas į incidentus;
- kultūros ir etikos gairių laikymasis;
- demokratija
- rizikos įvertinimas;
- apsaugos sistemų kūrimas ir diegimas;
- saugumo sistemų valdymas;
- vertinimas.

EBPO vis labiau savo veiklą nukreipia ne tik į valstybes – nares, bet taip pat siūlo savo sukauptą analitinę ekspertizę besivystančioms ar kitoms bendradarbiavimu su EBPO suinteresuotoms valstybėms. Šiuo metu EBPO palaiko ryšius su daugiau nei 70 valstybių, siekiančių glaudesnio bendradarbiavimo su EBPO ar narystės šioje organizacijoje. Viena iš tokių valstybių yra Lietuva.

Atsižvelgiant į tai, kad EBPO veiklos pobūdis ir įtaka yra akivaizdžiai peržengę pačios organizacijos ribas, o EBPO rekomendacijos bei nuostatos tampa daugiašalių susitarimų bei tarptautinį bendradarbiavimą reglamentuojančių dokumentų neatsiejama dalimi, narystė EBPO suteikia valstybėms narėms galimybę būti ne tik pasyvia rekomendacijų vykdytoja, bet ir modernios ekonominės bei socialinės politikos formuotojoms, o taip pat sparčiau realizuoti ekonominės politikos tikslus, užtikrinti sėkmingą funkcionavimą ES vieningoje rinkoje bei padidinti prekių ir paslaugų pardavimą į trečiųjų šalių rinkas.

Tarptautinė telekomunikacijos sąjunga (International Telecommunications Unijon, ITU). Organizacija pagrindinį dėmesį skiria telekomunikacijos technologijoms, jų plėtrai ir apsaugai. Ši organizacija veikia labai plačiai - rengia standartus valstybėms narėms, konsultuoja dėl telekomunikacijų politikos įgyvendinimo, rengia seminarus, leidžia standartizavimo dokumentus.

ITU tarptautiniu mastu paskirstomas radijo dažnių spektras ir geostacionariųjų palydovų pozicijos – riboti ištekliai, be kurių neįmanoma telekomunikacijų veikla, rengiami elektroninių ryšių ir informacinės visuomenės plėtros planai, todėl dalyvavimas ITU veikloje yra būtinas kiekvienai šaliai, aktyviai vystančiai telekomunikacijas, sparčiai einančiai į informacinę visuomenę.

[47] Organisation for economic co-operation and development
http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html

Verslo ir pramonės patariamasis komitetas priklauso Ekonominio bendradarbiavimo ir plėtros organizacijai, tačiau veikia atskirai ir veikia tik verslo sektoriuje. Šiai organizacijai priklauso apie 30 narių, kurie rūpinasi verslo bei pramonės plėtra ir siekia šios srities gerinimo. Tikslams pasiekti, organizacija įgyvendina daugybę tarptautinių projektų ir programų. Organizacija veikia nuo 1962 metų ir yra vertinama už savo pasiekimus.

Tyrimai ir programos informacijos saugumui pagerinti

Europos Taryba, matydama informacijos saugumo spragas, kurios kelia grėsmę ES informacinės visuomenės plėtrai ir joje veikiantiems asmenims, ypatingai vaikams, rengia įvairias programas, kurios turėtų pagerinti situaciją valstybėse narėse. Viena tokių programų yra „Saugesnis Internetas plius“ (Safer Internet Plus) 2005-2008 metams48. Šia programa siekiama sustabdyti neigiamo turinio informacijos plitimą globaliame tinkle.

“Saugesnio interneto plius” programos tikslas – skatinti saugaus interneto bei naujų elektroninės saugos technologijų vartojimą, kovoti prieš neteisėto ir nepageidaujamo interneto turinio sklaidą[49]. Ypatingas dėmesys skiriamas saugaus interneto turinio naudojimui vaikų tarpe. Programa apima kovą su nelegaliu turiniu, žalingo ir nepageidaujamo turinio šalinimą, saugios aplinkos skatinimą ir visuomenės švietimą.

Informacinės visuomenės technologijų tyrimus apimantis projektas **IST Results** service veikia Europos Sąjungos šalyse ir rūpinasi tyrimais ir jų rezultatų sklaida informacinės visuomenės plėtros srityje [50]. Tyrimuose dalyvauja valstybinės institucijos, informacinių technologijų ir ryšio vartotojai bei tiekėjai, žiniasklaidos atstovai ir kiti informacinėje visuomenėje veikiantys subjektai. Tyrimai apima elektronines paslaugas, interneto saugumą, informacijos, duomenų bei vartotojų apsaugą.

Informacijos visuomenės plėtra ir informacijos apsauga besirūpinanti Europos Taryba priėmė visus minėtus ir daugelį kitų teisės aktų ir projektų siekdama sukurti efektyvią informacijos saugumo politiką. 1995 m. buvo pasirašytas aktas dėl autorinių ir gretutinių teisių (Green Paper on Copyright and Related Rights in the Information Society), 2004 metais buvo įsteigta Europos tinklų ir informacijos saugumo agentūra (European Network and Information Security Agency ENISA), pradėtos įgyvendinti tokios programos, kaip eEurope, eEurope+ ir kitos.[51] Tikėtina, kad šios programos atskleis priimtų teisės aktų privalumus ir trūkumus, užtikrins jų įgyvendinimą.

[48] Draugiškas internetas http://www.draugiskasinternetas.lt/lt/youth/news?id=1965
[49] Safer internet plus http://europa.eu.int/information_society/activities/sip/index_en.htm
[50] IST Results http://istresults.cordis.europa.eu/
[51] Information Society // European Commmission http://www.europa.eu.int/scadplus/leg/en/s21012.htm

Tačiau programų įgyvendinimas labai priklauso nuo kiekvienos šalies ir jos vadovų informacinės visuomenės plėtros ir informacijos saugumo politikos suvokimo, nuo šalies mentaliteto, tradicijų ir patirties šioje srityje. Jeigu valstybė suvokia šiuos aspektus ir pasiruošusi veikti žiniomis grįstoje visuomenėje, tuomet Europos Komisijos parengtos programos yra tik papildomos priemonės nacionalinei informacijos apsaugos politikai tobulinti ir šalies konkurencingumui didinti.

Europos Sąjungoje vyrauja pažangus požiūris į informacinę visuomenę ir žinių ekonomiką. Parengusi Lisabonos strategijos tikslus ir priemones jiems įgyvendinti, Europos Komisija žengė rimtą žingsnį informacijos saugumo politikos įgyvendinimo link. Vienas iš svarbiausių Lisabonos strategijos tikslų yra konkurencingumo didinimas, kuriam vienas iš reikšmingiausių aspektų yra informacinių technologijų plėtra, saugi prieiga prie informacijos ir asmens duomenų apsauga.

Europos Sąjungos informacijos ir informacinių sistemų saugumo politika užtikrina saugią prieigą prie informacijos ir išsaugo jos vertę išlaikant svarbios informacijos duomenų konfidencialumą ir autentiškumą. Šie aspektai yra nuolat pabrėžiami visuose rengiamuose dokumentuose. Į šiuos aspektus atsižvelgiama rengiant visas Europos Sąjungos programas šioje srityje.

Europos Komisijos parengtos direktyvos ir reglamentai yra atspirties taškas valstybėms narėms rengiant nacionalinius teisės aktus, tačiau šių direktyvų perkeltinas į nacionalinę teisę priklauso nuo kiekvienos šalies mentaliteto, tradicijų bei realios situacijos suvokimo. Šiuo metu Europos Sąjungoje yra keletas pagrindinių direktyvų ir jas lydinčių papildomų dokumentų.

Viena reikšmingiausių direktyvų informacijos ir duomenų apsaugai yra Duomenų apsaugos ir elektroninės komunikacijos sektoriaus direktyva, priimta 2002 metais, kuri reglamentuoja naujų technoloijų ir naujų paslaugų elektroninėje terpėje atsiradimą bei naudojimą, vartotojų teises ir pareigas, bei „spam“ (nepageidaujamų elektroninių laiškų) plitimą Internetu.

Kita svarbi direktyva daugiausia apima elektroninio ryšio naudojimą ir duomenų srautą elektroninio ryšio kanalais, o taip pat ir elektroninėje terpėje veikiančius subjektus. Tai 2002 metais Europos Parlamentas ir Europos Taryba priimta Direktyvą dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos. Ši direktyva yra plačiai taikoma daugelyje Europos Sąjungos valstybių ir nustato elektroninių ryšių paslaugų, elektroninių ryšių tinklų, susijusių priemonių ir susijusių paslaugų reguliavimo suderintą sistemą. Ji nustato nacionalinių reguliavimo institucijų užduotis ir procedūras, kurios užtikrintų, kad reguliavimo sistema būtų suderintai taikoma visoje Bendrijoje.

Siekdama visapusiško informacijos ir ryšių apsaugos politikos įgyvendinimo, Europos Komisija steigia tarptautines organizacijas, tokias, kaip Ekonominio bendradarbiavimo ir plėtros organizacija

(OECD), Tarptautinė telekomunikacijos sąjunga (ITU), Verslo ir pramonės patariamasis komitetas (BIAC), kurios rengia teisės aktus, rekomendacijas valstybėms narėms, koordinuoja programas, projektus ir kitas iniciatyvas. Tokių organizacijų patirtis yra neįkainojama, nes jų nariai, ateidami į organizaciją, atsineša savo sukauptą patirtį, žinias ir veiklos metodus ir panaudoja bendram darbui.

Šiuo metu visame pasaulyje atliekami tyrimai šioje srityje ir bandoma sukurti tokią techniką, kuri maksimaliai apsaugotų duomenis. Tai ypatingai svarbu tarptautinei elektroninei prekybai tarp Europos Sąjungos šalių ir trečiųjų šalių ir daugiausiai apima elektroninę bankininkystę, kur perkantis asmuo privalo pateikti savo duomenis, o juridiniai ir fiziniai asmenys atsiskaitymui naudojasi elektroninio parašo galimybėmis.

4. Lietuvos informacijos saugumas po įstojimo į ES: situacijos vertinimas

Informacijos saugumo tyrimai Lietuvoje apima tik statistinių duomenų analizę, vertina nusikaltimų elektroninėje erdvėje skaičių, nusako kaip plačiai naudojamos informacijos ir kompiuterio apsaugo priemonės. Tačiau iki šiol nebuvo bandyta apklausti tas institucijas kurios dirba informacijos ir tinklų saugumo srityje, bet atsakingos už skirtingą saugumo sritį. Patys darbuotojai gali žymiai geriau įvertinti kas šiuo metu daroma šioje srityje, kaip pasikeitė interneto vartotojai, ko galime tikėtis ateityje.

4.1. Tyrimo metodika

Tyrimo tikslas - nustatysi pagrindinius Lietuvos informacijos saugumo politikos pokyčius, kurie įvyko po įstojimo į ES. Tyrimo atlikimo laikas - 2007 metų balandžio 1-30 dienomis. Buvo apklausta 10 respondentų, iš kurių keturi dirba privačiame sektoriuje ir 6 - valstybiniame. Dalyvavo dvi telekomunikacijų bendrovės, dvi įmonės, kurios dirba IT (informacinių technologijų) srityje, bankas, taip pat valstybinės, kurios užtikrina konfidencialių ir asmens duomenų apsaugą, rengia įstatymus, rekomendacijas informacijos ir tinklų saugumui užtikrinti, siekia apsaugoti elektroninį ryšį ir interneto vartotojus nuo kompiuterinių nusikaltimų. Respondentų amžius svyruoja nuo 25 iki 45 metų amžiaus.

Interviu buvo atliekamas Vilniuje respondentų darbovietėje tiesioginio pokalbio metu, telefonu ir panaudojant *skype* programą. Pokalbio trukmė svyruoja nuo 15 iki 30 minučių. Vidutinis interviu laikas yra 22,5 minutės.

4.2. Tyrimo rezultatai.

Galima išskirti svarbiausius interviu aspektus, kurie atspindi Lietuvos informacijos saugumo politikos pokyčius ir ES įtaką. Pirmiausia tai kompiuterinių nusikaltimų skaičius, pažeidimų sąrašas, prevencijos priemonės. Kitas aspektas susijęs su tarptautiniu tarpinstituciniu bendradarbiavimu, visuomenės informavimu, vartotojo pasirengimu priimti naujus iššūkius.

Kompiuteriniai nusikaltimai ir jų prevencija. Daugelyje apklaustų organizacijų atsirado nauji skyriai, nauji padaliniai, už įmonės informacijos saugumą atsakingi darbuotojai. Nors šie skyriai susiformavo tik pastaraisiais metais, tačiau daugelis teigia, kad įstojimas į ES šių skyrių atsiradimo

neįtakojo. Beveik visose valstybinėse institucijose šiuo metu veikia padaliniai prižiūrintys organizacijos informacines sistemas ir atsakingi už informacijos ir tinklų saugumą.

Lietuvos Respublikos Ryšių reguliavimo tarnyba taip pat įkūrė Tinklų ir informacijos saugumo skyrių. Šis skyrius rūpinasi Lietuvos ryšių ir tinklų saugumu, rengia apsaugos nuo kompiuterinių nusikaltėlių priemones, informuoja visuomenę apie aktualiausias problemas, vykdo rinkos tyrimus. Iki šio skyriaus įkūrimo Lietuvoje jokie tyrimai informacijos saugumo srityje nebuvo vykdomi, išskyrus LR Statistikos departamentą, kuris 2003 metais vykdė apklausą. Apklausoje dominuojantys du klausimai neatspindėjo situacijos. Nebuvo įtraukta naujų kompiuterinių nusikaltimų tokių, kaip konfidencialios informacijos išgavimas (Phishing). Nors šis skyrius buvo įkurtas jau po įstojimo į ES - 2005 metais, tačiau skyriaus darbuotojai šį aspektą sieja daugiau su pasikeitusia rinka, naujais vartotojų poreikiais.

Kai kuriose valstybinėse institucijose informacijos saugumas yra tik informacinių technologijų (IT) padalinio viena iš veiklos sričių. Tokie padaliniai taip pat užsiima IT diegimu, plėtra, priežiūra, mokomaisiais seminarais vartotojams. Tačiau informacijos ir tinklų saugumas nėra pagrindinė šio skyriaus veikla.

Lietuvos Respublikos Vidaus reikalų ministerija (VRM) įkūrė Informatikos ir ryšių departamentą, kuris dalyvauja įstatymų, rekomendacijų, nutarimų ir kitų priemonių rengime. Tačiau daugelis darbų prasidėjo dar prieš stojimą į ES.

Kompiuterinių nusikaltimų gausa yra žinoma daugeliui IT specialistų, tačiau tyrimo metu buvo akcentuojami nusikaltimai, su kuriais Lietuvos vartotojai susiduria dažniausiai, tai:

- kompiuteriniai virusai;
- SPAM (nepageidaujami elektroniniai laiškai);
- šnipinėjimas (Spyware).

Valstybinės įstaigos išskyrė taip pat ir konfidencialios informacijos vagystę, kaip vieną iš pavojingiausių nusikaltimų elektroninėje erdvėje. Su SPAM (nepageidaujamais elektroniniais laiškais) beveik kasdien susiduria absoliuti dauguma Lietuvos vartotojų. Kaip valstybinės, taip ir privačios organizacijos bendradarbiauja su Nusikaltimų elektroninėje erdvėje tyrimų skyriumi ir teigia, kad yra buvę atvejų, kuomet buvo pavogti slaptažodžiai, įsibrauta į kompiuterinę sistemą ir pavogta slapta informacija. Daugiausia dėl to yra kalti patys vartotojai, kadangi neteikia pakankamai dėmesio apsaugai iki tol, kol patys nenukenčia. Institucijų atstovai teigia, kad svarbiausia yra saugoti asmens kodą, nes jis yra vienas pagrindinių raktų duomenų vagystėms.

Lietuvos interneto vartotojus dažniausiai atakuoja ne Lietuvoje sukurti virusai, nors kompiuterinių nusikaltėlių gausu ir Lietuvoje. Tačiau siekdami išlikti neatpažinti, Lietuvos kompiuteriniai nusikaltėliai veikia užsienyje. Kaip išimtį galima paminėti „SANDRA“ virusą, kurio kūrėjai atrado pakankamai naują elektroninį komunikacijos kanalą „Skype“, kuriame ir paplito.

Nors kompiuteriniai nusikaltėliai slepia savo buvimo tinkle vietą, tačiau tikimybė pagauti nusikaltėlius tikrai yra ir tuo rūpinasi minėtas Nusikaltimų elektroninėje erdvėje tyrimų skyrius prie LR Vidaus reikalų ministerijos. Kitos įstaigos ir organizacijos bendradarbiauja su šiuo skyriumi gaudant kompiuterinius nusikaltėlius. Pavyzdžiui, yra atveju kuomet pinigine bauda buvo nubausti asmens duomenų vagys. Šiuo atveju bendradarbiavo net trys institucijos.

Yra daug įvairių receptų kaip apsisaugoti nuo virusų ir kitų nepageidaujamų įsibrovimų į kompiuterius**.** Valstybinės įmonės turi laikytis LR Vidaus reikalų ministerijos išleistais nutarimais apie informacinių sistemų ir ryšio saugumą.[52] Taip pat turi atsižvelgti į standartus taikomus informacinėms sistemoms. Pavyzdžiui, norėdami rinkti asmens duomenis, įmonės darbuotojai privalo užregistruoti savo informacinę sistemą. Valstybinė duomenų apsaugos inspekcija prižiūri visas registruotas informacines sistemas ir stebi duomenų srautus, kad jie nepatektų trečiajai šaliai.

Tyrimo metu apklaustos institucijos rūpinasi ne tik savo institucijos informacijos bei tinklų saugumu, bet ir tais duomenų srautais, kurie eina per jų institucijas. Kokių darbo principų laikosi šios organizacijos?

- Naudoja atitinkamas antivirusines programas;
- Sugeba aptikti virusą ir žino kaip jį pašalinti;
- Konsultuoja ir informuoja darbuotojus apie kompiuterinius pavojus ir apsisaugojimo būdus
- Vykdomi periodiniai pilni informacijos skanavimai;
- Antišnipinėjimo programas (Antispyware);
- Naudoja ugniasienes;
- Vykdo informacinių sistemų auditą;
- Periodiškai atnaujina sistemą.

.

Svarbiausias aspektas, kurį išskyrė respondentai, yra informacijos ir interneto vartotojo budrumas ir atsargumas skelbiant duomenis internete, dirbant su programine įranga ir informacinėmis sistemomis. Efektyviausia yra vartotojų supažindinimas su būtinybe ir priemonėmis, nes kad ir kaip gerai veiktų kiti dalykai, jeigu vartotojas pats nesieks savo duomenų saugumo – jo nebus.

[52] LR VRM nutarimas

Atsakomybės už Lietuvos interneto vartotojų saugumą neprisiima nei viena institucija, nes visa atsakomybė tenka pačiam vartotojui, tačiau yra institucijų, kurios stengiasi apsaugoti ne tik saugomą konfidencialią informaciją, bet ir per tas institucijas einančius duomenų srautus, kurie patenka į viešą elektroninę erdvę. Skirtingos institucijos atsakingos už skirtingą veiklą IT srityje, bet dalis respondentų tai laiko problema, nes bendradarbiavimas yra nenuoseklus. Vyriausybė taip pat identifikavo tai kaip vieną iš problemų, kuria bandoma išspręsti „Tinklų ir informacijos saugumo įstatymu“. Įstatymas turi aiškiai suformuluoti koordinuojančios institucijos ir kitų organizacijų veiklą šioje srityje.

Pagal VRM nutarimą, kiekviena informacinė sistema turi turėti saugos įgaliotinį, bent vieną žmogų arba padalinį, atsakingą už tos sistemos saugumą. Stambios telekomunikacijų bendrovės ir valstybinės institucijos, tiesiogiai susijusios su tinklų ir ryšio saugumu, prisiima atsakomybę kaip institucijos, tačiau tose organizacijose, kuriose už informacijos saugumą atsako tik skyrius arba vienas žmogus, visą atsakomybę turi prisiimti darbuotojas, dėl kurio kaltės arba kuriam dalyvaujant, įvyko informacijos saugumo pažeidimas.

Į klausimą „Ar iki įstojimo į ES buvo kokių nors kompiuterinių nusikaltimų prevencijos priemonių?“ vienos organizacijos atsakė, kad buvo, bet neefektyvios, kitos teigė, kad tik pastaruoju metu pradėjo taikyti tam tikras priemones, diegti antivirusines ir kitas apsaugos programas. Periodas, kada buvo pradėtos diegti apsaugos priemonės, apima apie dvejus metus.

Tačiau ne visos valstybinės institucijos yra pažangios informacinių technologijų ir jų apsaugos srityje. Pavyzdžiui, Valstybinė duomenų apsaugos inspekcija (ADA) kontroliuoja Asmens duomenų apsaugos įstatymo[53] vykdymą, priima skundus iš gyventojų dės asmens duomenų vagystės. Siekdami apsaugoti duomenis ADA laiko juos popieriniu formatu - popierinėse bylose. Tokią laikmeną jie teigia esant saugesne palyginus su skaitmeniniu formatu ir taip išsprendžia informacijos saugumo problemą. Į klausimą „Ar planuojate pereiti prie skaitmeninio duomenų saugojimo formato?“, atsakė: „*Mes neturime teisės, nes mes atsakingi už jų saugojimą*“. Institucijos skirtingai supranta ir informacijos apsaugą ir kompiuterinių sistemų saugumą.

Palyginus su 2003-2004 metų tyrimų duomenimis[54] , nusikaltimų el. erdvėje skaičius auga. Tačiau dauguma vartotojų atsakė, kad šį aspektą įtakoja ne stojimas į ES, bet kompiuterių naudojimo koeficientas, interneto vartotojų skaičiaus augimas ir kiti aspektai. Valstybinės institucijos, kuri vykdo tyrimus informacijos ir tinklų naudojimo srityje, darbuotojai teigia, kad „*..jeigu 2003 metais interneto vartotojų skaičius, įskaitant ir mobiliąją telefoniją, buvo 4 procentai, 2006 metais šis skaičius išaugo iki*

[53] Lietuvos Respublikos Asmens duomenų apsaugos įstatymas
[54] RRT tyrimas

46 procentų. Būtent tai įtakojo, jog didelė visuomenės dalis tapo priklausoma nuo internetinio ryšio. Todėl tapo būtinybė rūpintis saugumu, vartotojų informavimu ir priemonių rengimu.“

Teisinis reglamentavimas. Pasikeitė reikalavimai toms informacinėms sistemoms, kurios yra bendro naudojimo su ES šalimis. Pavyzdžiui, muitinė turi bendrą sistemą, todėl jai galioja bendri ES šalių reikalavimai. O Lietuvos institucijos vadovaujasi tais teisės aktais, kurie galioja Lietuvoje. Dalis respondentų mano, jog dėl informacijos saugos ir kompiuterinių sistemų saugos naujų reikalavimų neatsirado ir vidaus darbo nepaveikė, tačiau VRM atstovai teigia, kad rengia nutarimus dėl informacijos saugumo, kuriais turi vadovautis visos valstybinės institucijos.

Kadangi RRT tiesiogiai susijusi su ryšiais, todėl informacinių technologijų sritis visada buvo aukšto lygio, buvo naudojamos naujausios sistemos. Tarnyba saugo informaciją apie visus Lietuvos įrenginius, bokštus, ryšio saugumas visada buvo užtikrinamas. Tačiau sunku pasakyti, ar tai susiję su stojimu į ES. Informacinės sistemos nuolat tobulinamos, atliekamas sistemų auditas ir siekiama efektyviai apsaugoti elektroninį ryšį, informaciją ir tinklus. „*Tai daugiau susiję su tuo, kad mūsų darbuotojai bendradarbiauja su ES šalimis, mokosi iš jų ir dalinasi patirtimi. Tuomet grįžta su atitinkamais reikalavimais mums. Turbūt tai daugiausia paveikė, prasiplėtė akiratis*“.

Į kokius Lietuvos ir ES reikalavimus, rekomendacijas, teisės aktus atsižvelgia Lietuvos valstybinės ir privačios institucijos? Duomenų apsaugos srityje visos ES direktyvos perkeltos į nacionalinę teisę. Tačiau problema yra ir pačioje ES, nes iki šiol nėra atskiros tinklų ir kompiuterių saugumo direktyvos, kuria remiantis ES šalys galėtų parengti įstatymą. Yra tik Elektroninių ryšių, duomenų apsaugos direktyvos, kurias Lietuvos valstybinės institucijos laiko geromis. Tačiau trūksta direktyvos, reglamentuojančios informacijos ir tinklų saugumą. Todėl kiekviena šalis pati rūpinasi informacijos saugumo teisine baze. Pvz. Suomija, Vokietija, respondentų nuomone, yra toli pažengusi. Kai kurios valstybinės institucijos minėjo ir Olandiją, kaip vieną pavyzdingiausių ES šalių šioje srityje, Tačiau privačios institucijos bendradarbiauja su daugeliu ES šalių. Lietuva planuoja perimti kitų šalių praktiką, ruošiasi priimti „Tinklų ir informacijos saugumo įstatymą“, kuris kitose šalyse yra jau seniai priimtas.

Institucijos, kurių pagrindinis tikslas nėra duomenų apsauga ir kurios turi tik atskirus darbuotojus atsakingus už informacijos saugumą, teigia, kad „*jeigu nedarai nieko nusikalstamo, tai nereikia atsižvelgti į teisės aktus*“ ir darbe neatsižvelgia, išskyrus įrangos įsigijimo taisykles. „*Darbe taikome tai kas yra naudingiausia ir praktiškiausia mūsų atveju*“.

Visuomenės informavimas ir bendradarbiavimas

Kokias galimybes informacijos saugumo politikai atvėrė stojimas į ES? Pirmiausia, tarptautinis bendradarbiavimas. VRM dalyvauja ES šalių darbo grupėse, kurios užsiima informacijos ir tinklų saugumo politika, leidžia nutarimus, kurie nusako pagrindinius reikalavimus informacinėms sistemoms, naudojamoms teikiant paslaugas, renkant duomenis ir kt.

ADA dalyvauja visose asmens duomenų apsaugos programose, darbo grupėse Lietuvoje ir ES šalyse. Visos rekomendacijos išverstos į lietuvių kalbą, perkeltos direktyvos. Dabar į tai kreipiama daugiau dėmesio, bet tai susiję su kompiuterinių nusikaltimų skaičiaus augimu..

Telekomunikacijos bendrovės daugelį akcijų vykdo iškart keliose šalyje, taip pat nuolat vykdo tarptautinius mainus ir dalinasi patirtimi ne tik saugumo, bet ir darbo organizavimo srityje.

Kai kurios organizacijos, pavyzdžiui, RRT vykdo akcijas, kurių metu informuoja vartotojus apie būtinybę apsaugoti informaciją bei kompiuterinius tinklus. Viena iš labiausiai pavykusių akcijų yra „Apsaugok savo kompiuterį. RRT išleido kompaktinį diską, kuriame yra patarimų ir kompiuterinių apsaugos programų, kurias galima įdiegti. Buvo išleista 1000 egzempliorių ir nemokamai platinama visoje Lietuvoje, mokyklose ir kitose įstaigose bei viešose vietose. Akcijos metu kiekvienas vartotojas, atėjęs į RRT, taip pat galėdavo gauti tokį diską.

Visuomenės informavimas daugiausiai vyksta per tinklapį e-saugumas. Siekiama, kad tai būtų centriniai vartai apie informacijos saugumą. Tinklapis administruojamas RRT, tačiau kitos institucijos bei RRT partneriai gali talpinti savo pranešimus. Pavyzdžiui, kompanija Blue Bridge nuolat parengia informaciją aktualiausiomis temomis. Bankai „išeina“ su svarbia informacija apie elektroninę bankininkystę. Todėl šis tinklapis laikomas sėkmingu. Tinklapyje taip pat talpinami visi įspėjimai, kaip pvz., apie „Sandra“ virusą, kaip neužsikrėsti, o jeigu užsikrėtė, tai kaip apsaugoti kompiuterį, surasti ir sunaikinti virusą. RRT dalyvauja programoje „Safer Internet Plus“. Tai ES koordinuojama programa, kuri vyksta 24-iose šalyse, tame tarpe ir Lietuvoje.

Privačios institucijos daugiau informuoja savo darbuotojus išleisdamos informacijos ir kompiuterių naudojimosi vadovus, tačiau į visuomenę išeina tik su atskirais spaudos pranešimais arba reklaminiais bukletais.

ADA informuoja gyventojus apie visus kompiuterinių nusikaltimų pavojus interneto svetainėje, bendradarbiauja su Lietuvos ir užsienio institucijomis. Bendradarbiauja su Vokietija, su kitomis šalimis, nes kiekvienoje šalyje yra tik viena už asmens duomenų saugumą atsakinga įmonė. Jeigu Lietuva nebūtų įstojusi į ES, nebūtų vienos organizacinės struktūros, nebūtų vieningo mechanizmo. Lietuvoje yra labai

daug valstybinių institucijų, kurios yra dar labai nepatyrusios ir kurioms reikia daugiau šviečiamosios veiklos. Pavyzdžiui mokyklose apie tai net nešnekama, trūksta specialistų, postūmio iš valdžios.

Tačiau kaip viena iš valstybinių institucijų problemų, dėl kurios jaučiamas informacijos apie informacijos apsaugos priemones stygius, išskiriama lėšų ir žmogiškųjų resursų stoka. Privačios institucijos vardija laiko trūkumą. Vienos organizacijos sugeba užsidirbti pinigų tokioms priemonėms, o kai kurioms yra sudėtingiau.

Bendradarbiavimo su kitomis šalimis, teisinė praktika buvo perkelta į nacionalinę teisę, buvo priimtas Elektroninių ryšių įstatymas, ES lėšomis kuriami mokymai, perkami kompiuteriai. Įmonės iš ES šalių siekdamos didesnių rinkų, stengiasi kuo labiau informuoti visus apie savo produktus, bei saugumo būtinybę.

Kokios Lietuvos institucijos ir organizacijos bendradarbiauja tarpusavyje siekiant sustiprinti informacijos saugumo politiką?

- Microsoft,
- Bankai,
- VGTU,
- Baltic Amadeus,
- IBM,
- HP,
- Kitos privačios institucijos.

Respondentai išskyrė bevielį tinklą kaip vieną iš aktualiausių IT problemų, nes juo lengva ir patogu naudotis, tačiau saugumo atžvilgiu jis turi daugiausia spragų. Ryšis yra viešas ir jeigu jis perimamas, tuomet galima disponuoti visais duomenimis. Šiuo metu tai yra jautriausia vieta visoje saugumo politikoje.

Ar Lietuvos informacijos ir interneto vartotojai jaučiasi saugesni po įstojimo į ES? Respondentų nuomone, saugesnę elektroninę erdvę įtakoja naujos priemonė, bet ne stojimas į ES. Saugumo priemonės yra paplitusios visose šalyse, tiek Amerikoje yra incidentų, tiek Lietuvoje. Internetas yra globalus tinklas, neturi jokių sienų ir vartotojai gali nevaržomai komunikuoti, bet tai yra atviri vartai nusikaltimams. Jeigu pažiūrėtume statistiką ir palygintume 2005 ir 2006 metų RRT tyrimus, tai 2006 vartotojai mažiau susiduria su incidentais, o priemonių naudojimas išaugo. Tačiau labai didelis procentas

vis tiek susiduria, naudojamos priemonės pagerino situaciją, bet neišsprendė jos. Dar reikalingos didelės pastangos, kad situacija pasikeistų.

Visos apklaustos institucijos ir organizacijos mano, jog stojimas į ES buvo daugiau pastūmėjimas saugesnės informacijos politikos ir efektyvesnių priemonių rengimo link, bet ne svarbiausias įvykis. Respondentai nemano, jog jeigu Lietuva nebūtų įstojusi į ES, Lietuvos saugumas išliktų toje pačioje vietoje, vis tiek šis procesas vyktų. Respondentų teigimu daugybė faktorių įtakoja šią sritį, kaip, pavyzdžiui, ūkio, informacinių technologijų plėtra. Valstybinės institucijos IT specialistas teigia, kad įstojimas į ES „ *galbūt prisidėjo, tačiau nemanau, jog neįstojus į ES, toliau taip pat kaip dabar besivystant IT būtų mažiau skirta dėmesio apsaugai. Ar šiaip ar taip kiekvienas nori būt saugus, nesvarbu kokiame bloke gyvena. Tarkim Malaizija juk nėra ES, bet aš nemanau jog ten reziduojantys specialistai mažiau skiria dėmesio saugumui*“.

„*Tikimės, kad vartotojai jaučiasi saugesni...*“ – Valstybinės institucijos darbuotojas.

„*Manau, kad mūsų vartotojai nieko nežino apie saugumą, ypač imant dideliu mastu...*“ – valstybinės įstaigos darbuotoja.

4.3. Tyrimo rezultatų interpretacija.

Tyrimo dalyviai pateikė daug įvairių nuomonių, tačiau visi vieningai teigia, kad stojimas į Europos Sąjungą nebuvo lūžis Lietuvos informacijos saugumo politikoje. Teigiama, kad daug įvairių aspektų lėmė tai, jog dabar daugelis informacijos ir interneto vartotojų, eilinių darbuotojų, studentų žino, kad norint apsaugoti savo duomenis, informaciją ir asmeninį kompiuterį, reikia naudoti antivirusines programas, nuolat tikrinti kompiuterį dėl naujų virusų atsiradimo, saugotis nepageidaujamų elektroninių laiškų. Tokių priemonių atsiradimą tyrimo dalyviai susiejo su ūkio plėtra, pažangą IT srityje, informacijos sklaidą. Tačiau liko neįvertinta tai, kad ūkio plėtrą labai įtakojo ne tik IT plėtra, bet ir stojimas į ES, nes Lietuva gavo finansavimą daugeliui veiklos sričių būtent iš ES struktūrinių fondų. Tai ir švietimas, ir kompiuterizavimas (ypač kaimų, mokyklų, bibliotekų), ir IT sritis.

Lūžis įvyko šiek tiek anksčiau, nei stojimas į ES. Lietuva ruošėsi stojimui ir turėjo padaryti pažangą daugelyje sričių bei atitikti ES standartus.

Pagrindinis ES nuopelnas informacijos saugumo srityje, kurį nurodė respondentai yra ES teisinė praktika. Tačiau yra daugybė kitų aspektų, kurių apklaustos institucijos nevertina kaip įtakos. Atsivėrė naujos galimybės keliauti, lengviau susisiekti su kitomis šalimis (be sienų), daugelis procedūrų, susijusių su kelionėmis, prekyba, tapo paprastesnės ir užima mažiau laiko. Būtina įvertinti ir tai, kad bendraudami

su kitų šalių ekspertais, lietuviai gali praplėsti akiratį, dažniau susitikti su kolegomis iš kitų šalių (pavyzdžiui, lėktuvų bilietai dabar yra pigesni, dažnai vyksta akcijos, „paskutinės minutės“ pasiūlymai). Lietuvai dabar galioja ir ES standartai, rekomendacijos, direktyvos visose srityse. Tikėtina, kad šie laiko ir praktikos išbandyti standartai nebūtų priimti, jeigu Lietuva nebūtų įstojusi į ES. Bendradarbiavimas su ES šalimis vyko nuolat, tačiau po įstojimo į ES jis tapo glaudesnis.

Nei vienas respondentas nepaminėjo naujų darbo vietų atsiradimo. Iki įstojimo į ES bedarbystė Lietuvoje klestėjo, tačiau, kai sienos tapo atviros, lietuviai susirado darbą ir kitose ES šalyse. Tai turi įtakos ir informacijos saugumui, nes lietuviai gali stažuotis ir kelti kvalifikaciją kitose šalyse, kur informacijos saugumo politika efektyvesnė ir labiau pažengusi.

Respondentai informacijos vartotojų saugumą sieja su naujų priemonių kūrimu, vartotojų skaičiaus augimu. Tačiau vartotojų skaičiaus augimas tiesiogiai priklauso nuo kompiuterizacijos lygio, kurio kėlimui ir naudojamos ES lėšos. Todėl galima teigti, kad ES turi įtakos Lietuvos interneto vartotojų skaičiaus augimui.

Lietuva, galėdama pasinaudoti ES fondais, ES šalių praktika ir kitais privalumais, kelia savo BVP, kas yra, remiantis Lisabonos strategija[55], visos ES ir kitų šalių tikslas.

Atsižvelgiant į tyrimo rezultatus ir Lietuvos praktiką dirbant informacijos saugumo srityje, galima išskirti stojimo į ES pasekmes:

- Glaudesnis bendradarbiavimas tarp vietinių ir užsienio institucijų ir įmonių;
- Teisinės bazės tobulinimas;
- Tarptautinių standartų taikymas;
- Užsienio šalių geros praktikos pavyzdžių taikymas;
- Finansiškai silpnų sričių palaikymas (žemės ūkis, kompiuterizavimas);
- Naujų darbo vietų kūrimas;
- Interneto vartotojų skaičiaus augimas.
- BVP augimas.

Lietuva IT srityje bendradarbiauja ne tik su ES šalimis, bet ir su Japonija, JAV. Šios šalys yra pažangios ir informacijos bei tinklų saugumo srityje ir yra pavyzdys Lietuvai. Tikėtina, kad dėl šios priežasties Lietuvos IT specialistai labiau linkę pripažinti šias šalis kaip įtakojančias Europos rinką, o kartu ir Lietuvos informacijos saugumo politiką.

[55] Lisabonos strategijoje vienas iš tikslų yra kelti bendrą vidaus produktą ir pralenkti JAV.

IŠVADOS

Naujų informacijos technologijų skverbimasis į mūsų kasdieninį gyvenimą suteikia daugiau galimybių pažangioms informacinėms sistemoms, naujoms paslaugoms atsirasti, pagerina informacijos saugojimo, naudojimo ir perdavimo galimybes. Tačiau kaip matome iš darbe pateikiamų informacijos ir elektroninio ryšio saugumo problemų ir spragų pavyzdžių, ši tema yra aktuali ir elektroninių paslaugų tiekėjai bei vartotojai dažnai su ja susiduria. Elektroninio ryšio saugumo problemos kelia nerimą daugumai Lietuvos piliečių ir įmonių.

Lietuvoje atlikti tyrimai parodo skirtingus rezultatus. Lietuvos Respublikos ryšių reguliavimo tarnybos tyrimas parodė, kad dauguma informacijos vartotojų jaučiasi saugūs veikdami internete, tačiau ekskomisarų biuro atlikto tyrimo rezultatai yra netikėti ir parodo nepakankamą šalies dėmesį informacijos saugumo politikai. Tyrimas parodė, jog dauguma Lietuvos įmonių vadovų klaidingai mano, jog jų kompiuterinės sistemos ir duomenų srautai yra saugūs. Lietuvos įmonių kompiuteriai, kuriuose yra konfidenciali strateginė, finansinė informacija, nėra pakankamai apsaugoti ir įsilaužėliai gali nekliudomi naudotis sistemų resursais. Todėl ši problema vis dar labai aktuali ir neišspręsta iki galo.

Lietuvos Respublikos ryšių reguliavimo tarnyba bandė išspręsti Lietuvos informacijos ir interneto vartotojų saugumo problemas išleisdama daugybę apsaugos programų talpinantį kompaktinį diską „Apsaugok savo kompiuterį“. Ši akcija, nors ir pagerino situaciją, tačiau tai visiškai neišsprendė problemos. Kompiuterinių nusikaltimų skaičius išaugo, bet ši šuolį galima vertinti tik lyginant su vartotojų skaičiaus augimu. Išaugo interneto vartotojų skaičius, išaugo ir pavojų tikimybė.

Tyrimo rezultatų ir dalyvių nuomonės nesutapimas leidžia suprasti, kad Lietuvoje informacijos saugumo politika yra pakankamai silpna. Tačiau informacijos visuomenės plėtros strategijos ir veiksmų planų kūrimas bei įgyvendinimas, naujų teisės aktų, reglamentuojančių informacijos saugumo sritį, priėmimas ir senų aktų papildymas teikia vilties, kad bus kryptingai dirbama informacijos saugumo politikos efektyvumo gerinimo link.

Elektroninės erdvės galimybių analizė parodė, jog informacijos technologijos sukūrė papildomus nusikaltimo įrankius. Galimybė prisijungti prie globalaus tinklo (interneto) suteikia erdvę e-verslo, e-paslaugų, e-demokratijos plėtrai, bet tuo pačiu leidžia prisijungti prie bet kurio kompiuterio esančio šioje erdvėje ir panaudoti gautą informaciją nusikalstomai veiklai. Todėl iškyla būtinybė imtis papildomų priemonių informacijos apsaugos ir kontrolės srityje, kurios kiek galima sėkmingiau užkirstų kelią nusikalstamoms veikloms, kurioms vis didesnes galimybes atveria informacinės technologijos.

Viena iš aktualiausių problemų šiuo metu laikomas bevielio ryšio naudojimas. Tai pakankamai nauja sritis ir šiuo metu labiausiai pažeidžiama informacijos saugumo politikos grandis. Ši sritis yra neištirta ir reikalauja naujausių ir pažangiausių tyrimų, didesnio ekspertų dėmesio, tarptautinės praktikos panaudojimo ir kitokių efektyvių sprendimų.

Teisės aktai, reglamentuojantys informacijos saugumą, padeda nustatyti svarbiausius aspektus, į kuriuos turi atsižvelgti kiekvienas informacinėje visuomenėje veikiantis subjektas. Tai - asmens duomenų apsauga, intelektualios nuosavybės apsauga, elektroninių ryšių apsauga, teisės į privatumą apsaugą, pagrindinių žmogaus teisių laikymasis, valstybinės informacijos konfidencialumas, demokratinės visuomenės pagrindai ir kiti. Lietuva, kaip Europos Sąjungos narė, vadovaujasi ne tik nacionaliniais teisės aktais, bet ir Europos Konvencija bei Europos Tarybos Ministrų komiteto teikiamomis rekomendacijomis ir gairėmis.

Reikėtų pabrėžti, kad šiuolaikiniai teisinai ir norminiai aktai, etikos kodeksai reglamentuoja ne tik informacijos kūrybos, informacijos teikimo, perdavimo kokybę, bet apibrėžia ir pačios informacijos turinį bei pobūdį. Spraga pastebima informacijos ir tinklų saugumo reglamentavime. ES neturi informacijos ir tinklų saugumo direktyvos, tuo tarpu Lietuva neturi atitinkamo įstatymo. Tačiau šią problemą bandoma spręsti, ir Lietuvos valstybinės institucijos artimiausiu metu turėtų svarstyti taip trūkstamo įstatymo rengimą. Daugelis ES šalių turi tokį įstatymą, todėl Lietuva planuoja panaudoti ir kitų šalių praktiką.

Siekdami apsaugoti asmens duomenis elektroninėje terpėje, turėtume ugdyti interneto vartotojus neskelbti svarbių asmeninių duomenų internete arba skelbti tik tam tikrais atvejais, kai įsitikinama sistemos patikimumu. Vartotojas arba duomenų suteikėjas turi turėti galimybę sutikti skelbti savo duomenis arba bet kada atsiimti savo sutikimą ir gauti garantiją, kad jo duomenys nebuvo panaudoti jam nežinant. Asmens duomenys gali būti naudojami tik tam tikrais teisėtais atvejais, kai šie duomenys turi viešą interesą ir gali padėti užkirsti kelią nusikaltimui ar kitu valstybinės reikšmės atveju.

Duomenų valdytojai turi imtis atitinkamų techninių ir organizacinių priemonių, skirtų užtikrinti asmens duomenų konfidencialumą. Ypač jie turėtų imtis tokių priemonių, kurios užkirstų kelią be leidimo prieiti prie informacijos, keisti, pranešti ar kokia kita neleistina forma tvarkyti duomenis. Jeigu duomenis būtina išlaikyti tokioje formoje, kurioje negalima nustatyti asmenų tapatybės, turi būti pasitelkti organizaciniai ir techniniai, ypač automatizuoti, ištekliai, siekiant užkirsti kelią neleistinam duomenų subjekto tapatybės nustatymui.

Socialinės atsakomybės ugdymas pirmiausia prasideda nuo kiekvieno piliečio sąmoningumo ir visuomenės tinkamo elgesio normų suvokimo. Norėdamas būti socialiai atsakingu, elektroninio ryšio tiekėjas turėtų laikytis tokių principų, kaip prieigos suteikimas prie saugaus tinklo, sąžiningas derėjimasis dėl elektroninio ryšio paslaugų, sąžiningas jų apmokėjimas, ryšio integralumo užtikrinimas, paslaugų

kokybė, tinklų saugumas. Tuo tarpu vartotojas turėtų atsakingai naudotis kompiuterinėmis programomis, neskelbti neteisėto turinio informacijos, nepersiųsti virusų kitam vartotojui, bet kuo skubiau jį panaikinti.

Elektroninio ryšio tiekėjai turėtų supažindinti vartotojus su bendromis e-paslaugų naudojimosi rekomendacijomis:

1. Naudoti antivirusines programas;
2. Nuolat atnaujinti programinę įrangą;
3. Saugotis neaiškios kilmės elektroninių laiškų su prikabintais failais;
4. Naudoti ugniasienes (firewall);
5. Išsaugoti svarbių failų atsargines kopijas;
6. Naudoti sudėtingus slaptažodžius;
7. Šifruoti svarbius pranešimus;
8. Periodiškai atlikti auditą;
9. Naudoti kitas papildomas apsaugas.

Atliktas tyrimas parodė, kad Lietuvos institucijų darbuotojai ir IT specialistai pastebi pažangą, kuri padaryta informacijos ir tinklų saugumo srityje, tačiau nesieja jos su Lietuvos stojimu į ES. Šią pažangą jie suvokia kaip pačios Lietuvos ir jos informacinių technologijų specialistų nuopelną, nors dauguma išvardintų faktorių yra stojimo į ES pasekmė. Tai - glaudesnis bendradarbiavimas tarp vietinių ir užsienio institucijų bei įmonių, teisinės bazės tobulinimas, tarptautinių standartų taikymas, užsienio šalių geros praktikos pavyzdžių taikymas, finansiškai silpnų sričių palaikymas, naujų darbo vietų kūrimas, interneto vartotojų skaičiaus augimas, BVP augimas.

Saugumo supratimas nuolat kinta šiandieniame informacinių technologijų pasaulyje. Nors Lietuva rūpinasi šiuolaikinės visuomenės problemomis, bet kai kurios taip ir lieka neišspręstos. Naujos technologijos sparčiai tobulinamos, todėl yra pakankamai sunku nuspėti galimas spragas ir tinkamai apsaugoti tinklus bei informaciją. Tačiau tarptautinis bendradarbiavimas ir dalinimasis patirtimi bei gera praktika padeda išspręsti šias problemas ir pasiekti geresnių rezultatų kuriant nacionalinę informacijos saugumo politiką.

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS

1. A new framework for electronic communications services [žiūrėta 2007 01 20] Prieiga per Internetą: <**http://www.europa.eu.int/scadplus/leg/en/lvb/l24216.htm**>

2. A new start of Lisbon Strategy: [žiūrėta 2007 01 20] Prieiga per Internetą: <http://europa.eu/scadplus/leg/en/cha/c11325.htm> (2005)

3. Bus ugdoma informacijos saugumo kultūra, Tarptautinis žinių ekonomikos ir žinių vadybos centras, [interaktyvus]. Vilnius, 2005.– [žiūrėta 2005 m. gruodžio 20 d.]. Prieiga per internetą: <http://www.tzc.vu.lt/index.php?cid=1383&new_id=2786&page_nr=5>

4. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 19 November 2004: "Challenges for European Information Society beyond 2005" [**COM(2004) 757** final. [žiūrėta 2007 01 20] Prieiga per Internetą:<http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2004&nu_doc=757>

5. Data protection in the electronic communications sector [žiūrėta 2007 01 20] Prieiga per Internetą: <**http://www.europa.eu.int/scadplus/leg/en/lvb/l24120.htm 2002/58/EC**>

6. DG for Information and Media. (2005) European Commission, Brussels

7. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013, 19/01/2000 p. 0012 – 0020. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

8. Draugiškas internetas [žiūrėta 2007 01 20] Prieiga per Internetą: <http://www.draugiskasinternetas.lt/lt/youth/news?id=1965 >

9. Europos Komisija Finansinė 2007–2013 m. perspektyva“ KOM(2004) 487

10. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių dokumenų judėjimo. (1996).

11. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 460/2004 2004 m. kovo 10 d.

12. Europos Tarybos informacijos biuras. Ministrų komiteto rekomendacijos [interaktyvus]. Vilnius, 2005– [žiūrėta 2005 m. gruodžio 18 d.]. Prieiga per internetą: <http://www.etib.lt/?s=docs_lt&item=25&lang=lt>

13. Facin the Chalenge: The Lisbon strategy for gowth and employment. Luxembourg: Office for Official Publications of the European Communities, 2004.- 51 p

14. General Agreement on Trade and Tariffs, GATT Information Society. [Interaktyvus]. European Commmission, 2005.– [žiūrėta 2005 m. gruodžio 18 d.]. Prieiga per internetą: <http://www.europa.eu.int/scadplus/leg/en/s21012.htm>

15. Glosienė, Audronė Biblioteka informacijos politikos kontekste. Informacijos mokslai. Vilnius:Vilniaus universiteto l-kla, 2000, Nr. 15, p. 11-27

16. Gudauskas, Renaldas Informacijos visuomenės kūrimo strategija: Lietuva globalių permainų kontekste. Informacijos mokslai. Vilnius:Vilniaus universiteto l-kla, 2000, Nr. 14, p. 9-17

17. Informacijos apsauga: Kodėl reikia saugotis? [Interaktyvus]. Iš Apsauga.lt, 2004.– [žiūrėta 2005 m. gruodžio 18 d.]. Prieiga per internetą: <http://www.apsauga.lt/?m1=item20040801234651>

18. Informacijos apsauga valstybės institucijų ir įstaigų darbuotojams, 2005.

19. Internet Law & Policy Forum. Survey of International Electronic and Digital Signature Initiatives [Žiūrėta 2007 01 20]. Prieiga per internetą// <http://www.ilpf.org/digsig/survey.htm>

20. . International telecommunication union [Žiūrėta 2007 01 20]. Prieiga per internetą <http://www.itu.int/aboutitu/ >

21. Informacijos visuomenės teisinio pamato raida Lietuvoje ir pasaulyje. [Žiūrėta 2007 01 20]. Prieiga per internetą <http://www.infovi.vu.lt/ivs/biblioteka/temos/teisinis.htm>

22. Information Society // European Commmission [žiūrėta 2007 01 20] Prieiga per Internetą: <http://www.europa.eu.int/scadplus/leg/en/s21012.htm>

23. Jarukaitis, I. Elektroninių ryšių teisė. – 2005. – p.333

24. Kardelis, K. Mokslinių tyrimų metodologija ir metodai: vadovėlis. – Kaunas:Judex, 2002. – 400 p.

25. „Komisijos ataskaita pavasario Europos Vadovų Tarybai. Lisabonos strategijos įgyvendinimas. Išsiplėtusios Sąjungos reformos“ KOM(2004) 29

26. Lietuvos informacijos visuomenės strategija: įdirbis ir perspektyvos II [Interaktyvus]. Vilniaus universiteto filosofijos fakultetas. Vilnius.– [žiūrėta 2005 m. gruodžio 18 d.]. Prieiga per internetą: <http://www.infovi.vu.lt/ivs/biblioteka/temos/infovistrat.htm>

27. Lietuvos Respublikos autorinių ir gretutinių teisių įstatymas// LRS, 1999 m. gegužės 18 d.

28. Lietuvos Respublikos civilinis kodeksas // Žin., 1964, Nr. 19-138.

29. Lietuvos Respublikos Ryšių reguliavimo tarnyba. Tinklų ir informacijos saugumo buklės Lietuvoje tyrimas. Įmonių ir IPT apklausa [Interaktyvus]. Vilnius, 2005– [žiūrėta 2005 m. sausio 20 d.]. Prieiga per internetą: <http://www.rrt.lt/index.php?174255322>

30. Lietuvos Respublikos Vyriausybė. Nutarimas dėl Lietuvos Informacinės visuomenės Pletros strategijos patvirtinimo. [Interaktyvus]. Vilnius, 2005 m [žiūrėta 2005 m. gruodžio 18 d.]. Prieiga per internetą: http://www.ivpk.lt/teises_aktai/files/102.pdf

31. OECD Measuring the Information Economy 2002“; „OECD Information Technology Outlook“, 2004 m.

32. Organisation for economic co-operation and development [žiūrėta 2007 01 20] Prieiga per Internetą: <http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html >

33. Pfleeger, Charles P., Shari Lawrence (2002) Security in Computing, Third Edition,

34. Rethinking the ICT-agenda. Price Waterhouse Coopers“, 2004 m. rugpjūtis

35. SANS Institute. The Twenty Most Critical Internet Security Vulnerabilities[Interaktyvus]. The Experts Consensus, 2005– [žiūrėta 2005 m. sausio 20 d.]. Prieiga per internetą: <http://www.sans.org/top20/>

36. Tinklų ir informacijos saugumo Lietuvoje tyrimas: Lietuvos įmonių ir interneto paslaugų tiekėjų apklausa. (2005).//RRT, Vilnius

37. The business and Industry Advisory Committee to the OECD [2007 01 20] Prieiga per Internetą< http://www.biac.org/>

38. The Lisbon Strategy for growth and jobs [žiūrėta 2007 01 20] Prieiga per Internetą: < http://ec.europa.eu/growthandjobs/index_en.htm > (2000)

39. The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus, (2005). // SANS Institute. [2007 01 20] Prieiga per Internetą: <http://www.sans.org/top20/ >

40. Vaitkus, Vygantas (2006) Interneto reglamentavimas Lietuvoje. //Teisės departamento Teisės taikymo skyriaus vedėjas Lietuvos Respublikos ryšių reguliavimo tarnyba

41. VRM Informacinės politikos departamentas. Informacinių technologijų sauga. [Interaktyvus]. Vilnius, 2003– [žiūrėta 2005 m. sausio 5 d.]. Prieiga per internetą: <http://www2.vrm.lt/nuorodos/ipd/ipd-saugospatarimai.htm>

PRIEDAI

1 Priedas Dvidešimt pavojingiausių Interneto saugumo pažeidimų.

2. Priedas. Klausimai, kurie buvo užduoti interviu metu.

THE IMPACT OF EU ON THE LITHUANIAN INFORMATION SECURITY POLICY

SUMMARY

Majority of social relations is moving to the virtual space. People are using electronic communications more actively not only for finding important information on the web, but also for ordering and purchasing goods, paying for services and transferring money, watching TV and etc. Development in electronic devices and data transfer technologies allows connectivity to services anywhere anytime. Government institutions, service providers are searching for more ways to provide their services for citizens via the Internet.

Information society development is highly related to network and information security. This paper addresses Lithuanian information security policies before EU enlargement and after it. The main goal is to evaluate the impact of EU on the Lithuanian information and network security, safer internet, information technology and development.

The paper also proposes qualitative research on Lithuanian information security issues and EU impact of new policies. Governmental and business companies that participated in the research do not relate EU enlargement with IT security progress in Lithuania. They emphasized some factors, that have impact on information and network security. It is IT development, economy, legislation, user friendly information society. Information and network security is also influenced by better financing after the EU enlargement, international cooperation, best practice examples and others.

1 Priedas Dvidešimt pavojingiausių Interneto saugumo pažeidimų.

Windows spragų sąrašas

• W1 Žiniatinklio serveriai ir paslaugos

• W2 Darbo stoties paslauga

• W3 Windows nuotolinio priėjimo paslaugos

• W4 Microsoft SQL serveris (MSSQL)

• W5 Windows autentifikacija

• W6 Žiniatinklio naršyklės

• W7 Windows lygiavertis dalijimasis failais (P2P)

• W8 LSASS

• W9 Pašto klientas

W10 Tiesioginis bendravimas Internetu

UNIX spragų sąrašas

• U1 BIND Vardų sričių sistema

• U2 Žiniatinklio serveris

• U3 Autentifikacija

• U4 Versijų valdymo sistemos

• U5 Pašto perdavimo paslauga

• U6 Simple Network Management Protocol (SNMP)

• U7 Open Secure Sockets Layer (SSL)

• U8 NIS ir NFS paslaugų konfigūracijos spragos

• U9 Duomenų bazės

• U10 Branduolys

2. Priedas. Klausimai, kurie buvo užduoti interviu metu.

1. Ar jūsų organizacija turi skyrių, kuris atsakytų už informacijos ir tinklų saugumą? Kada jis buvo įkurtas?
2. Su kokiais kompiuteriniais nusikaltimais dažniausiai susiduriate? Ar jų sąrašas prasiplėtė po įstojimo į ES ar sumažėjo?
3. Kaip apsisaugote nuo kompiuterinių virusų ir kaip apsaugote kitus?
4. Kokias informacijos ir kompiuterio apsaugos priemones naudojate? Kokios jūsų nuomone efektyviausios?
5. Ar įmanoma surasti Lietuvos ir užsienio kompiuterinius nusikaltėlius? Ar bendradarbiaujate gaudant nusikaltėlius? Ar Lietuvos kompiuteriniai nusikaltėliai tokie pat pažangūs kaip ir užsienio?
6. Kaip apsaugote duomenų srautus einančius per jūsų įstaigą?
7. Palyginus su 2003-2004 metais nusikaltimų el. erdvėje skaičius auga?
8. Kaip informuojate kitus apie kompiuterinius nusikaltėlius, būtinybę apsaugoti kompiuterinius tinklus ir elektroninį ryšį?
9. Kokios privačios ir valstybinės institucijos dalyvauja informuojant visuomenę apie informacijos ir tinklų saugumą Lietuvoje? Su kokiomis bendradarbiaujat?
10. Ar iki įstojimo į ES buvo kokių nors kompiuterinių nusikaltimų prevencijos priemonių? (Informavimo, praktinių ir kt.)
11. Ar jus savo darbe atsižvelgiate į ES reikalavimus, rekomendacijas, direktyvas? Ar atsižvelgiate į Lietuvos teisės aktus?
12. Su kokiomis ES šalimis bendradarbiaujate (dalinatės patirtimi) informacijos ir kompiuterių saugumo klausimais?
13. Kas įtakojo naujų priemonių rengimą, Lietuvos informacijos saugumo politikos vystymąsi? Ar įstojimas į ES buvo lūžis formuojant saugesnė e-terpę Lietuvoje?
14. Kokias galimybes Lietuvos informacijos saugumo politikai atvėrė stojimas į ES?
15. Ar dalyvaujate ES programose, projektuose informacijos saugumo srityje?
16. Kaip jus manote, ar Lietuvos informacijos vartotojai jaučiasi saugesni po įstojimo į ES?