Vilniaus universitetas
Komunikacijos fakultetas

Indrė Selskaitė,
Informacijos vadybos studijų programos studentė

INFORMACIJOS SAUGA VIEŠĄJAME IR PRIVAČIAME SEKTORIUJE

MAGISTRO DARBAS

Vadovas doc. dr. P. Abarius

Vilnius, 2008

Indrės Selskaitės magistro baigiamasis darbas

„Informacijos sauga viešąjame ir privačiame sektoriuje“

„Information security in public and private sector“

Patvirtinu, kad magistro baigiamasis darbas parašytas savarankiškai, nepažeidžiant kitiems asmenims priklausančių autorių teisių, visas baigiamasis magistro darbas ar jo dalis nebuvo panaudoti kitose aukštosiose mokyklose.

_____

(magistro baigiamojo darbo autoriaus parašas)

Sutinku, kad magistro baigiamasis darbas būtų naudojamas neatlygintinai 5 metus Vilniaus universiteto Komunikacijos fakulteto studijų procese.

_____

(magistro baigiamojo darbo autoriaus parašas)

Magistro baigiamąjį darbą ginti _____

_____ _____

(data) (magistro baigiamojo darbo vadovo parašas)

Magistro baigiamasis darbas įregistruotas

Informacijos ir komunikacijos katedroje

_____ _____

(data) (katedros reikalų tvarkytojos parašas)

Recenzentu skiriu _____

_____ _____

(data) (katedros vadovo parašas)

Darbą recenzuoti gavau _____ _____

(data) (recenzento parašas)

Referato lapas

Selskaitė, Indrė
Sel52

Informacijos sauga viešajame ir privačiame sektoriuje: magistro darbas/ Selskaitė Indrė; mokslinis vadovas doc. dr. Povilas Abarius; Vilniaus universitetas.

Komunikacijos fakultetas. Informacijos ir komunikacijos katedra. – Vilnius, 2008. – 74 [1] lap.: lent. – Mašinr. – Santr. angl. – Bibliogr.: p. 68 – 70 (31 pavad.).
UDK 659.2.621.377

Raktiniai žodžiai: *informacija, informacinis turtas, informacijos sauga, informacijos saugumo incidentai, viešasis sektorius, privatus sektorius, reglamentavimas.*

Magistro *darbo objektas* – informacija ir informacinis turtas. *Darbo tikslas* – išanalizuoti informacijos saugos problemą viešajame ir privačiame sektoriuje ir palyginti informacijos apsaugos lygį viešosiose ir privačiose organizacijose. *Darbo uždaviniai*: atskleisti informacijos ir informacinio turto organizacijose apsaugos būtinybę; apžvelgti pagrindines kiekviename sektoriuje kylančias informacijos saugumo problemas, grėsmes, pažeidžiamumus; išnagrinėti, kokiomis priemonėmis saugoma informacija viešojo ir privataus sektoriaus organizacijose; nustatyti priežastis, dėl kurių laikomasi arba nesilaikoma informacijos saugumo politikų ir taisyklių organizacijose; ištirti, ar informacijos saugumo srities reglamentavimas teisės aktuose įtakoja praktinę informacijos apsaugą organizacijose.

Naudojantis mokslinės literatūros analizės metodais, atlikus kiekybinį viešojo ir privataus sektorių organizacijų tyrimą, prieita prie išvados, kad informacinis turtas šiuolaikinėje organizacijoje, tiek viešoje, tiek privačioje verslo, yra brangesnis net už materialųjį turtą, todėl jo apsauga yra neginčytina būtinybė. Taip pat buvo nustatyta, kad nepaisant daugelio institucijų darbo šioje srityje, informacijos apsaugos problema yra ypač opi ir aktuali, nes nė vienas rinkos dalyvis – nei valstybės institucija, nei pelno siekianti verslo organizacija – nėra apsaugotas nuo sunkių nuolat vykstančių informacijos saugumo incidentų pasekmių. Atliekant kiekybinį tyrimą valstybės institucijose ir interneto bei elektroninės prekybos organizacijose prieita prie išvados, kad nepaisant daugelio priemonių, tikslingai naudojamų tinkamam informacijos saugumo lygiui užtikrinti, organizacijos patiria žalą dėl nuolat kylančių informacijos saugos incidentų. Apibendrinant atliktą kiekybinį tyrimą galima teigti, kad dėl stipresnio informacijos saugumo viešajame sektoriuje

reglamentavimo, valstybės institucijose naudojama informacija yra apsaugota tikslingiau, daugiau ir geriau, čia patiriama mažiau informacijos saugumo incidentų, plačiau vykdoma informacijos saugos politika, beveik kiekvienoje organizacijoje valdomi informacijos saugumo incidentai.

Magistro darbas gali būti naudingas viešojo sektoriaus dalyviams, verslo organizacijoms, informacijos disciplinų dėstytojams ir studentams, bei kiekvienam, kuriam rūpi informacijos sauga.

TURINYS

ĮVADAS.....7
1. INFORMACIJOS SAUGOS VIEŠĄJAME IR PRIVAČIAME SEKTORIUJE PROBLEMA....9
1.1. Informacija ir informacinis turtas.....9
1.2. Kodėl reikia saugoti informaciją?.....10
1.3. Informacijos saugumas – konfidencialumo, vientisumo, prieinamumo užtikrinimas.....11
1.4. Informacijos saugumo brandos lygiai.....13
1.5. Informacijos saugumo tikslai.....14
2. INFORMACIJOS SAUGOS TEORINIS ASPEKTAS.....16
2.1. Informacija ir informacijos saugumo problema viešąjame sektoriuje.....16
2.1.1. Informacijos saugos problemų priežastys viešąjame sektoriuje. Informacijos saugumo incidentai.....17
2.1.2. Viešojo sektoriaus informacinio turto grėsmės, pažeidžiamumai ir rizikos.....18
2.1.3. Informacijos saugos įgaliotinis. Informacijos saugos tikslai viešąjame sektoriuje.....20
2.1.4. Informacijos saugumą viešąjame sektoriuje reglamentuojantys dokumentai.....21
2.2. Informacija ir informacijos saugumo problema privačiame sektoriuje.....24
2.2.1. Informacija privačiame sektoriuje.....24
2.2.2. Komercinės paslaptys. Verslo informacijos grėsmės ir pažeidžiamumai.....26
2.2.3. Informacijos sauga elektroniniame versle ir elektroninėje prekyboje.....27
2.2.4. Verslo informacijos apsaugos priemonės.....28
2.2.5. Informacijos saugumą privačiame sektoriuje reglamentuojantys dokumentai. Konfidencialumo sutartys.....29
2.3. Informacijos saugos patarimai ir standartai.....32
3. INFORMACIJOS SAUGOS VIEŠĄJAME IR PRIVAČIAME SEKTORIUJE TYRIMAS.....39
3.1. Tyrimo metodologija.....39
3.2. Tyrimo rezultatai.....42
3.3. Tyrimo išvados.....61
IŠVADOS.....65
Bibliografinių nuorodų sąrašas.....68
1 priedas. Kiekybinio tyrimo anketos pavyzdys.....71
Information security in public and private sector (summary).....73

PAVEIKSLŲ SĄRAŠAS

1 pav. Informacijos saugumas – konfidencialumo, vientisumo ir prieinamumo užtikrinimas.....11

LENTELIŲ SĄRAŠAS

1 lentelė. Elektroninės apklausos atsakymų grąža.....43
2 lentelė. Organizacijų skaičius, kuriose nėra vykdoma informacijos saugumo politika.....54
3 lentelė. Priežastys, dėl kurių būtina saugoti informaciją, kurias nurodė viešojo ir privataus sektoriaus organizacijos.....59
4 lentelė. Identifikuotų informacijos saugos problemų sprendimo būdai viešąjame sektoriuje.....61
5 lentelė. Identifikuotų informacijos saugos problemų sprendimo būdai privačiame sektoriuje.....62

DIAGRAMŲ SĄRAŠAS

1 diagrama. Tyrime dalyvavusių interneto ir elektroninės prekybos bendrovių darbuotojų skaičius.....44
2 diagrama. Tyrime dalyvavusių valstybės institucijų darbuotojų skaičius.....45
3 diagrama. Valstybės institucijų, susiduriančių su informacijos saugumo incidentais, skaičius.....47
4 diagrama. Interneto ir elektroninės prekybos bendrovių, susiduriančių su informacijos saugumo incidentais, skaičius.....47
5 diagrama. Viešąjame sektoriuje naudojamos informacijos apsaugos priemonės.....49
6 diagrama. Privačiame sektoriuje naudojamos informacijos apsaugos priemonės.....49
7 diagrama. Žala, kurią dėl saugumo incidentų patyrė valstybės institucijos.....52
8 diagrama. Žala, kurią dėl saugumo incidentų patyrė interneto ir elektroninės prekybos bendrovės.....52
9 diagrama. Informacijos saugumo incidentų valdymas viešojo sektoriaus organizacijose.....55
10 diagrama. Informacijos saugumo incidentų valdymas privataus sektoriaus organizacijose.....55
11 diagrama. Prieigos prie tam tikros informacijos valdymas valstybės institucijose.....57
12 diagrama. Prieigos prie tam tikros informacijos valdymas interneto ir elektroninės prekybos bendrovėse.....57

ĮVADAS

Informacinė veikla išsivysčiusiose šalyse užima vieną svarbiausių tiek ekonomikos, tiek ir kitų gyvenimo sferų vietų. Spartus naujausiųjų technologijų įsiveržimas į šiuolaikinės visuomenės gyvenimą, be naujų galimybių, sukėlė ir daugybę problemų, visų pirma informacijos saugumo.

Daugeliui sąvoka „informacijos saugumas“ asocijuojasi su duomenų saugumu. Tačiau apsaugoti įmonės ar įstaigos informaciją reiškia daug daugiau negu tik apsaugoti duomenis. Informacijos saugumas – tai informacijos, nesvarbu elektroninės ar kitame pavidale egzistuojančios, apsauga. Informacijos saugumo tikslas – visos įmonėje egzistuojančios informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

Su informacijos saugumo problemomis susiduria daugelis – tiek dirbantieji viešąjame, tiek privačiame sektoriuje, tiek įmonių vadovai, tiek eiliniai darbuotojai. Priklausomai nuo įstaigos ar organizacijos veiklos, jos tikslų ir kitų dalykų, susiduriama su skirtingomis informacijos saugumo problemomis, dėl įvairių priežasčių tos problemos kyla, skirtingais būdais jos ir sprendžiamos. Viešąjame sektoriuje, skirtingai negu privačiąjame, informacijos sauga – įstatymais ir kitais teisiniais aktais stipriai reglamentuota sritis, todėl valstybės institucijose ar kitose viešosiose organizacijose dirbantieji yra įpareigoti saugoti informacinį turtą. Privataus sektoriaus atstovai informacijos sauga rūpinasi dėl kitų priežasčių – pirmiausia dėl to, kad konfidenciali ir saugi įmonės informacija, komercinės paslaptys užtikrina geras pozicijas konkurencinėje kovoje, o apsisaugojimas nuo informacijos incidentų padeda išvengti finansinių nuostolių ar dar sunkesnių padarinių – įmonių bankrotų.

Darbe „Informacijos sauga viešąjame ir privačiame sektoriuje“ siekiama pažvelgti į informacijos saugumo problemą šiuolaikinėje visuomenėje, ypatingą dėmesį atkreipiant į viešąjį ir privatųjį sektorius, aptarti pagrindines kylančias informacijos saugos grėsmes bei jų priežastis, apžvelgti informacijos saugumą reglamentuojančius teisės aktus bei už informacijos saugumą atsakingas institucijas.

Darbo temos pasirinkimą motyvavo temos aktualumas ir naujumas. Informacija šiandieniniame konkurencingame verslo pasaulyje bei kiekvienos šalies valdymo institucijose yra prilyginama, o kartais ir labiau vertinama nei materialusis jos turtas. Kompiuterinių nusikaltimų, duomenų vagysčių, virusų, kasdien į elektroninio pašto dėžutes plūstančių nepageidaujamų laiškų skaičius nuolat auga. Kai kurie informacijos saugumo incidentai gali praeiti be sunkesnių pasekmių, tačiau daugelis jų daugiau ar mažiau sutrikdo organizacijos veiklą, gali atnešti materialinių nuostolių, pakenkti organizacijos įvaizdžiui ar netgi tapti organizacijos žlugimo priežastimi.

Informacijos saugumo problemos aktyviau pradėtos spręsti tik pastarąjį dešimtmetį, kai didelė dalis organizacijoje naudojamos informacijos buvo perkelta į elektroninę erdvę ir tapo prieinama didesniam skaičiui žmonių nei tuomet, kai buvo saugoma tik popierinėje laikmenoje. Taigi, nuolat augantis informacijos incidentų skaičius, didėjantis svarbios informacijos kiekis, informacinio turto svarba organizacijos gyvavime verčia susirūpinti informacinio saugumo problema. Rašant darbą taip pat iškilo klausimas: ar tai, kad informacijos saugumo sritis viešajame sektoriuje labiau reglamentuota negu privačiajame, įtakoja informacijos saugos lygį šių dviejų sektorių organizacijose? Į šį klausimą bus pamėginta atsakyti praktinėje darbo dalyje.

Mokslinis naujumas – į informacijos saugumo problemą pamėginta pažvelgti iš dviejų skirtingų sektorių – viešojo ir privataus – pusių bei kiekybinio tyrimo metodu ištirti problemą minėtuose sektoriuose.

Magistro **darbo objektas** – informacinis turtas ir jo saugumas viešojo ir privataus sektoriaus organizacijose. **Darbo tikslas** – nustatyti, ar sprendžiama ir kaip sprendžiama informacijos saugumo problema viešajame ir privačiame sektoriuje. Pagrindiniai **darbo uždaviniai** - palyginti, su kokiomis pagrindinėmis informacijos saugumo problemomis susiduria dirbantieji minėtuose sektoriuose; kokios informacijos apsaugos priemonės ir politikos taikomos viešosiose ir privačiose organizacijose naudojamos informacijos apsaugai; nustatyti, ar skirtingas informacijos saugumo srities reglamentavimas teisės aktuose įtakoja informacijos apsaugos lygį privačiose ir viešosiose organizacijose, ištirti, ar įmonės turi informacijos saugos politikas ir taisykles, nustatyti, dėl kokių pagrindinių priežasčių nėra užtikrinamas pakankamas informacijos saugos lygis organizacijose. Darbo metu buvo iškelta **hipotezė**, kad informacijos saugumo problema egzistuoja tiek privačiame, tiek viešajame sektoriuje ir ši problema sektoriuose sprendžiama pasitelkiant skirtingas technines, organizacines ir teisines priemones.

Siekiant realizuoti iškeltus tikslus, pirmojoje darbo dalyje bus nagrinėjamos pagrindinės informacijos saugos sąvokos ir apibrėžimai, antrojoje dalyje remiantis literatūros analizės metodu bus analizuojama informacijos saugumo problematika viešajame ir privačiame sektoriuje, o paskutinėje, trečiojoje, dalyje, pasitelkus kiekybinio tyrimo metodą, bus atliktas dviejų sektorių tyrimas, kurio tikslas - išsiaiškinti pagrindines tiek viešajame, tiek privačiame sektoriuje kylančias problemas, nustatyti informacijos apsaugos lygį ir naudojamas informacijos saugumo priemones bei politikas tiek viename, tiek kitame sektoriuje, bendras šios srities tendencijas. Darbo pabaigoje bus pateiktas naudotų literatūros šaltinių sąrašas bei priedai, taip pat santrauka anglų kalba.

Šis magistro **darbas gali būti naudingas** informacijos saugumo specialistams, įstaigoms, kurios yra atsakingos už informacijos saugą bei kiekvienam, dirbančiajam tiek privačioje bendrovėje, tiek viešojo sektoriaus įmonėje.

1. INFORMACIJOS SAUGOS VIEŠĄJAME IR PRIVAČIAME SEKTORIUJE PROBLEMA

Informacinė era atnešė daug pokyčių įvairių profesijų atstovams, dirbantiems tiek privačiame, tiek viešąjame sektoriuje. Šiandien kiekvienas valstybės tarnautojas ar įmonės darbuotojas disponuoja tokiu dideliu kiekiu tikslios ir operatyvios informacijos, kokiu niekada anksčiau nedisponavo.

Šiame skyriuje remiantis straipsniais, publikacijomis bei internetiniais šaltiniais bus aprašytos pagrindinės informacijos saugos sąvokos, aptarta, kodėl informaciją ir informacinį turtą būtina saugoti, kas yra informacijos saugumo užtikrinimas ir informacijos saugos tikslai.

1.1. Informacija ir informacinis organizacijos turtas

Prieš pradedant analizuoti informacijos saugumo problemą viešąjame ir privačiame sektoriuose, reikėtų pasiaiškinti, kas yra informacija ir informacinis organizacijos turtas.

Yra keletas informacijos apibrėžimų. Informaciją būtų galima apibrėžti kaip įvairias žinias, perduodamas žodžiu, raštu ar žiniasklaidos priemonėmis. Informacija – tai mokslinės, visuomeninės ar techninės žinios, perduodamos vienų asmenų kitiems įvairių priemonių pagalba (žiniasklaidos priemonėmis, rašto, kalbos pagalba ir pan.). Vartotojo atžvilgiu šios žinios turi būti suprantamos, priimtinos bei naudingos.

Ne visa mus supanti informacija yra kiekvienam vienodai naudinga. Ji turi vertę tada, kai yra tiksli, išsami ir tinkama sprendimų priėmimui.

Privačios įmonės ar viešosios įstaigos informacinį turtą gali sudaryti [4]:

- **Informacija**: tai duomenų bazės, sutartys, sisteminė dokumentacija, vartotojo vadovai, mokymo medžiaga, veiklos tęstinumo planai, auditų medžiaga ir kt.
- **Programinė įranga**: tai taikomoji programinė įranga, sistemos programinė įranga, programavimo priemonės.
- **Fizinė įranga**: tai kompiuterinė įranga, nešiojamosios bei saugojimo laikmenos, kita informacijos perdavimo ar saugojimo įranga.
- **Paslaugos**: tai skaičiavimo, ryšių paslaugos ir bendrosios aprūpinimo paslaugos (šildymas, apšvietimas, elektros tiekimas).
- **Žmonės**: tai įmonėje dirbančiųjų kvalifikacija, žinios ir patirtis.
- **Nematerialios vertybės**: tai organizacijos įvaizdis, reputacija.

Kalbant apie informaciją jos saugumo aspektu reiktų aptarti ir informacines sistemas, be kurių neįsivaizduojamas nė vienos šiuolaikinės organizacijos darbas. Informacinė sistema pateikia prasmingą informaciją žmogui ir organizacijoms. Informacinė sistema apibūdinama kaip kartu veikianti programinės įrangos, fizinės įrangos, žmonių, procedūrų ir duomenų visuma. Informacinės sistemos priima, saugo ir apdoroja duomenis.

Informaciją pagal jos reikšmingumą, naudingumą ir aktualumą, taip pat pagal jos pasiekiamumo, vientisumo ir konfidencialumo kriterijus galima klasifikuoti. Šis klasifikavimas yra labai svarbus siekiant užtikrinti tinkamą informacinio turto apsaugos lygį.

1.2. Kodėl reikia saugoti informaciją?

Žvelgiant į informacijos saugumo problemos istoriografiją aišku, kad ši problema buvo aktuali ir seniau, ji egzistavo ir „senose“ telekomunikacinėse sistemose – telegrafo, telefono, radijo ryšio. Tačiau plintant elektroniniams ryšiams ir perkeliant didžiąją dalį informacijos į kompiuterių tinklus ji įgavo visai kitą mastą.

Kalbant apie vieną iš labiausiai plintančių ir efektyviausių ryšio ir bendravimo priemonių – internetą, svarbu suprasti: susijungus į pasaulinį tinklą milijonams kompiuterių, atsiranda ir nuolat didėja pavojus, kad kompiuterinėje įrangoje saugomi asmeniniai duomenys, svarbi įmonės informacija, elektroninio pašto korespondencija gali būti stebima, pakeista ar perimama pašalinių asmenų. Informacijos ir ryšių technologijos - šiuolaikinės visuomenės ir ekonomikos pagrindas, todėl tinklų ir informacijos saugumas tampa vis svarbesnis.

Informacija – tai turtas, kuris kaip ir kitas svarbus veiklos turtas yra būtinas organizacijos veiklai. Todėl jis turi būti tinkamai apsaugotas. Tai ypač svarbu stiprėjant tarpusavio ryšiams, dėl kurių informacija tampa vis labiau ir įvairiau pažeidžiama, jai iškyla vis daugiau ir įvairesnių grėsmių.

Informacijos saugumą užtikrinti nėra lengva. Jis pasiekiamas taikant deramą valdymo priemonių, tokių kaip politikos, procesai, procedūros, organizacinės struktūros bei programinės ir techninės įrangos funkcijos, rinkinį [18]. Šios valdymo priemonės turi būti ne tik įdiegiamos ir pritaikomos, bet ir nuolat prižiūrimos, peržiūrimos ir, jei yra būtinybė, gerinamos, kad būtų įgyvendinti ypatingi organizacijos saugumo bei veiklos tikslai.

Kodėl būtina saugoti organizacijos informacinį turtą? Informacijos saugumo pasiekimas, priežiūra bei nuolatinis gerinimas yra labai svarbūs siekiant išlaikyti konkurencinį pranašumą, grynųjų pinigų cirkuliaciją, pelningumą, teisinę atitiktį ir organizacijos įvaizdį. Neužtikrinus aukšto informacinio turto apsaugos lygio organizacijoje rizikuojama daugeliu dalykų – reputacija,

įvaizdžiu, konkurencingumu, santykiais su verslo partneriais ir kt. [2]. Taigi, pastaraisiais metais informacijos apsauga susirūpinta ne tik siekiant užtikrinti duomenų ir informacinio turto saugumą, bet ir dėl tiesioginių ar netiesioginių rinkos reikalavimų.

Informacijos saugumas svarbus tiek viešojo, tiek privataus sektorių veiklai apsaugant svarbias infrastruktūras. Abiejuose sektoriuose informacijos saugumas laikui bėgant turės funkcionuoti kaip priemonė, leidžianti įgyvendinti elektroninę vyriausybę ar elektroninę prekybą, išvengti ar sumažinti aktualią riziką.

Informacinės visuomenės plėtra ir informacijos saugumo didinimas reikalauja reikšmingų koordinuotų ir nepavėluotų pastangų tiek privačiame, tiek viešajame sektoriuose. Lietuvoje informacijos saugumo veikla pagrinde yra susitelkus į šias sritis [23]:

- vartotojų ugdymą ir sąmoningumo informacijos saugumo atžvilgiu didinimą;
- neigiamo informacijos saugumo pažeidimų poveikio mažinimą;
- saugumo pažeidimų valdymą;
- teisinių ir standartizavimo priemonių kūrimo skatinimą.

1.3. Informacijos saugumas – konfidencialumo, vientisumo ir prieinamumo užtikrinimas

Informacijos apsauga nėra tik informacijos ar duomenų konfidencialumo užtikrinimas. Be konfidencialumo turi būti užtikrinamas ir informacijos prieinamumas bei vientisumas.

1 paveikslas. Informacijos saugumas – konfidencialumo, vientisumo ir prieinamumo užtikrinimas [4]

Konfidenciali informacija – tai tokia informacija, kuri gali būti atskleista tik tam teisę turintiems asmenims. Duomenų vagystė ar komercinės paslapties atskleidimas yra traktuojami kaip informacijos konfidencialumo pažeidimai. Informacijos konfidencialumui gali kilti šios grėsmės

[14]: neleistinas prisijungimas, neleistinas atskleidimas, sandorių sekimas arba stebėsena, kopijavimas, neturint tam leidimo.

Vientisa infomacija – tai tiksli ir išbaigta informacija. Netiksliai duomenų sistemoje įvesti duomenys ar klaidos – tai informacijos vientisumo pažeidimai.

Informacijos prieinamumas – tai užtikrinimas, kad informacija visada bus prieinama teisėtiems jos vartotojams. Kompiuterinės įrangos gedimas – vienas iš informacijos prieinamumo pažeidimų.

Taigi, saugi informacija – tai ne tik nepavogta įmonės ar įstaigos informacija, bet taip pat ir nepakitusi ir laiku prieinama informacija [20].

Viena pagrindinių įvykstančių informacijos incidentų priežastis – nepakankamas švietimas informacijos saugumo srityje. Net ir minimalios informacinio saugumo žinios galėtų padėti išvengti daugelio klaidų ir incidentų, užbėgti už akių nusikaltimams. Vartotojų švietimas informacijos saugumo klausimais užtikrina keturis kompiuterinių ir informacijos resursų apsaugos lygius:

- išvengimą – prieigą prie informacijos turi turėti tik autorizuoti vartotojai;
- aptikimą – turi būti užtikrinamas ankstyvas sukčiavimų ir nusikaltimų aptikimas;
- apribojimą – jei nusikaltimas, nepaisant taikomų išvengimo ir aptikimo priemonių, vis dėlto įvyko, sumažinamas padarytos žalos dydis;
- atkūrimą – turi būti užtikrintas efektyvus informacijos atkūrimas pasitelkiant patikrintus atkūrimo planus.

Svarbi problema, susijusi su informacijos apdorojimu kompiuterių pagalba, yra didelis tokios informacijos pažeidžiamumas bei grėsmės tokios informacijos saugumui. Įvairiuose šaltiniuose (teisiniuose aktuose, informacijos saugumo standartuose ir kt.) pabrėžiami trys pagrindiniai informacijos apsaugą reglamentuojantys lygiai:

- organizacinis – techninis saugumas (tai yra techninių priemonių organizavimas, siekiant apsaugoti kompiuteriniuose tinkluose saugomą informaciją. Šiam lygiui priskiriamos ir tokios priemonės kaip informacijos saugumo politikos nuostatos, ugniasienių diegimas, antivirusinių programų diegimas, varotojų teisių sistema);
- fizinis saugumas (tai metodai, skirti apsaugoti kompiuterinę ir programinę įrangą nuo nelaukiamo fizinio pašalinių jėgų poveikio. Šiam lygiui priskiriamos tokios priemonės kaip nepertraukiamo maitinimo šaltiniai, signalizacijų sistemos, fizinis apsaugos darbuotojų budėjimas);
- teisinis reglamentavimas (norminių dokumentų paketo įvedimas įmonėje. Šie dokumentai turėtų reglamentuoti įmonės darbuotojų elgesį su svarbiais dokumentais bei duomenimis, įmonės komercinėmis paslaptimis).

1.4. Informacijos saugumo brandos lygiai

Įmonių ir įstaigų informacijos apsauga skirstoma į tam tikrus brandos lygius. Pagrindiniai iš jų yra šie [20]:

- Lygis 0 – informacijos apsaugos organizacijoje nėra;
- Lygis 1 – informacijos apsauga organizacijuoja traktuojama kaip „techninė problema“;
- Lygis 2 – informacijos apsauga - tai organizacinių ir techninių priemonių kompleksas;
- Lygis 3 – informacijos apsauga yra organizacijos kultūros dalis.

Lietuvoje dažniausiai sutinkamas 0 ir 1 informacijos apsaugos brandos lygiai.

Organizacijos, kurių informacijos apsaugos brandos lygis yra nulinis, krizių atveju patiria labai didelius nuostolius, o jei yra labiau priklausomos nuo informacinių sistemų ir informacinių technologijų – net ir bankrutuoja [20].

Pirmas informacijos apsaugos brandos lygis pasireiškia tose organizacijose, kuriose informacijos apsauga patikėta tik informacinių technologijų skyriaus darbuotojams ir į tai jokio dėmesio nekreipia organizacijos vadovai. Dažnai informacijos saugumui užtikrinti pasitelkiamos tik antivirusinės programos ar ugniasienės. Toks informacijos apsaugos suvokimas yra vienas labiausiai paplitusių ir Lietuvoje. Krizių atveju įmonei gali labai pakenkti bet kokia ne techninė problema.

Antrame informacijos apsaugos brandos lygyje atsiranda organizacijos informacijos saugumo politika, taisyklės, nuostatos. Pasitelkiamos organizacinės apsaugos priemonės, kurios už technines dažnai būna pigesnės ir žymiai efektyvesnės. Šiame lygmenyje dalyvauja ir įmonės vadovai, pasirūpinantys tam tikromis procedūromis, atsarginiais planais. Su krizėmis organizacija susidoroja be didesnio streso, po iškilusių incidentų greitai atstatoma įmonės veikla, patiriami minimalūs nuostoliai. Nors tai yra ne aukščiausias informacijos apsaugos brandos lygis, jį Lietuvoje yra pasiekusi tik nedidelė dalis organizacijų.

Kalbant apie aukščiausią – trečiąjį informacijos apsaugos lygį – svarbus pabrėžti, kad jame informacijos apsauga yra organizacijos kultūros dalis. Tokių organizacijų darbuotojai moka puikiai atpažinti informacijos incidentus ir apie juos pranešti atsakingiems asmenims, o vadovybė imasi priemonių, kad tokie incidentai nesikartotų. Tokiose organizacijose krizių nebūna arba jos labai greitai ir be sunkesnių padarinių pašalinamos. Šiuo metu Lietuvoje nėra nei vienos organizacijos, pasiekusios trečią apsaugos lygį [20].

Kalbant apie organizacijos informacijos saugumo lygį, svarbu atsižvelgti į saugumo pakankamumo principą, kuris teigia: saugumas turi būti toks, kad jį pralaužti kainuotų brangiau, nei pati informacija, arba kad pralaužimo laikas viršytų informacijos aktualumo laiką.

1.5. Informacijos saugumo tikslai

Taigi, norint sumažinti kompiuterinių nusikaltimų skaičių ir užtikrinti kuo geresnį informacijos saugumą, būtina imtis saugumo priemonių. Pagrindiniai literatūroje apžvelgiami informacijos saugumo tikslai – apsaugoti informaciją užtikrinant jos tikslumą ir vientisumą, sumažinant nuostolius, kuriuos gali sukelti informacijos pasisavinimas, pakeitimas ar sunaikinimas. Informacijos saugumo priemonės turi užtikrinti kritiškai svarbios informacijos konfidencialumą, informacijos ir jos procesų vientisumą, prieigą prie informacijos, kai jos reikia.

Trumpai apžvelgus egzistuojančią ir vis didėjančią informacijos saugos problemą bei atsižvelgiant į visa apimantį informacijos ir ryšių technologijų ir informacinių sistemų paplitimą, aišku, kad tinklų ir informacijos saugumas pateikia iššūkių visiems [5]:

- viešojo valdymo institucijos turi atkreipti dėmesį į naudojamų sistemų saugumą, siekdamos ne tik užtikrinti viešojo sektoriaus informacijos saugumą, bet ir kad parodytų pavyzdį kitiems rinkos dalyviams;
- įmonės ir organizacijos turi žiūrėti į tinklų ir informacijos saugumą kaip į turtą ir privalumą konkurencijos sąlygomis;
- atskiri vartotojai turi suvokti, kad jų namų sistemos yra svarbi bendros saugumo sistemos dalis.

Informacijos turto saugumu turėtų būti susirūpinta ne tik valstybės, bet taip pat ir visos Europos lygmeniu. 2005 metų birželio 1 dieną Europos Bendrijų Komisija komunikate „i2010 – Europos informacinė visuomenė augimui ir užimtumui skatinti“ kaip vieną pagrindinių uždavinių kuriant bendrą Europos informacinę sistemą išskyrė saugumą, t.y. saugesnio nuo piktavalių, žalingo turinio ir gedimų interneto kūrimą, skatinant pasitikėjimo augimą. Patikima ir saugi informacija bei ryšių technologijos reikalingos platesniam elektroninių paslaugų prieinamumui. Nors Europos Sąjunga valstybėms narėms nėra nustačiusi specifinių informacijos saugumo reikalavimų, visgi informacijos apsaugojimas šiandien Europoje priskiriamas prie prioritetinių dalykų.

Taigi, apžvelgus informacinio organizacijos turto svarbą, aptarus pagrindines informacinio turto grėsmes ir pažeidžiamumus, stebint vis didėjantį informacinių incidentų skaičių, augantį elektroninių paslaugų poreikį tampa aišku, kad informaciją būtina saugoti. Jos apsauga – nuolatinis

procesas, pateikiantis iššūkių visiems – tiek paprastiems informacijos vartotojams namuose, tiek viešojo sektoriaus institucijoms, tiek privataus verslo atstovams.

Lietuvoje yra keletas už informacijos apsaugą atsakingų institucijų. Vienos iš jų yra atsakingos už informacijos apsaugą tik viešąjame sektoriuje, kitų veikla apima informacijos apsaugą tiek viešąjame, tik privačiame sektoriuje. Dėl skirtingo informacijos pobūdžio skiriasi ir šių institucijų funkcijos ir atsakomybė.

Išskiriamos šešios pagrindinės institucijos, veikiančios informacijos saugumo srityje: Informacinės plėtros komitetas (IVPK), Valstybinė duomenų apsaugos inspekcija (VDAI), Ryšių reguliavimo tarnyba (RRT), Vidaus reikalų ministerija (VRM), Nusikaltimų elektroninėje erdvėje tyrimų skyrius (NEETS) ir Valstybės saugumo departamentas (VSD).

Informacinės visuomenės plėtros komitetas (IVPK) prie Lietuvos Respublikos Vyriausybės dalyvauja formuojant valstybės informacijos technologijų ir telekomunikacijų kūrimo politiką ir koordinuoja jos įgyvendinimą.

Valstybinės duomenų apsaugos inspekcijos (VDAI) uždavinys yra asmens duomenų apsaugos užtikrinimas.

Ryšių reguliavimo tarnyba (RRT) siekia, kad būtų užtikrintas elektroniniais ryšiais teikiamų paslaugų pasiekiamumas [23]. Tarnyba prisideda ir prie informacinės visuomenės plėtros komiteto kuruojamos elektronio parašo politikos bei kovos su elektroninėmis šiukšlėmis.

Vidaus reikalų ministerija (VRM) – viena iš pagrindinių institucijų, užsiimančių informacinių sistemų apsauga valstybinėse institucijose. Vidaus reikalų ministerija rengia reikalavimus ir rekomendacijas dėl informacijos saugumo.

Nusikaltimų elektroninėje erdvėje tyrimų skyrius (NEETS) dirba su nusikaltimų elektroninėje erdvėje problemomis, kurios, anksčiau buvusios aktualios užsienio valstybėse, pasiekė ir Lietuvą. NEETS ne tik atlieka elektroninę žvalgybą, bet ir atlieka sukčiavimo, grasinimo, vaikų išnaudojimo pornografijai ir kitų sričių ikiteisminius tyrimus.

Pagrindinės valstybės saugumo departamento (VSD) funkcijos yra žvalgyba, kontražvalgyba ir kova su terorizmu. Be šių funkcijų Valstybės saugumo departamentas taip pat yra atsakingas už įslaptintos informacijos saugumo kontrolę.

Nepaisant daugelio šioje srityje dirbančių organizacijų pastangų, informacijos saugumo problema vis dar yra opi ir neišspręsta.

2. INFORMACIJOS SAUGOS TEORINIS ASPEKTAS

2.1. Informacija ir informacijos saugumo problema viešąjame sektoriuje

Viešasis sektorius apima įvairias institucijas, institucijų veiklos rūšis, sprendimų priėmimą ir įgyvendinimą tose institucijose. Viešąjame sektoriuje veikia politinės institucijos, vyriausybė bei kitos įstaigos, finansuojamos iš valstybės ir savivaldybių biudžetų. Pagrindinis viešojo sektoriaus įstaigų ir institucijų tikslas yra įstatymų įgyvendinimas.

Kalbant apie informaciją valstybinėse institucijose ir kitose viešojo sektoriaus įstaigose, galime pastebėti, kad šių organizacijų veikla paremta informacijos gavimu, saugojimu, apdorojimu ir pateikimu. Viešojo sektoriaus įstaigose rengiami įvairūs dokumentai: įstatymai, teisės aktai, reglamentai, įsakymai, potvarkiai, paklausimai ir t.t. Bendravimas telekomunikacinių priemonių pagalba viešojo sektoriaus veikloje tapo kasdieniniu dalyku. Taip pat bene kiekviena įstaiga savo darbe naudojasi kompiuteriais, interneto teikiamais privalumais, o pačias įstaigas internete reprezentuoja jų tinklalapiai. Informacijos, kaupiamos duomenų bazėse ar duomenų registruose, kiekis nuolat auga. Siekdamos pagreitinti aptarnavimą bei pagerinti teikiamų paslaugų kokybę, įstaigos stengiasi įgyvendinti „vieno langelio“ aptarnavimo principą, o taip pat didelė dalis informacijos perkeliama į internetą. Nuolat didėja viešųjų elektroninių paslaugų, tokių kaip pašto, bibliotekų paslaugų, pajamų deklaravimo ar elektroninio užsiregistravimo pas gydytoją, poreikis. Šių paslaugų įdiegimui yra būtinos saugios, patikimos, be trukdžių funkcionuojančios informacinės technologijos ir visa informacinė sistema. Tai – elektroninės valdžios požymis.

Kaip teigiama „Elektroninės informacijos saugos valstybės institucijų informacinėsė sistemose srategijoje iki 2008 metų“, patvirtintoje 2006 metų birželio 19 dieną, valstybės institucijose ir įstaigose lemiamą reikšmę įgijo neįslaptinta informacija, kuri saugoma, perduodama ar kitaip apdorojama elektroniniu būdu valstybės institucijų valdomose informacinėse sistemose. Šios strategijos pagrindiniai siekiai – informacinių technologijų saugos teisinio reguliavimo plėtra, svarbiausių informacinių sistemų saugos stiprinimas, informacinių technologijų atitikties saugos reikalavimams vertinimo sistemos sukūrimas, valstybės tarnautojų mokymo informacinių technologijų saugos ugdymas.

Elektroninei informacijai įgaunant vis didesnę reikšmę institucijų veiklose nuolat didėja tikimybė susidurti su įvairiais informacijos saugumo incidentais - svarbių duomenų praradimais, konfidencialios informacijos paviešinimais, informacijos pasisavinimais, kenksmingomis

programomis ir daugeliu kitų. Siekiant užtikrinti ir sitprinti informacijos saugą viešąjame sektoriuje, tam turi būti sukurtas stiprus metodinis bei teisinis pagrindas.

2.1.1. Informacijos saugos problemų priežastys viešąjame sektoriuje. Informacijos saugumo incidentai

Svarbu išsiaiškinti, dėl kokių priežasčių viešąjame sektoriuje susiduriama su informacijos saugumo pažeidimais.

Susipažinus su šios srities publikacijomis bei straipsniais, galima pastebėti, kad informacijos saugumo problemos viešąjame sektoriuje dažniausiai kyla dėl tokių priežasčių kaip netinkamas elgesys ir neįprastas sistemų veikimas.

Pavojus informacijos saugumui dažnai kyla ne dėl techninės įrangos netobulumo, o dėl netinkamo darbuotojų, vienaip ar kitaip susijusių su informacijos apdorojimu, elgesio. Netinkamas elgesys apima informacinių sistemų arba informacijos panaudojimą asmeniniais ar komerciniais tikslais. Naudojantis informacija asmeniniais tikslais gali būti netinkamai išnaudojami informaciniai resursai, kitiems įstaigos darbuotojams gali kilti sunkumų norint laiku pasiekti reikalingą informaciją, bereikalingai švaistomos lėšos sistemos plėtrai, gali iškilti viešųjų ir privačių interesų konfliktų pavojus ar atsakomybė dėl neteisėto turinio laikymo. Nesankcionuota prieiga prie įstaigos sistemų ar tinkų, įrangos gadinimas, virusų bei kenksmingų programų platinimas taip pat traktuojami kaip netinkamas elgesys [15].

Neįprastas sistemų veikimas nėra tik techninių problemų priežastis. Dažnai neįprastas sistemos veikimas (t. y. esant neįprastiems klaidų pranešimams, vaizdo ekrane pasikeitimams, dažniems kompiuterinės sistemos užstrigimams) gali būti virusų arba įsilaužimo į sistemą požymis.

Įvykis, turintis neigiamos įtakos įprastinei informacinės sistemos veiklai arba joje apdorojamai informacijai, vadinamas informacijos saugumo incidentu. Incidento sąvoka taip pat apibūdina informacinių sistemų ir informacijos naudojimą neleistinai ar nusikalstamai veiklai. Informacijos saugumo incidento pavyzdžiu galėtų būti bandymas prieiti prie duomenų ar tinklų, kurie pagal pareigas neturėtų būti prieinami. Tokius įsilaužimus įstaigoje dažniausiai gali pastebėti tik atitinkamų žinių turintis specialistas. Vienas iš dažniausiai pastebimų informacijos saugumo incidentų yra netinkamas elgesys su slaptažodžiais. Saugumo incidentų kyla ir aplink kompiuterius esančioje aplinkoje (pvz., kai spausdintuve paliekamas konfidencialus dokumentas, neįjungiama apsauginė signalizacija, neužrakinamos duomenų saugyklos durys ir kita).

Incidentų skaičių galima ženkliai sumažinti žinant, ką reikia daryti jų metu. Pirmiausia reikia stengtis kaip galima labiau sumažinti galimas neigiamas incidento pasekmes (pvz., radus

konfidencialų dokumentą nunešti ten, kur jis turėtų būti, radus atrakintas duomenų saugyklos duris, jas užrakinti). Tuomet reikėtų apie įvykusį incidentą informuoti atsakingą darbuotoją.

Incidentų skaičių sumažinti padėtų ir informacijos apsaugą reglamentuojančių nuostatų laikymasis. Įstaigos darbuotojai taip pat turėtų dalyvauti kompiuterinio raštingumo bei informacijos apsaugos mokymuose. Labai svarbu, kad įstaigos darbuotojai neliktų abejingi informacijos saugumo problemoms. Įvykus incidentui ir pradėjus tirti jo priežastis dažnai paaiškėja, kad daugelis darbuotojų žinojo apie netinkamą elgesį ar iškilusias grėsmes, tačiau apie tai nieko neinformavo. Informacijos saugumo užtikrinimas įstaigoje – visų bendras interesas.

2.1.2. Viešojo sektoriaus informacinio turto grėsmės, pažeidžiamumai ir rizikos

Pagrindinės viešojo sektoriaus informacijos grėsmės ir pažeidžiamumai darbe nagrinėjami remiantis “Valstybės institucijų ir įstaigų informacinėse sistemose apdorojamos elektroninės informacijos rizikos analizes apibendrinančia atsakaita”, kurią 2007 metais atliko Vidaus reikalų ministerija [16].

Ataskaitoje grėsmė suprantama kaip galimybė grėsmę iššaukiančiam objektui išnaudoti tam tikrą pažeidžiamumą ir padaryti žalą informaciniam turtui – kompiuterinei įrangai, tinklui, informacijai, pačiai valstybės institucijai ar įstaigai. Grėmes iššaukiančiais objektais/subjektais gali būti žmonės, įranga ar gamta. Grėsmės gali būti iššsaukiamos ir išnaudojamos dėl įvairių motyvų, tiek tyčia (pvz. mėginant įsilaužti į elektroninės bankininkystės sistemą), tiek ne (pvz., klaidingai suvedus duomenis į sistemą). Kiekviena grėsmė veda prie pasekmių – duomenų vagystės, neteisėto slaptų ir konfidencialių dokumentų paviešinimo, pakeitimo ar praradimo.

Pažeidžiamumas ataskaitoje, kuria buvo remtasi nagrinėjant informacinio turto grėsmes ir pažeidžiamumus, suprantamas kaip tam tikrų saugos priemonių nebuvimas ar nepakankamas buvimas. Dėl to gali būti padaryta žala informaciniam įstaigos turtui ar pačiai valstybės įstaigai.
Informacinio turto pažeidžiamumo lygis gali būti skirtingas kiekvienoje įstaigoje. Jo lygį įtakoti gali šie veiksniai [16]:

- informacijos jautrumas;
- darbuotojų sugebėjimas reaguoti į informacijos saugumo pažeidimo incidentus;
- institucijos/įstaigos galimybė aptikti pažeidimus;
- darbuotojų moralė;
- darbuotojų išprusimas informacijos saugos srityje;
- esamos informacijos saugos procedūros.

Taigi, kiekvienai viešojo sektoriaus įstaigai, siekiančiai užtikrinti savo informacinio turto tinkamą apsaugos lygį, būtina suprasti pagrindines informacijai kylančias grėsmes ir pažeidžiamumus. Tik įvertinus grėsmes ir pažeidžiamumus galima tikėtis, kad saugumo užtikrinimo priemonės įstaigoje bus diegiamos efektyviai.

Vidaus reikalų ministerija, ruošdama minėtąją ataskaitą, atliko valstybės institucijų ir įstaigų grėsmių ir pažeidžiamumų tyrimą, kurio metu buvo nustatyta, kokios grėsmės ir pažeidžiamumai iškyla tipinėms viešojo sektoriaus informacinėms sistemoms. Buvo išskirtos šios grėsmių ir pažeidžiamumų grupės:

- darbuotojo apsimetimas kitu informacinės sistemos vartotoju;
- išorės asmens apsimetimas kitu informacinės sistemos vartotoju;
- neautorizuotas programinės ir techninės įrangos naudojimas;
- kenksminga programinė įranga (pvz., virusai);
- ryšio sutrikimai;
- techniniai sutrikimai (tarnybinių stočių, duomenų saugojimo įrangos; darbo vietų ir spausdinimo įrangos, tinklo įrenginių, saugos įrangos);
- techninės ir programinės įrangos priežiūros klaidos;
- vartotojų klaidos;
- personalo kompetencijos trūkumas;
- darbuotojo ar išorės asmens įvykdyta vagystė;
- duomenų sugadinimas;
- neatitiktis reikalavimams bei teisiniams aktams.

Iš išvardintų informaciniam turtui kylančių grėsmių ir pažeidžiamumų dažniausiai valstybės institucijose ir įstaigose buvo susiduriama su techniniais tarnybinės stoties sutrikimais, kenksminga programine įranga bei informacijos vartotojų klaidomis. Taigi, užtikrinus nepertraukiamą tarnybinių stočių darbą, įdiegus su kenksminga programine įranga kovojančias priemones ir užkertant kelią darbuotojų klaidoms, arba, trumpai tariant, užtikrinant organizacinį - techninį informacijos saugumą, būtų galima žymiai pagerinti informacijos saugos lygį.

Ataskaitoje taip pat pateikiama informacija apie valstybės institucijų ir įstaigų įvertintas rizikas informacinėms sistemoms. Iš pateiktos informacijos galima spręsti kurios rizikos yra labiausiai paplitę ir daugiausiai įtakoja viešąjame sektoriuje naudojamų informacinių sistemų saugą. Ataskaitos išvadose teigiama, kad didžiausios yra šios rizikos:

- įsiskverbimo į ryšius ir ryšių manipuliacijas;
- kenksmingos programinės įrangos įsiskverbimo (pvz., virusų);
- išorės asmens apsimetimo informacinės sistemos vartotoju;

- darbuotojo apsimetimo kitu sistemos vartotoju.

Problemos, su kuriomis susiduriama informacijos saugos srityje, turi būti suskirstomos pagal kritiškumą ir perduodamos spręsti atsakingiems darbuotojams. Šis metodas padeda trukdžius šalinti daug greičiau ir efektyviau.

2.1.3. Informacijos saugos įgaliotinis. Informacijos saugos tikslai viešąjame sektoriuje

Aptariant informacijos apsaugos principus viešąjame sektoriuje svarbu paminėti, jog ši sritis valstybinėse institucijose ir viešojo sektoriaus organizacijose yra reglamentuota įvairiais teisės aktais, kurie plačiau taip pat bus aptarti šiame darbe. Vienas iš teisės aktų reikalavimų yra informacijos saugos įgaliotinio, atsakingo už įstaigos informacinio turto apsaugą, skyrimas. Jis turi parengti duomenų saugos nuostatas, tvarkas ir procedūras bei užtikrinti tinkamą informacijos apsaugą įstaigoje. Vykdydamas informacijos apsaugos priežiūrą informacijos saugos įgaliotinis turi periodiškai atlikti auditus: įvertinti informacijos saugumo būklę įstaigoje bei pateikti siūlymus dėl probleminių informacijos apsaugos sričių sustiprinimo. Įgaliotinis taip pat privalo įstaigos darbuotojus supažindinti su duomenų saugos nuostatomis, išmokyti informacijos apsaugos principų.

Kalbant apie informacijos saugumo viešąjame sektoriuje pagrindinius tikslus, jie sutampa su bendraisiais informacijos saugumo tikslais: svarbus tiek informacijos konfidencialumo (informacijos vartotojų prieigos teisių valdymas), tiek vientisumo (informacijos tvarkymo, koregavimo, pekeitimo teisę turinčių darbuotojų skyrimas, antivirusinių, ugniasienių, įsilaužimo nustatymo programų diegimas), tiek ir informacijos prieinamumo (atsarginių kopijų darymas, pasrūpinimas atsarginiais ryšio kanalais ir nepertraukiamo elektros tiekimo priemonėmis) išsaugojimas. Taip pat svarbi yra atitiktis teisės ir norminių aktų reikalavimams.

Aptarus elektroninės informacijos apsaugojimo principus svarbu paminėti ir kitoje, popierinėje laimenoje saugomą informaciją. Valstybinių institucijų ir viešųjų įstaigų kasdieniniame darbe naudojamas didelis kiekis dokumentų, nutarimų, įgaliojimų ir kitų skirtingų dokumentų rūšių, todėl be diegiamų elektroninės informacijos apsaugos priemonių būtina siekti apsisaugoti ir nuo dokumentų sunaikinimo, pakeitimo ar paviešinimo. Tam pasitelkiamos ne vien fizinės apsaugos priemonės. Paplitusios dokumentų apskaitos sistemos, padedančios nustatyti, kada ir kam buvo išduotas konkretus dokumentas, naudojamos informacijos konfidencialumą nurodančios žymos ant dokumentų, nustatančios dokumentų gavėjų ratą ir įpareigojančios darbuotojus laikytis numatytų saugos procedūrų.

Informacijos apsauga yra nesibaigiantis procesas. Labai svarbu, kad šiam procesui pritartų įstaigos vadovybė. Be vadovybės pritarimo informacijos apsauga įstaigoje yra pasmerkta žlugti.

Reikėtų pabrėžti ir tai, kad derama informacijos apsauga bus užtikrinta tik tuomet, kai į šį procesą įsitrauks visi įstaigos darbuotojai.

2.1.4. Informacijos saugumą viešąjame sektoriuje reglamentuojantys dokumentai

Kaip jau buvo minėta, informacijos bei duomenų saugą valstybinių institucijų informacinėse sistemose reglamentuoja įvairūs dokumentai. Svarbiausi iš jų apžvelgiami šiame skyriuje, kurio tikslas – pažvelgti, kiek jau yra nuveikta informacijos saugumo teisinio reglamentavimo srityje, nustatyti, kaip yra reglamentuotas informacijos ir duomenų saugumas ne tik kiekvienoje viešojoje organizacijoje, bet taip pat ir skirtingų kategorijų informacinėse sistemose.

Dokumente „Informacijos technologijų saugos valstybinė strategija", patvirtintame 2001 metų gruodžio 22 dieną, nagrinėjami informacijos technologijų saugumo klausimai ir iškeliami tokie tikslai, kaip informacijos technologijų saugos teisinio reglamentavimo plėtra, svarbiausių valstybės informacinių sistemų saugos sustiprinimas, informacijos technologijų saugumo atitikties vertinimo sistemos kūrimas, valstybės tarnautojų mokymas informacijos technologijų saugos, informacijos technologijų saugos įgyvendinimo kontrolės užtikrinimas [17].

Dokumente pabrėžiama, kad informacijos technologijų saugos priemonės valstybės institucijų informacinėse sistemose bei registruose taikomos atsitiktinai ir nepakankamai.

Valstybės institucijų informacijos technologijų saugumas plėtojamas remiantis tam tikrais principais: aplinkos stebėjimo principu (būtina stebėti aplinką, norint atitikti nuolat kintančias aplinkos sąlygas), informacijos technologijų saugos sistemos ir informacinių sistemų tarpusavio priklausomybės principu (informacijos technologijų saugos sistema turi būti kuriama kartu su informacine sistema), informacijos technologijų saugos užtikrinimo pagal informacijos svarbą principu (diegtinos duomenų apsaugos priemonės pasirenkamos atsižvelgiant į jų svarbą), informacijos technologijų vartotojų ir specialistų švietimo principu (vartotojams turėtų būti rengiami kursai apie saugos svarbą ir saugos reikalavimų nesilaikymo padarinius, o informacijos technologijų specialistų kvalifikacija privalo būti nuolat keliama).

Įgyvendinant minėtas informacijos technologijų saugos priemones, reikėtų laikytis informacijos technologijų saugos bendrųjų reikalavimų, metodikos, ISO standartų.

Lietuvos Respublikos Vyriausybės nutarime „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų", kuris buvo priimtas 2006 metų birželio 19 dieną, aptariamos elektroninės informacijos apsaugos problemos valstybinėse institucijose [17].

Dokumente nurodoma, kad elektroninės informacijos apsauga turi būti vykdoma remiantis tam tikrais principais: suvokimo principu (siekiant apsaugoti informaciją, būtina suvokti apsisaugojimo nuo galimos grėsmės elektroninei informcijai priemonių naudojimo būtinybę), atsakomybės principu (kiekvienas, naudojantis elektroninę informaciją, turi suvokti savo atsakomybę saugant informaciją. Elektroninės informacijos saugą turi užtikrinti įstaigos ar institucijos vadovas, o ją įgyvendinti – saugos įgaliotiniai), reagavimo principu (labai svarbu laiku aptikti elektroninės informacijos saugos incidentus ir užkirsti jiems kelią), demokratiškumo principu (elektroninės informacijos apsauga turi būti suderinta su esminėmis demokratinės valstybės vertybėmis), rizikos įvertinimo principu (siekiant parinkti tinkamas priemones elektroninės informacijos saugumui užtikrinti, reikia periodiškai atlikti elektroninės informacijos saugos informacinėse sistemose rizikos vertinimą), elektroninės informacijos saugos kultūros kėlimo principu (norint gerinti informacijos apsaugos kokybę ir kelti informacijos saugos kultūrą viešąjame sektoriuje, būtina daug dėmesio skirti elektroninės informacijos vartotojų mokymams), elektroninės informacijos apsaugos priemonių projektavimo ir diegimo principu (elektroninės informacijos sauga įstaigoje kuriama kartu su informacine sistema. Elektroninės informacijos saugumui turi būti skiriama pakankamai lėšų).

Lietuvos Respublikos Vyriausybės nutarimu „Dėl elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose“, priimtu 2007 metų balandžio 25 dieną, siekiama, kad informacija būtų patikima ir apsaugota nuo neteisėto sunaikinimo, pakeitimo ar atskleidimo [26]. Šiuo dokumentu Lietuvos Respublikos Vyriausybė nutarė patvirtinti bendruosius elektroninės informacijos saugumo valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus. Šių reikalavimų tikslas – saugus automatiniu būdu tvarkomos informacijos panaudojimas valstybės informacinėse sistemose, registruose arba kitose informacinėse sistemose.

Užtikrinant informacijos saugumą vadovaujamasi Lietuvos standartais LST ISO/IEC 17799:2006, LST ISO/IEC 27001:2006, o taip pat tarptautiniais standartais, kurie apibūdina saugų informacinės sistemos duomenų tvarkymą.

2006 metų gruodžio 13 dieną Lietuvos Respublikos Vyriausybė priėmė nutarimą „Dėl elektroninės informacijos saugos koordinavimo komisijos sudarymo ir jos nuostatų patvirtinimo“ [28]. Elektroninės informacijos saugos koordinavimo komisiją, kuri yra nuolatinė kolegiali neįslaptintos elektroninės informacijos apsaugą valstybės institucijose ir įstaigose koordinuojanti institucija, sudaro 9 nariai (Lietuvos Respublikos Vyriausybės skiriamas komisijos pirmininkas, po vieną narį iš Lietuvos Respublikos Vyriausybės kanceliarijos, Vidaus reikalų ministerijos, Susisiekimo ministerijos, Teisingumo ministerijos, Valstybinės duomenų apsaugos inspekcijos,

Ryšių reguliavimo tarnybos, Informacinės visuomenės plėtros komiteto ir Lietuvos kriminalinės policijos biuro).

Nutarime numatomi tokie komisijos uždaviniai kaip elektroninės informacijos saugos valstybės institucijose įgyvendinimo koordinavimas, elektroninės informacijos saugumo kultūros kėlimo skatinimas bei elektroninės informacijos apsaugos projektų rengimo inicijavimas.

2007 metų liepos 11 dieną Lietuvos Respublikos vidaus reikalų ministerija priėmė įsakymą „Dėl valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių ir valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“. Informacinių sistemų klasifikavimo gairės reglamentuoja informacinių sistemų klasifikavimą pagal jose tvarkomos informacijos svarbą. Informacinės sistemos yra klasifikuojamos pagal kategorijas nuo pirmos (aukščiausios) iki ketvirtos (žemiausios):

- pirmos kategorijos informacinė sistema – tai tokia sistema, kurios duomenų praradimas gali sukelti ypač sunkius padarinius valstybei. Šios sistemos pagrindu funkcionuoja pagrindinis valstybės registras, ji leidžia stebėti valstybės piniginių išteklių srautus;
- antros kategorijos informacinė sistema – tai tokia informacinė sistema, kurios duomenų praradimas gali turėti sunkių padarinių valstybės institucijos ar įstaigos darbui bei neigiamai įtakoti kitų valstybės institucijų ar įstaigų veiklą. Šioje informacinėje sistemoje tvarkomi ypatingi asmens duomenys. Antros kategorijos informacinė sistema užtikrina pirmos kategorijos informacinių sistemų sąveiką;
- trečios kategorijos informacinė sistema – tai tokia informacinė sistema, kurios duomenų praradimas gali turėti neigiamos įtakos valstybės institucijos ar įstaigos veiklai. Šios sistemos pagrindu funkcionuoja žinybinis registras;
- visos kitos informacinės sistemos yra ketvirtos kategorijos.

Šiame įstatyme skelbiami ir informacinių sistemų elektroninės informacijos saugos reikalavimai: informacinės sistemos valdytojo ir informacinės sistemos vartotojų pareigos, reikalavimai informacinės sistemos įrangai bei patalpoms.

Lietuvos Respublikos vidaus reikalų ministerijos 2004 metų gegužės 6 dieną priimtame įsakyme „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ nustatoma informacinių technologijų saugos vertinimo metodika [26]. Ji parengta remiantis bendraisiais duomenų apsaugos reikalavimais, Lietuvos standartu LST ISO/IEC 17799:2000 bei kitais standartais.

Įstaigos informacinių technologijų saugos atitiktis vertinama dviem etapais. Pirmajame etape renkama ir vertinama reikalinga informacija: informacija apie informacinių technologijų saugos

padėtį bei dokumentai, užtikrinantys informacinės sistemos saugą (duomenų saugos nuostatai, saugaus darbo su duomenimis taisyklės ir kita). Vertinimo metu vertintojas gali atlikti įstaigos darbuotojų apklausą. Antrasis etapas apima informacinių sistemų saugos atitikties vertinimo ataskaitos rengimą, kurioje nurodomi rasti trūkumai, pateikiamos rekomendacijos trūkumams pašalinti. Parengta ataskaita su išvadomis teikiama įstaigos vadovui.

Taigi, galiojantys teisės aktai rekomenduoja, kad įstaigos vadovybėje dirbtų asmuo, kuruojantis informacines sistemas. Organizacijose su išplėtotomis informacinėmis sistemomis turėtų veikti informacinių sistemų valdymo komitetas, kuriam vadovautų įstaigos vadovybės atstovas. Atskiroms informacinėms sistemoms įstaigoje turi būti patvirtinti atskiri valdytojai, o visa informacinių sistemų priežiūra turi būti patikėta informacinių sistemų padaliniui.

Trumpai apžvelgus pagrindinius informacijos ir informacinių sistemų, elektroninių duomenų saugumo valstybės institucijose ir kitose viešojo sektoriaus įstaigose reglamentuojančius teisės aktus aišku, kad informacinės saugos srityje dirba daugelis institucijų, šioje srityje nuolat išleidžiami įvairūs nutarimai, kuriamos informacijos saugumo strategijos. Įstaigos darbas su dokumentais, informacija, informacinėmis sistemomis kasmet vis labiau reglamentuojamas, o tai padeda užtikrinti geresnį saugumą. Taigi, informacijos saugumo problema sprendžiama jau ne tik institucijų, pavienių organizacijų, bet taip pat ir valstybės lygmenyje.

2.2. Informacija ir informacijos saugumo problema privačiame sektoriuje

Aptarus viešojo sektoriaus informacijos saugos specifiką, apžvelgus pagrindines kylančias problemas ir incidentus, pasigilinus į informacijos saugą reglamentuojančius teisės aktus, šio skyriaus tikslas – panašiu principu, remiantis surinktais straipsniais, pranešimais bei konferencijomis informacijos saugumo tematika, apžvelgti informacijos apsaugos problemą privačiame sektoriuje, verslo organizacijose, kuriose informacinis turtas yra viena iš pagrindinių priemonių gauti pelno.

2.2.1. Informacija privačiame sektoriuje

Verslo įmonėse informacija sudaro didžiąją dalį pačios organizacijos vertės: įmonės žinomi nebrangūs tiekėjai ar pasiturintys klientai, įvairios komercinės paslaptys ir operatyvinė informacija leidžia organizacijai tinkamai konkuruoti bei varžytis šiandien sparčiai kintančioje ir konkurencingoje verslo aplinkoje. Būtent informacija turi lemiamą vaidmenį kovoje su

konkurencija. Šiandien natūralu, kad verslo informacija domina ne tik pačios įmonės vadovybę, bet ir konkurentus.

Dalis ar visa informacija, kuria disponuoja kiekviena įmonė, yra svarbi komerciniu požiūriu, todėl ji turi būti ypatingai saugoma. Tai, ar informacija yra konfidenciali ir svarbi komerciniu požiūriu, apibėžia žemiau išvardinti kriterijai [21]:

- tokios informacijos saugumui pasitelkiamos išskirtinės apsaugos priemonės;
- įmonė gali patirti žalą dėl tokios informacijos praradimo ar neteisėto paviešinimo;
- tokia informacija gali naudotis tik ribotas skaičius žmonių;
- už šios informacijos atskleidimą numatoma atsakomybė;
- tokia informacija dėl komercinio intereso turi būti laikoma paslaptyje.

Norint apsaugoti įmonės konfidencialią informaciją, svarbu išsiaiškinti jos galimus gavimo būdus, panaudojimo tikslus ir apsaugos priemones. Tokios informacijos kontroliavimas yra gyvybiškai svarbus kiekvienos įmonės egzistavimui, todėl būtina pasirūpinti jos apsauga.

Kompiuterių sistemos ir jų tinklai – kita svarbi visos informacijos sistemos dalis. Būtent jų pagalba šiuolaikinėje įmonėje paskirstoma, perduodama ir apdorojama didžioji dalis komercinės informacijos. Biuruose vis mažėja popieriaus, daugėja failų. Kompiuteriai šiandien kaip niekad anksčiau yra pilni informacijos apie verslą. Esant tokiai situacijai informacijos apsaugos problema tampa dar aktualesnė. Aišku, kad didelė dalis kompiuteriuose laikomos informacijos yra arba slapta, arba bent jau vidutinio naudojimo. Jei ją sužinos konkurentai ar bent jau nepatikimi bendradarbiai, pasekmės gali būti nuo nežymių iki įmonių bankrotų.

Stambesnėse įmonėse kuriami informacijos saugumo skyriai, kontroliuojantys ne tik įmonės teritorijos fizinį saugumą, bet ir analizuojantys darbuotojų fizinius portretus, filtruojantys bendradarbiams pasiekiamas interneto svetaines, archyvuojantys ir saugantys konfidencialią įmonės informaciją. Šie skyriai be minėtos veiklos stengiasi daugiau sužinoti apie konkurentų veiklą bei stebi visus interesantų veiksmus.

Kalbant apie verslo informacijos apsaugojimą Lietuvos įmonėse, pastebima, jog saugumui užtikrinti gana įprasta tapo pasitelkti tokias priemones kaip signalizacija, grotos, apsauginės durys, langai ir panašiai. Dažnai samdomi apsaugos darbuotojai, užtikrinantys įmonės turto apsaugą visą parą. Trumpai tariant, daugiausia dėmesio buvo skiriama fizinėms informacijos ir informacinio turto apsaugos priemonėms [3]. Laikui bėgant ir atsirandant vis daugiau ir vis įvairesnių grėsmių ir pažeidžiamumų informacijos atžvilgiu, taip pat informacijai tampant vis vertingesniu įmonės turtu, dėmesys kreipiamas ir į informacinių technologijų ir sistemų apsaugą, po truputį diegiamos organizacinės informacijos apsaugos priemonės (pvz., prisijungimų kontrolė, teisinė atsakomybė, personalo mokymai). Kartais net ir labai nedidelis kiekis informacijos, patekęs į konkurentų rankas,

gali atnešti įmonei didelių nuostolių. Norint užtikrinti aukštą verslo informacijos apsaugos lygį, kurio pasiekimas – ilgas ir nuolatinis procesas, reikalaujantis nemažai lėšų, informacijos apsaugojimui reikėtų skirti nemažą dalį įmonės biudžeto. Tačiau tą sau leisti gali tik stambios ar tarptautinės organizacijos.

Mažą lėšų skyrimą taip pat labai įtakoja ir pernelyg didelis pasitikėjimas įmonės darbuotojais. Konfidenciali įmonės informacija egzistuoja keliais pavidalais – dokumentuose, žmonių mintyse, elektroniniuose laiškuose, todėl tinkamai ją apsaugoti reikia imtis kompleksinių priemonių.

2.2.2. Komercinės paslaptys. Verslo informacijos grėsmės ir pažeidžiamumai

Nepaisant išvardintų priemonių, dažnai atsitinka taip, kad teisinių informacijos apsaugos priemonių įmonės komercinėms paslaptims apsaugoti imamasi tik tada, kai informacija patenka į konkurentų rankas. Nepakankamą dėmesį informacijos ir įmonės konkurencinių paslapčių apsaugai lemia ir neteisingas informacijos vertinimas. Komercinės paslaptys, kaip ir kita įmonėje saugoma ir naudojama informacija, yra intelektinės nuosavybės dalis. Komercinės paslaptys plačiąja prasme – tai bet kokia konfidenciali informacija, turinti komercinę vertę ir susijusi su įmonės ūkine, gamybine, prekybine veikla, technikos laimėjimais, įmonės valdymo ir organizavimo ypatumais. Ši informacija, patekusi į konkurentų rankas, gali jiems suteikti didelį konkurencinį pranašumą.

Su komercinėmis paslaptimis įmonėje dirba jos darbuotojai, jie ne tik kaupia informaciją, bet sugeba ją ir analizuoti, platinti, daryti tam tikras išvadas ar sprendimus. Esant palankioms sąlygoms ir turint vienokių ar kitokių motyvų komercines paslaptis ar kitą itin vertingą verslo informaciją galima parduoti, suklastoti, panaudoti savo poreikių tenkinimui.

Todėl labai svarbu tinkamai saugoti komercines paslaptis, sudarant komercinę paslaptį sudarančių žinių sąrašą, apsaugos taisykles, atsakomybės ribas neteisėtai atskleidus tokią informaciją [21].

Dažnai kyla grėsmė ir kitai verslo įmonių valdomos informacijos rūšiai – viešai gaunamai informacijai. Tokia informacija dalinamasi ryšių su visuomene metu, derybose su verslo partneriais, sudarant sutartis su tiekėjais ir panašiai. Netinkamai disponuojant tokio pobūdžio viešai prieinama informacija galima ne tik pakenkti įmonės įvaizdžiui, bet taip pat ir sustiprinti konkurentų pozicijas suteikiant jiems nors ir nedaug, tačiau labai vertingos informacijos.

Dar viena informacijos rūšis – neskelbtina informacija, tokia kaip vadovo namų telefonas, įmonės piniginė apyvarta ar išlaidos kanceliarinėms prekėms. Tokios informacijos atskleidimas nors ir nežymiai, tačiau taip pat gali pakenkti.

Svarbu prisiminti ir tai, kad versle plačiai naudojamos kompiuterinės sistemos genda ir atsiranda tikimybė prarasti svarbius verslui duomenis. Svarbių duomenų praradimas gali ne tik įtakoti produktyvumą, bet ir didelių pinigų praradimą. Taigi, versle naudojamos naujausios technologijos ne tik suteikia naujų galimybių, bet ir kelia grėsmę duomenų bei informacijos saugumui.

2.2.3. Informacijos sauga elektroniniame versle ir elektroninėje prekyboje

Atsiradus internetui – pasauliniam tinklui – jis imtas naudoti ir kaip pagalbinė priemonė vykdyti verslą. Beveik kiekviena įmonė turi savo tinklalapį, kuriame siūlo ar parduoda savo prekes bei paslaugas.

Elektroninė prekyba yra daugiau nei prekių ar paslaugų prikimas ir pardavimas internetu. Ji apima bet kokią transakciją, atliktą elektroniniu būdu, elektroninėmis priemonėmis, elektroninėje aplinkoje. Elektroninės prekybos įstatymo projekte [8] elektroninė prekyba apibrėžiama kaip prekybinės veiklos būdas, kai sutartys sudaromos, o esant reikalui ir vykdomos, naudojant informacines technologijas bei priemones kompiuterių tinklais keičiantis elektroniniais duomenų pranešimais.

Elektroninės prekybos duomenų rinkimo taisyklės yra nustatytos Europos Sąjungos duomenų apsaugos direktyvoje 95/46/EC, priimtoje 1995 metų spalio 24 dieną. Direktyva užtikrina elektroninių žinučių slaptumą, draudžia bet kokį trečiųjų asmenų įsikišimą.

Elektroninio verlo procedūroms reikalingi asmens duomenys gali būti renkami, apdorojami ir panaudojami tik tuomet, kai tai leidžia įstatymai arba yra gautas asmens sutikimas. Duomenys panaudoti gali būti tik tais tikslais, kuriais buvo renkami, jie negali būti perduodami tretiesiems asmenims. Todėl duomenys privalu tinkamai apsaugoti.

Informacijos saugumas elektroninėje prekyboje yra vienas iš svarbiausių reikalavimų. Akivaizdu, kad elektronio verslo plitimo tempai labai priklauso nuo visuomenės narių pasitikėjimo. Pagrindiniai informacijos saugos elektroniame versle reikalavimų aspektai yra šie [1]:

- slaptumas: siųsdamas dokumentą siuntėjas tikisi, kad jį skaitys tik gavėjas. Tai ypač svarbu siunčiant elektroninėje prekyboje būtinus duomenis – kreditinės kortelės numerį, gyvenamosios vietos adresą ir kt.;
- autentiškumas: gaudamas dokumentą, gavėjas pageidauja patvirtinimo, kad gautas autentiškas dokumentas ir kad jo siuntėjas yra tas asmuo, su kuriuo buvo kontaktuojama;
- efektyvumas: tiek pirkėjui, tiek pardavėjui svarbu, kad pritaikius informacijos saugumo sistemą darbo našumas nesumažėtų.

2.2.4. Verslo informacijos apsaugos priemonės

Aptarus verslo informacijai kylančius pavojus bei būtinybę apsaugoti įmonės informacinį turtą, svarbu apžvelgti ir pagrindines rekomenduojamas apsaugos priemones. Priemonės nėra universalios visoms privačiojo sektoriaus įmonėms, tačiau nuo jų galima būtų pradėti informacijos saugumo įgyvendinimą.

Norint užtikrinti versle naudojamos informacijos saugumą, patariama imtis šių techninių ir organizacinių informacijos saugos priemonių:

- įdiegti ir palaikyti ugniasienę (įmonės kompiuteriniame tinkle yra daug vertingos ir svarbios informacijos, kuri, be ugniasienės, yra lengvai prieinama įsibrovėliams. Jie, patekę į vidinį įmonės tinklą, gali pažeisti ar neteisėtai pasisavinti duomenis. Įmonės vadovybė privalo numatyti išlaidas tinkamos ugniasienės įdiegimui);
- apsaugoti verslą nuo kompiuterinių virusų (siekiant sumažinti riziką apkrėsti įmonės kompiuterius pavojingais virusais, reikia pasirūpinti naujausia apsauga nuo jų – antivirusinėmis programomis. Įmonės darbuotojai taip pat turi būti apmokomi reguliariai atnaujinti bei patikrinti antivirusinių programų duomenų bazes);
- įdiegti modernias duomenų kopijų darymo sistemas (duomenų kopijos, kilus informacijos saugos incidentams, padės greičiau grįžti prie normalaus darbo tempo ir likviduoti nuostolius);
- ruoštis blogiausiam (plėtojant verslą, būtina įvertinti riziką bei turėti tinkamą veiksmų planą įvykus nelaimei, dar vadinamą veiklos tęstinumo planu. Toks planas padeda per maksimaliai trumpą laiką pašalinti dėl elektros nuotėkio, gaisro ar vagystės atsiradusius sutrikimus bei atstatyti prarastus duomenis);
- įsitikinti įmonės darbuotojų sąžiningumu (svarbios verslo informacijos patekimas į nesąžiningo darbuotojo rankas gali turėti labai didelių neigiamų pasekmių. Siekiant to išvengti verslo organizacijose diegiama darbuotojų naudojamų įmonės duomenų sekimo sistema, kuri leidžia kontroliuoti informacijos srautus).

Daugelis įmonių savininkų ir vadovų nelinkę sureikšminti informacijos valdymo svarbos ar investuoti į verslo informacijos saugumą. Šis nenoras rodo, kad daugelis verslininkų arba labai pasitiki įmonės kompiuterinių sistemų saugumu, arba savo organizacijų darbuotojų gebėjimais protingai saugoti bei valdyti verslo informaciją.

Mobilioje ir nuolat kintančioje verslo aplinkoje labai svarbi ir galimybė reikalingą verslo informaciją pasiekti iš bet kur ir bet kuriuo metu. Nuotolinio prisijungimo prie organizacijos resursų galimybė dažnai suteikiama ne tik darbuotojams, bet ir verslo partneriams. Įmonės saugumo

politika paprastai apibrėžia, kam, iš kur ir prie kokių informacinių resursų suteikiama nuotolinė prieiga [4]. Visgi tokie prisijungimai iš bet kur ir bet kada yra labai rizikingi. Norint užtikrinti nuotolinės prieigos prie organizacijos informacinių resursų saugumą, būtina atsižvelgti į šiuos faktorius:

- vartotojų atpažinimą (labiausiai paplitęs vartotojų atpažinimo būdas yra slaptažodžių kortelė arba vienkartinių slaptažodžių sistema);
- apsisaugojimą nuo įrenginio, iš kurio jungiamasi (turi būti užtikrinama, kad jungimosi įrenginys yra saugus ir kad jame nepaliekami jokie duomenys, kuriais pasinaudojus organizacijos informacijos tinklas galėtų būti pažeistas vėliau);
- duomenų apsaugojimą juos perduodant (tam tradiciškai pasitelkiamas virtualus privatus tinklas, arba VPN);
- tinklo prieigos ribojimą (pagrindinė naudojama priemonė yra užkarda, kuri riboja prieigą prie tinklo ir apsaugo tinkle esančius resursus);
- vartotojų teisių ir nuotolinės prieigos apskaitos valdymą (po prisijungimo prie informacinių technologijų tinklo svarbu kontroliuoti, kokiais resursais vartotojas gali naudotis, o kuriais - ne. Tai svarbu, nes daugiausia pažeidimų padaro teisėti vartotojai, kurie tinkle prisijungia prie neleistinos informacijos. Sprendimas – vartotojų teisių valdymas, dažnai naudojant papildomus slaptažodžius, taip pat labai svarbu turėti visą informaciją, kas ir kada naudojosi tam tikrais resursais).

2.2.5. Informacijos saugumą privačiame sektoriuje reglamentuojantys dokumentai. Konfidencialumo sutartys

Privačiame sektoriuje informacinio įmonės turto apsauga taip pat, nors ir ne taip plačiai kaip viešajame, reglamentuota teisės aktuose. Trumpai jie bus apžvelgti šiame skyriuje.

Lietuvos Respublikos akcinių bendrovių įstatyme, priimtame 2000 metų liepos 13 dieną, bendrovės vadovui ar įmonės valdybos nariams nustatoma pareiga saugoti komercines paslaptis, kurias šie asmenys sužinojo eidami savo pareigas [9].

Lietuvos Respublikos civiliniame kodekse šalys, dalyvaujančios derybose, yra įpareigojamos neatskleisti ir savo tikslais nenaudoti derybų metu gautos konfidencialios informacijos. Jei šią pareigą kažkuri šalis pažeidžia, ji privalo kitai šaliai atlyginti padarytus nuostolius.

Lietuvos Respublikos darbo kodekso 235-ajame straipsnyje kaip vienas iš šiurkščių darbo pareigų pažeidimų traktuojamas komercinių ar technologinių paslapčių atskleidimas arba jų pranešimas konkurentų įmonei [10].

Manyti, kad įmonių konfidencialią informaciją ir komercines paslaptis kuo puikiausiai apsaugo įstatymai, klaidinga. Dažnai remiantis minėtais straipsniais susiduriama su įrodinėjimo problema, nes nėra lengva nustatyti, ar buvo nusižengta anksčiau aprašytoms įstatymų nuostatoms. Taigi, remiantis vien įstatymais nėra taip paprasta identifikuoti pažeidimus ir pašalinti jų pasekmes. Svarbu ir tai, kad įmonės darbuotojas, dažnai nesuprasdamas informacijos svarbos, gali ją atskleisti nenorėdamas ar nesitikėdamas jokių blogų pasekmių. O vieną kartą atskleista konfidenciali įmonės informacija ir iš jos gaunama nauda gali būti prarasta visam laikui.

Norint užtikrinti gerą konfidencialios įmonės informacijos apsaugą, būtina sudaryti informacijos, kuri yra laikoma komercine paslaptimi, sąrašą. Tokiame sąraše gali būti minima įmonės rinkodaros strategija, technologijos, darbo procesų organizavimas, žinios apie įmonės partnerius, įvairios sutartys ir pan. Į šį sąrašą galima įtraukti bet kokią informaciją, išskyrus tą, kuri įstatymais pripažįstama kaip vieša (įmonės steigimo dokumentai, duomenys apie valdymo organus ar steigėjus negali būti įslaptinti). Sudarinėjant konfidencialios informacijos sąrašą svarbu numatyti būdus, kaip ši informacija saugoma [25].

Lietuvos Respublikos konkurencijos įstatyme numatoma, kad asmenys, kurie dėl darbo ar kitokių sutartinių santykių su ūkio subjektu sužinoję komercinę paslaptį, ją naudoti gali praėjus ne mažiau kaip vieniems metams nuo darbo ar kitokių sutartinių santykių pasibaigimo [7]. Šia sąlygą galima įtraukti į konfidencialumo su įmonės darbuotojais sutartį. Ši konfidencialumą užtikrinanti sąlyga sutartyje gali būti derinama su nekonkuravimo reikalavimu [25]. Jo esmė yra darbuotojo įsipareigojimas, nutraukus darbo santykius su įmone, nedirbti konkuruojančioje kompanijoje. Juk perėjus dirbti į ta pačia veikla užsiimančią įmonę, perduodama ankstesnėje darbovietėje sukaupta patirtis.

Minėtieji konfidencialumo pasižadėjimai arba konfidencialumo sutartys yra bene populiariausia informacijos apsaugos priemonė, taikoma ne tik pačioje organizacijoje, bet ir palaikant santykius su klientais ar partneriais.

Civiliniame kodekse konfidencialumo sutartys nėra reglamentuojamos kaip atskira sutarčių rūšis. Taigi, konfidencialumo sutarčių teisinis reglamentavimas nėra visiškai aiškus. Visgi versle rekomenduotina į bent kiek svarbesnes sutartis įtraukti konfidencialumo sąlygą ar sudaryti atskirą konfidencialumo sutartį. Kiekvienoje konfidencialumo sutartyje turi būti apibrėžta, kas laikoma konfidencialia informacija, kas laikoma konfidencialumo pareigos pažeidimu bei kokia yra nustatyta atsakomybė už konfidencialumo pareigos pažeidimą.

Kokia informacija laikoma konfidencialia, sutartyje reikėtų apibrėžti labai tiksliai. Patariama informaciją apibrėžti ne tik turinio atžvilgiu, bet ir pagal kitus kriterijus (informacijos paskirties, gavimo būdo). Paprastai informaciją, kuri yra traktuojama kaip konfidenciali, šalis gali paskelbti tik

gavusi išankstinį kitos šalies sutikimą. Sutartyje reikėtų nustatyti, kad toks sutikimas turi būti rašytinis, patvirtintas bendrovės antspaudu ir bendrovės atstovo parašu.

Kad konfidencialumo sutartys būtų veiksmingos ir reikšmingos, svarbu:

- konfidencialumo sutartis sudaryti kaip atskirus dokumentus;
- konfidencialumo sutartis sudaryti ne tik su organizacijos darbuotojais, bet ir su valdymo organų nariais bei partneriais;
- tiksliai apibrėžti kriterijus, pagal kuriuos skiriama informacija yra konfidenciali;
- tiksliai apibrėžti, kas yra laikoma konfidencialumo pareigos pažeidimu ir numatyti baudas už tai;
- nurodyti konfidencialumo sutarties tikslą ir galiojimo terminą.

Kalbant apie informacijos ir duomenų saugumą svarbu paminėti ir asmens duomenų teisinės apsaugos įstatymą, priimtą 1996 m. birželio mėnesio 11 dieną. Kadangi vis daugiau su privačiu gyvenimu susijusių duomenų yra tvarkoma automatizuotu būdu, iškyla pavojus, kad duomenys bus panaudoti be leidimo arba netinkamai.

Šio įstatymo tikslas yra ginti žmogaus privataus gyvenimo neliečiamumo teisę, arba apsaugoti asmens duomenis.

Asmens duomenų teisinės apsaugos įstatyme asmens duomenys apibrėžiami kaip bet kuri informacija, susijusi su fiziniu asmeniu. Tokio asmens tapatybė yra žinoma arba gali būti nustatoma pasinaudojant tokiais duomenimis, kaip asmens kodas, asmeniui būdingi tam tikri požymiai [11].

Yra išskiriamas ir atskiras asmens duomenų tipas – ypatingieji asmens duomenys. Tai yra rasinė arba etninė kilmė, priklausomybė tam tikroms organizacijoms, duomenys apie asmens sveikatos būklę, teistumą ir kt. Šio įstatymo esmė – kad kiekvienas žmogus turi teisę žinoti, kaip yra tvarkomi jo duomenys, kur jie yra naudojami, leisti arba neleisti trečiosioms šalims naudoti asmens duomenis [11].

Be duomenų subjekto sutikimo asmens kodą galima naudoti tik tais atvejais, kai:

- tokia teisė yra nustatyta įstatymuose,
- atliekant mokslinius arba statistinius tyrimus,
- valstybės registruose ir informacinėse sistemose, jei jie yra įteisinti teisės aktų nustatyta tvarka.

Statistikos tikslais surinkti asmens duomenys gali būti naudojami, lyginami ir sujungiami tik tuomet, kai užtikrinama apsauga nuo neteisėto jų panaudojimo kitais tikslais.

Šiuolaikinėje visuomenėje dažnai pasitaiko, kad dėl techninio kopijavimo paprastumo be autorių sutikimo ir nesumokėjus jų prašomos kainos yra kopijuojama programinė įranga, muzikiniai kūriniai, filmai bei elektroninės knygos. Šis reiškinys yra vadinamas piratavimu. Piratavimas padaro

žalos ne tik kūrinio autoriui, kuris negauna atlygio už savo darbą, bet ir valstybei, kuri surenka mažiau mokesčių už parduotus gaminius. Autorių teisių ir gretutinių teisių įstatymas, priimtas 1999 m. gegužės mėn.18 dieną, reguliuoja autorių teises ir numato atsakomybę už šių teisių pažeidimus [12]. Kompiuteriuose aptikus programinės įrangos, už kurią nebuvo sumokėta (nelegali, arba piratinė programinė įranga), filmų ar muzikinių kūrinių, kurių kopijavimui nebuvo duota sutikimo, autoriai gali pareikalauti žalos atlyginimo ir kompensacijos. Įdiegus piratinę kompiuterinę įrangą namuose, gresia bauda. Jei tokia piratinė įranga naudojama organizacijoje ar įstaigoje, jai taip pat bus skiriama bauda. Be to, rizikuojama pakenkti įstaigos ar organizacijos įvaizdžiui.

Elektroninių ryšių įstatymas, priimtas 2004 m. balandžio mėn. 15 dieną, nustato reikalavimus telekomunikacinių paslaugų teikėjams [13]. Tai įstatymas, reglamentuojantis visuomeninius santykius, susijusius su elektroninių ryšių paslaugomis, tinklais, elektronių ryšių išteklių naudojimu. Elektronių ryšių įstatymo tikslas – kad ryšių ir elektroninių paslaugų vartotojas galėtų pasinaudoti ryšiu ir paslaugomis tada, kai jam reikia ir perduodama informacija nebūtų iškreipta. Taip pat nustatomi reikalavimai telekomunikacinių paslaugų tiekėjams užtikrinti paslaugų teikima krizių metu.

Naudoti elektroninių ryšių paslaugas (pvz. elektroninio pašto pranešimų siuntimą) rinkodaros tikslu leidžiama tik iš anksto sutinkant abonentui, kuris turi teisę bet kada atsisakyti šių paslaugų. Draudžiama tiesioginės rinkodaros tikslu siųsti elektroninio pašto pranešimus slepiant siuntėjo, kurio vardu informacija siunčiama, tapatybę arba nenurodant galiojančio adreso, kuriuo gavėjas galėtų pareikalauti nutraukti tokios informacijos siuntimą [22].

2.3. Informacijos saugos patarimai ir standartai

Aptarus informacijos saugumo problematiką iš viešojo ir privataus sektorių perspektyvų, šioje dalyje bus aptarti informacijos saugumo standartai, kurių rekomendacijomis ir patarimais galėtų pasinaudoti kiekvienas – nuo namų vartotojo, iki valstybinės institucijos, nuo eilinio tarnautojo, iki stambių organizacijų vadovų.

Šioje dalyje bus remiamasi pagrindiniu Lietuvos informacijos saugumo standartu - „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo kodeksas (tapatus ISO/IEC 17799:2005). Lietuvos standartas“, trumpai, apibrėžiant pagrindines funkcijas ir tikslus, taip pat bus paminėti kiti svarbiausi šios srities standartai.

Leidinys „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo kodeksas (tapatus ISO/IEC 17799:2005). Lietuvos standartas“ buvo parengtas tarptautinės standartizacijos organizacijos (ISO) Didžiosios Britanijos informacijos apsaugos standarto BS7799-

1 pagrindu. Lietuvos standartizacijos departamentas patvirtino jį kaip Lietuvos standartą LST ISO/IEC 17799:2005. Standartas yra nuolat tobulinamas ir papildomas, todėl jis – pats išsamiausias informacijos saugos priemonių rinkinys, kurio pagrindines rekomendacijas, pritaikomas tiek privačiame, tiek viešąjame sektoriuose, pamėginsime aptarti.

Labai svarbu, kad viešoji įstaiga ar privati organizacija identifikuotų savo saugumo reikalavimus. Yra išskiriami trys pagrindiniai saugumo reikalavimo šaltiniai [18]:

1. Pirmasis šaltinis nustatomas vertinant organizacijos riziką, atsižvelgiant į bendrąją organizacijos veiklos strategiją ir tikslus. Atliekant rizikos vertinimą, įvertinamos turtui kylančios grėsmės, pažeidžiamumas.
2. Antrasis šaltinis yra teisiniai reglamentai ir sutarčių reikalavimai bei socialinė – kultūrinė aplinka.
3. Trečiasis šaltinis yra ypatingas informacijos apdorojimui taikomas principų, tikslų ir veiklos reikalavimų rinkinys.

Saugumo reikalavimai turi būti identifikuojami metodiškai vertinant saugumo rizikas. Identifikavus saugos reikalavimus ir riziką bei priėmus su rizikos priežiūra susijusius sprendimus, turėtų būti parenkamos ir įdiegiamos atitinkamos valdymo priemonės, leidžiančios užtikrinti, kad rizika bus sumažinta iki priimtino lygio.

Atsižvelgiant į teisinius reikalavimus, priklausomai nuo galiojančių įstatymų, organizacijai yra būtinos šios valdymo priemonės:

a) duomenų apsaugos ir asmeninės informacijos slaptumo;
b) organizacijos įrašų apsaugos;
c) intelektinės nuosavybės teisių.

Bendrojoje įstaigos ar įmonės informacijos saugumo praktikoje turėtų būti taikomos tokios valdymo priemonės, kaip informacijos saugumo politikos dokumentas, atsakomybės už informacijos saugumą skyrimas, informacijos saugumo supratimas, švietimas ir mokymas, korektiškas programų veikimas, techninio pažeidžiamumo valdymas, veiklos tęstinumo valdymas, informacijos saugumo incidentų ir tobulinimo valdymas bei kt.

Šiuolaikinė organizacija turėtų vykdyti informacijos saugumo politiką, kurios pagrindinis tikslas – nustatyti valdymo kryptį ir užtikrinti informacijos saugą atitinkančius veiklos reikalavimus ir atitinkamus įstatymus bei reglamentus [18]. Vadovybė turėtų nustatyti aiškią politikos kryptį, atitikančią veiklos tikslus, akivaizdžiai ją palaikyti ir įpareigoti, paskelbdama ir remdama informacijos saugumo politiką visoje organizacijoje.

Informacijos saugumo politikos dokumentas turėtų būti patvirtintas vadovybės, paskelbtas ir pateiktas visiems darbuotojams bei su tuo susijusioms išorinėms šalims. Dokumente turėtų būti pateikta [18]:

a) informacijos saugumo apibrėžtis, tikslai, taikymo sritis ir svarba;
b) vadovybės ketinimų remti informacijos saugumo tikslus ir principus nuostata;
c) valdymo tikslų ir priemonių numatymo bendroji programa;
d) trumpas saugumo politikos aiškinimas, principai, standartai;
e) bendrųjų ir ypatingų informacijos saugumo valdymo atsakomybių apibrėžimas;
f) dokumentų, kurie gali paremti saugumo politiką, nuorodos.

Organizacijos informacijos saugumo politika turėtų būti peržiūrima periodiškai. Taip pat turėtų būti numatytas asmuo, kuris, vadovybės įgaliojimu, būtų atsakingas už informacijos saugumo politikos tobulinimą, priežiūrą ir įvertinimą.

Nagrinėjamame Lietuvos standarte aprašomi ir informacijos saugumo reikalavimai dirbant su klientais. Visi organizacijos numatyti saugumo reikalavimai turėtų būti įgyvendinti prieš klientams suteikiant prieigą prie organizacijos informacijos ar turto. Labai svarbu apsvarstyti procedūras, skirtas apsaugoti organizacijos turtą, skirtas nustatyti, ar nėra kilęs pavojus turtui, taip pat informacijos kopijavimo ir atskleidimo pavojus. Organizacijai, dirbančiai su klientais, svarbu turėti ir prieigos valdymo politiką, kuri apimtų:

a) leidžiamus prieigos metodus bei unikalių vartotojų identifikatorių ir slaptažodžių naudojimą ir valdymą;
b) vartotojo prieigos sankcionavimo procedūrą ir privilegijas;
c) pareiškimą, kad bet kokia nesankcionuota prieiga yra draudžiama.

Informacija, siekiant užtikrinti tinkamą jos apsaugos lygį, turi būti klasifikuojama [18]. Yra įvairūs informacijos slaptumo ir pavojingumo lygiai. Informacija turi būti klasifikuojama atsižvelgiant į jos vertę, teisinius reikalavimus, slaptumą bei svarbą organizacijai. Turėtų būti numatomas klasifikavimo kategorijų skaičius ir iš jų gaunama nauda. Taip pat reikia pasirūpinti, kad klasifikavimo žymos ant dokumentų būtų suprantamos jais besinaudojantiems žmonėms. Turėtų būti nustatytas kiekvienas klasifikavimo lygmuo, priežiūros procedūros, įskaitant saugų apdorojimą, laikmeną, perdavimą, išplatinimą ir sunaikinimą.

Be fizinio, aplinkos ir įrangos saugumo reikia užtikrinti ir žmogiškųjų išteklių saugumą, t.y., kad darbuotojai, rangovai ir trečiosios šalys supranta savo atsakomybę ir yra tinkami jiems paskirtoms užduotims atlikti bei mažinti vagystės, sukčiavimo ar piktnaudžiavimo informacija ir informacijos apdorojimo priemonėmis riziką.

Darbuotojai turėtų veikti pagal organizacijos informacijos saugumo politikas, saugoti turtą nuo nesankcionuotos prieigos, paviešinimo, iškreipimo, sunaikinimo ar trukdžių, pranešti apie informacijos saugumo incidentus.

Darbuotojų saugumo įsipareigojimai ir atsakomybės gali būti reglamentuojamos ir pareigybiniuose aprašymuose.

Visi darbuotojai, rangovai ar trečiosios šalies atstovai, kuriems suteikta prieiga prie slaptos informacijos, turėtų pasirašyti konfidencialumo sutartis. Darbuotojams, pažeidusiems saugumo reikalavimus, turėtų būti taikoma oficiali drausminė procedūra. Pasibaigus darbo sutarties galiojimo laikui visos darbuotojui suteiktos prieigos prie informacijos ar informacijos apdorojimo priemonių teisės turėtų būti panaikintos.

Labai svarbu pasirūpinti ir fiziniu bei aplinkos saugumu. Jo tikslas – išvengti nesancionuotos fizinės prieigos, nuostolių ir trikdžių organizacijos veiklai ir informacijai.

Svarbios ir slaptos informacijos apdorojimo priemonės turėtų būti laikomos saugiose vietose, kurios yra saugomos nustatytomis saugumo aptvaromis su atitinkamomis saugumo kliūtimis ir įėjimo kontrole.

Apsauga būna patikimesnė, kai naudojama keletas kliūčių. Patariama imtis fizinės įėjimo kontrolės, kad būtų užtikrinta, jog įleidžiamas tik įgaliotas personalas. Turėtų būti registruojama kiekvieno lankytojo atvykimo ir išvykimo data ir laikas. Prieiga prie vietų, kuriose apdorojama ar laikoma slapta informacija, turėtų būti saugoma, į ją patekti leidžiant tik įgaliotiems asmenims.

Įrangos saugumo tikslas – išvengti turto netekties, žalos, vagystės arba defektų ir organizacijos veiklos pertrūkių [18]. Organizacijoje naudojama įranga turėtų būti apsaugota nuo fizinių ar aplinkos keliamų grėsmių. Įrangos vieta turi būti parenkama taip, kad kiek galima labiau būtų sumažinta nereikalinga prieiga į darbo vietas. Taip pat patariama numatyti gaires, reglamentuojančias valgymą, gėrimą ir rūkymą šalia informacijos apdorojimo priemonių.

Siekiant užtikrinti informacijos saugą organizacijoje labai svarbu valdyti ryšių ir darbo procedūras. Turėtų būti parengtos ir įformintos dokumentais sistemos veiklos, susijusios su informacijos apdorojimo ir ryšių priemonėmis, procedūros (pavyzdžiui, kompiuterio įjungimo ir išjungimo, atsarginių kopijų darymo, įrangos priežiūros, laikmenų tvarkymo procedūros).

Darbo procedūrose turėtų būti smulkiai apibūdinamas kiekvienos šių užduočių vykdymas:

a) informacijos apdorojimas ir priežiūra;
b) atsarginių kopijų darymas;
c) nurodymai, kaip tvarkyti klaidas ar kitas išimties sąlygas, kurios kiltų atliekant darbus;
d) ryšių palaikymas kilus netikėtiems darbo ar technikos sunkumams;
e) specialios informacijos išvesties ir laikmenų priežiūros instrukcijos;

f) audito eigos žurnalų ir informacijos apie prisijungimą prie sistemos valdymas.

Kalbant apie apsaugą nuo kenksmingų ir mobiliųjų programų, svarbu imtis atsargumo priemonių siekiant atpažinti kenksmingų programų (kompiuterinių virusų, tinklo kirminų ir pan.) įsibrovimą ir apsisaugoti nuo jų. Programinės įrangos naudotojai turėtų būti įspėti apie kenksmingų programų keliamus pavojus. Turėtų būti taikomos aptikimo, išvengimo ir atkūrimo priemonės, skirtos apsisaugoti nuo kenksmingų programų. Organizacijoje turėtų būti nustatoma oficiali politika, draudžianti naudoti nesankcionuotą programinę įrangą.

Viena iš svarbiausių procedūrų siekiant palaikyti informacijos ir informacijos apdorojimo priemonių vientisumą ir parengtumą – atsarginių kopijų darymas. Vadovaujantis organizacijoje numatyta atsarginių kopijų politika turėtų būti reguliariai daromos ir išbandomos informacijos ir programinės įrangos atsarginės kopijos. Organizacijoje turi būti apibrėžtas būtinos atsarginės informacijos lygis, tikslus ir išsamus atsarginių kopijų registravimas. Atsarginių kopijų darymo apimtis ir dažnumas turėtų atitikti organizacijos veiklos reikalavimus. Kopijos turėtų būti laikomos atskiroje, pakankamai nutolusioje patalpoje. Atsarginei informacijai turėtų būti numatomas tinkamas fizinės ir aplinkos apsaugos lygis. Kopijos turi būti periodiškai tikrinamos ir išbandomos.

Jei organizacija verčiasi elektronine prekyba, turėtų būti numatyti su elektroninės prekybos paslaugomis, įskaitant tiesioginėmis (interneto) transakcijomis, susiję saugumo aspektai ir reikalavimai. Taip pat turi būti numatytas elektroniniu būdu skelbiamos informacijos vientisumas ir prieinamumas [18].

Informacija, susijusi su viešaisiais tinklais atliekama elektronine prekyba, turėtų būti apsaugota nuo nesąžiningų veiksmų, išvengiant ginčų dėl sutarčių ir nesankcionuoto jos atskleidimo ir pakeitimo. Elektroninės prekybos sandoriai tarp prekybos partnerių turi būti paremti dokumentais įformintomis sutartimis, įpareigojančiomis abi šalis laikytis sutartų prekybos nuostatų.

Siekiant užtikrinti, kad informacija bus pasiekiama tik autorizuotiems vartotojams, labai svarbus yra prieigos valdymas. Prieiga prie informacijos, informacijos apdorojimo priemonių ir veiklos procesų turi būti prižiūrima pagal organizacijos veiklos ir saugumo reikalavimus.

Prieigos valdymo politika turėtų aiškiai nustatyti kiekvieno vartotojo ar vartotojų grupės prieigos valdymo taisykles ir teises. Prieigos valdymo priemonės būna loginės ir fizinės ir jos turi būti taikomos kartu.

Turėtų būti parengta oficiali vartotojo registravimo ir išregistravimo procedūra prieigai prie visų informacinių sistemų ir paslaugų.

Slaptažodžiai yra bene labiausiai paplitusi vartotojų tapatybės nustatymo priemonė. Kai tinka, turėtų būti numatomos ir kitos vartotojo identifikavimo ir autentiškumo patvirtinimo technologijos – biometrinės, pirštų antspaudų patvirtinimas, parašo patvirtinimas ir kt.

Visiems vartotojams turėtų būti privaloma laikytis slaptažodžių konfidencialumo, parinkti kokybiškus, pakankamo ilgio slaptažodžius, periodiškai juos keisti.

Popierinių dokumentų ir keičiamųjų laikmenų atžvilgiu turėtų būti taikoma „švaraus stalo“ politika, o informacijos apdorojimo priemonių atžvilgiu – „saugaus ekrano“ politika.

Slapta ir ypač svarbi organizacijos veiklos informacija, kai ji nėra naudojama ir ypač paliekant darbo vietą be priežiūros, turėtų būti laikoma užrakinta. Išsiunčiamos ir gaunamos korespondencijos laikymo vietos ir be priežiūros palikti fakso aparatai turėtų būti apsaugoti. Taip pat turėtų būti išvengta nesankcionuoto naudojimosi kopijavimo aparatais ir kita dauginimo įranga. Dokumentai, kuriuose pateikiama ypatingai slapta informacija, iš spausdintuvo turi būti išimami nedelsiant.

„Švaraus stalo“ politika sumažina nesankcionuotos prieigos, informacijos praradimo ar sugadinimo riziką įprasto darbo metu ar po jo.

Siekiant sumažinti neigiamus padarinius organizacijoje ir atkurti veiklą po informacijos praradimų iki priimtino lygio, turi būti įgyvendintas veiklos tęstinumo valdymo procesas, taikant prevencijos ir atkuriamąsias valdymo priemones. Siekiant, kad, nutrūkus svarbiausioms operacijoms, jos būtų atnaujinamos laiku, turi būti numatyti ir įgyvendinti veiklos tęstinumo planai.

Be visų išvardintų, standarte „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo kodeksas (tapatus ISO/IEC 17799:2005). Lietuvos standartas“ rekomenduojamų informacijos apsaugos priemonių labai svarbi yra ir atitiktis teisiniams reikalavimams, ypač viešąjame sektoriuje, kuriame informacijos apsauga yra griežtai reglamentuota įstatymais ir nutarimais.

Tarptautinė standartizacijos organizacija ISO jau yra paruošusi arba dar ruošia ir kitus informacijos saugumo standartus. Standarte ISO 27001:2005 aprašyta Demingo PDCA (Planavimas – Įgyvendinimas – Matavimas – Gerinimas) ciklu paremta informacijos apsaugos vadybos sistema. ISO 27002 standartas – tai informacijos saugos priemonių rinkinys, apimantis organizacines bei technines informacijos saugos priemones. Dabar šis standartas vadinasi ISO 17799:2005. ISO 27003 standarte išdėstytos rekomendacijos informacijos apsaugos vadybos sistemos įgyvendinimui. Šiais metais planuojamo išleisti ISO 27004 standarto tikslas – padėti organizacijoms įvertinti informacijos apsaugos valdymo proceso ir informacijos apsaugos priemonių efektyvumą, o standarto ISO 27005 – padėti organizacijoms įgyvendinti rizikų valdymo procesą. Pastarasis standartas planuotas išleisti 2007 – 2009 metų laikotarpyje.

Remiantis įvairiais literatūros šaltiniais – nuo straipsnių internetiniuose naujienų portaluose, iki už informacijos saugumą atsakingų institucijų pranešimų – šiame skyriuje buvo nagrinėjama informacijos saugumo problematika, bendrosios tendencijos, pagrindiniai informacijos saugos bruožai viešąjame ir privačiame sektoriuje. Didelis dėmesys skirtas ne tik informacijos saugumo

grėsmių, rizikų ir pažeidžiamumų, informacijos apsaugos priemonių analizei, bet taip pat ir teisinei šios srities pusei – buvo apžvelgta, kaip informacijos sauga yra reglamentuota viešojo valdymo institucijose, ir kokie teisės aktai saugo verslo informaciją.

Išnagrinėti literatūros ir informacijos šaltiniai leido padaryti tik abstrakčias prielaidas, su kokiomis informacijos saugumo problemomis susiduria privačiame ir viešąjame sektoriuje dirbantys asmenys, dėl kokių priežasčių tos problemomis kiekviename sektoriuje iškyla, kaip jos sprendžiamos. Nėra aišku ir tai, ar skirtingas kiekvieno sektoriaus informacijos saugumo srities reglamentavimas sąlygoja geresnę ar blogesnę informacijos apsaugą. Tikslesnius atsakymus į iškilusius klausimus turėtų pateikti atliktas tyrimas – informacijos saugos specialistų, informacinių technologijų specialistų ir duomenų saugos specialistų, dirbančių interneto ir elektroninės prekybos bendrovėse ir valstybės institucijose, apklausa.

3. INFORMACIJOS SAUGOS VIEŠĄJAME IR PRIVAČIAME SEKTORIUJE TYRIMAS

3.1. Tyrimo metodologija

Šiame darbe buvo nagrinėjama aktuali ir opi informacijos apsaugos problema. Buvo mėginama apžvelgti informacijos saugumo specifikas dviejuose sektoriuose – viešąjame, kurio institucijų veikla paremta informacijos gavimu, perdavimu, saugojimu, bei privačiame, kuriame informacija gali suteikti didelių pranašumų dirbant konkurencingoje verslo aplinkoje. Remiantis įvairiais straipsniais, pranešimais iš tarptautinių konferencijų, šia tema išleistomis knygomis, informacijos saugumo standartais bei informacijos saugumą reglamentuojančiais teisės aktais, buvo aprašytos pagrindinės viename ir kitame sektoriuje kylančios informacijos saugumo problemos, labiausiai pažeidžiamos vietos, galimos kylančių informacijos saugos incidentų priežastys bei jų likvidavimo būdai.

Šiame skyriuje bus pateikta atlikto kiekybinio tyrimo – elektroninės už informacijos saugumą ar informacines sistemas konkrečioje organizacijoje atsakingų asmenų apklausos analizė.

Analizė buvo atliekama pasitelkus kiekybinį tyrimą – elektroninę apklausą, kurioje dalyvavo skirtinguose sektoriuose (viešąjame ir privačiame) dirbantys informacijos, informacinių technologijų ir informacijos saugos specialistai. Kiekybinis tyrimas buvo pasirinktas su tikslu nustatyti bendras informacijos saugumo tendencijas sektoriuose, atlikti bendrus palyginimus.

Tyrimo problema:

Sparčiai plintant informacinėms technologijoms, didėjant informacijos kiekiui, tiek viešojo, tiek privataus sektoriaus darbuotojai susidūrė su informacijos apsaugojimo problemomis. Nustačius pagrindines informacijos saugumo grėsmes, su kuriomis susiduria kiekvieno sektoriaus darbuotojai, taip pat sužinojus jų naudojamas informacijos saugumo priemones, vadovybės požiūrį į šią problemą, informacijos saugumo politikos įgyvendinimo dažnumą bei jų pačių nuomonę apie šią problemą, būtų galima parengti tam tikras rekomendacijas kiekvieno sektoriaus darbuotojams, taip pat paraginti sektorius pasidalinti savo gerosiomis praktikomis informacijos saugumo srityje.

Tyrimo tikslas:

Nustatyti informacijos saugumo tendencijas, problemas, padėtį viešojo ir privataus sektoriaus organizacijose.

Uždaviniai:

- nustatyti, su kokiais informacijos saugumo incidentais susiduria privataus, ir su kokiais – viešojo sektoriaus darbuotojai;
- nustatyti, ar su kylančiais informacijos saugumo incidentais kovojama ir kokių priemonių imamasi kiekvieno iš tiriamų sektorių organizacijose;
- nustatyti, ar informacijos apsaugos priemonės viešose ir privačiose organizacijose taikomos tikslingai ir pakankamai;
- nustatyti, ar organizacijos patiria žalą dėl informacijos saugumo incidentų, ir, jei taip – tai kokią;
- ištirti, kaip organizacijose valdomi informacijos saugumo incidentai;
- nustatyti, ar su konfidencialia informacija dirbančiose organizacijose pasirašomos konfidencialumo pasižadėjimo sutartys;
- nustatyti, ar organizacijose laikomasi informacijos saugumo politikos, taisyklių, nuostatų;
- nustatyti, dėl kokių priežasčių organizacijoje taikoma informacijos saugumo politika;
- išsiaiškinti, kokios pagrindinės priežastys organizacijose trukdo spręsti informacijos saugos problemas.

Tyrimo metodai:

- Apklausa elektroniniu paštu, atlikta siekiant įgyvendinti užsibrėžtus tikslus. Tyrimo apklausa sudaryta iš atvirų ir uždarų klausimų;
- Apklausos elektroniniu paštu analizė, pateikiant bendruosius atsakymų pasiskirstymus ir komentarus.

Kadangi visų viešąjame ir privačiame sektoriuje dirbančiųjų apklausti dėl didelių laiko sąnaudų yra neįmanoma, planuojant tyrimą buvo nuspręsta, kad jame turėtų dalyvauti:

- Kompetetingi informacijos saugos srityje asmenys, galintys identifikuoti pagrindines šios srities problemas ir tendencijas – t.y. informacinių sistemų valdytojai, informacijos saugos įgaliotiniai, duomenų apsaugos specialistai;
- Pakankamas respondentų kiekis, kad kiekybinio tyrimo metu gauti duomenys būtų reprezentatyvūs ir patikimi;
- Konkrečios srities viešojo ir privataus sektoriaus organizacijų darbuotojai. Iš privataus sektoriaus buvo nuspręsta pasirinkti interneto ir elektroninės prekybos paslaugas teikiančias bendroves (šių bendrovių pagrindinė veikla – kokybiško internetinio ryšio tiekimas, informacinių sistemų aptarnavimas, duomenų perdavimas, gavimas, informacijos

saugojimas, prekybos elektroninėje erdvėje vykdymas), iš viešojo – valstybinės institucijos ir Vyriausybei atskaitingos institucijos (šių institucijų veikloje naudojama visa svarbiausia valstybės informacija – nuo asmens duomenų, iki informacijos apie valstybės biudžetą). Būtent dėl įvairialypės ir slaptos bei konfidencialios informacijos panaudojimo kasdieninėje savo veikloje buvo nuspręsta pasirinkti interneto bei eletroninės prekybos paslaugas teikiančias organizacijas (čia svarbi asmens duomenų apsauga, konfidencialios klientų informacijos saugumo užtikrinimas, saugaus interneto ryšio tiekimas) ir valstybės institucijas (svarbiausių valstybės informacinių srautų valdymas ir saugumas).

Duomenų rinkimas:

Kaip jau buvo minėta, tyrimui atlikti buvo pasirinktas elektroninės apklausos metodas. Pasirinkus šį metodą, svarbu buvo nustatyti reikalingą apklausos dalyvių skaičių. Duomenims rinkti dėl savo patogumo ir nedidelių laiko sąnaudų tyrime dalyvavusiems respondentams buvo pasirinktas informacijos rinkimo būdas elektroniniu paštu.

Tyrimo objekto elementas (imties vienetas):

1. Įmonė, kurios pagrindinė ekonominės veiklos rūšis yra interneto ir/arba elektroninės prekybos paslaugos.
2. Valstybės ir Vyriausybei atskaitinga institucija.

Tyrimo imties dydis: generalinę visumą sudarė 300 interneto ir elektroninės prekybos bendrovės, užsiregistravusios informacijos katalogo www.visalietuva.lt duomenų bazėje, ir 141 valstybės institucija ir Vyriausybei atskaitinga institucija.

Elektroninės apklausos dalyvių imtis buvo apskaičiuojama pagal formulę:

$$n = \frac{Nt^2 p\,q}{\Delta^2 N + t^2 p\,q}$$

Šioje formulėje n – imtis (reikalingas apklausti respondentų skaičius), N – generalinės visumos vieneto skaičius, pq – maksimali dispersijos reikšmė (0,25), Δ – numatytas ribinės imties paklaidos dydis <= 0,05, t – patikimumo koeficientas (t = 2, kai tikimybė P = 0,95). Imtis pagal šią formulę su 95 procentų tikimybe užtikrina, kad rezultatų paklaida yra ne daugiau kaip 2 procentai.

Pagal šią formulę apskaičiavus apklausos dalyvių imtį, buvo gautas rezultatas, kad elektroninėje apklausoje turi dalyvauti 171 interneto ir elektroninės prekybos bendrovė ir 104 valstybės institucijos.

Tyrimo laikas: elektroninė apklausa buvo vykdoma nuo 2008.03.18 iki 2008.04.02 dienos.

Tyrimas buvo vykdomas keliais etapais. Pirmasis – pasiruošimas tyrimui, t.y. literatūros informacijos saugumo tema studijavimas, pagrindinių problemų šioje srityje aiškinimasis, tyrimo tikslo ir uždavinių nustatymas. Sekančiame etape buvo pasirinktas tyrimo metodas, respondentų kontingentas, tyrimo imtis. Vėliau buvo vykdomas duomenų rinkimas respondentams klausimynus išsiunčiant elektroniniu paštu. Galiausiai gauti atsakymai buvo analizuojami, pateikiami bendrieji rezultatų pasiskirstymai, nurodantys svarbiausias tendencijas. Kiekybinio tyrimo duomenys buvo apdorojami teoriškai, t.y. atliktas duomenų aptarimas darbe.

Anketą „Informacijos sauga viešajame ir privačiame sektoriuje“ sudarė vienas atviras ir septyniolika uždarų klausimų. Didesnis uždarųjų klausimų skaičius buvo pasirinktas dėl keleto priežasčių: kad respondentams būtų lengviau pasirinkti, kad būtų paprasčiau apdoroti duomenis ir atlikti skaičiavimus bei palyginimus. Prie kai kurių uždarų klausimų buvo suteikiama galimybė ne tik pažymėti vieną iš atsakymų, bet taip pat ir paliekama vietos išsakyti savo nuomonę. Tai leido apklausoje dalyvavusiems respondentams išsakyti tai, ko dėl uždarų klausimų ribotumo jie negalėjo padaryti.

3.2. Tyrimo rezultatai

Kvietimai dalyvauti elektroninėje apklausoje informacijos saugumo tematika respondentams buvo išsiųsti elektroniniu paštu. Gautuose laiškuose respondentams buvo nurodoma, koks yra šio tyrimo tikslas, pagrindiniai uždaviniai, kas yra tyrimo sumanytojas ir vykdytojas. Pasirinktų organizacijų informacijos saugumo specialistams užpildžius elektronininę apklausą, visi atsakymai buvo gauti į tyrimo vykdytojo elektroninio pašto dėžutę, vėliau spausdinami, rūšiuojami ir analizuojami. Kaip jau buvo minėta, elektroninė apklausa vykdyta nuo 2008 metų kovo 18 dienos, kuomet buvo išsiųstos pirmosios anketos ir gauti pirmieji atsakymai, iki 2008 balandžio 2 dienos, kai buvo gauta paskutinė užpildyta anketa.

Prieš pradedant analizuoti elektroninės apklausos metu surinktus respondentų atsakymus, bus apžvelgta, kokia yra informacijos saugumo specifika tyrime dalyvaujančiose organizacijose – t.y., valstybės institucijose ir interneto bei elektroninės prekybos įmonėse.

Vykdydamos savo pareigas valstybės institucijos renka įvairią informaciją apie valstybės piliečius, ją saugo, perduoda trečiosioms šalims, pačios naudoja, ir, kai informacija jau

nebereikalingas, ją sunaikina. Tokios informacijos apie asmenis rūšis skiriasi nuo bet kokios kitos informacijos. Gyvename demokratinėje teisinėje visuomenėje, kur asmens teisės ir laisvės yra svarbiausios. Viena iš tokių teisių – asmens teisė į privatmą ir duomenų apsaugą. Dėl šios priežasties, norėdamos tvarkyti asmens duomenis, valstybės institucijos turi turėti tam teisinį pagrindą. Tokią teisę suteikti gali atskiras įstatymas ar bendro pobūdžio asmens duomenų apsaugą reglamentuojantis įstatymas.

Kalbant apie interneto ir elektroninės prekybos įmones, jų kasdieniniame darbe taip pat yra būtinas duomenų apie klientus rinkimas, kuriuos klientai pateikia patys. Keista, tačiau daugelis anksčiau atliktų tokių įmonių tyrimų patvirtino, kad informacijos kiekis, kurį prašoma pateikti įsigyjant tam tikrą produktą ar paslaugą elektroninėje erdvėje, dažnai yra perteklinis ir visiškai nebūtinas. Svarbu tai, kad duomenys apie klientus gali būti renkami tik jiems sutinkant ir tik juos informavus, o panaudojami tik tokiais tikslais, kokiais buvo renkami.

Atlikus literatūros informacijos saugumo tema analizę, apibrėžus, koks tyrimas bus vykdomas, nusistačius reikalingą tyrimo imtį, buvo pradėtas elektroninės apklausos vykdymas. Pirmoje lentelėje pateikiamas atsakymų grąžos lygis pagal imties parametrus. Grįžusių atsakymų kiekis rodo, kad apklausoje informacijos ir informacijos saugumo specialistai dalyvavo pakankamai aktyviai.

1 lentelė. Eletroninės apklausos atsakymų grąža

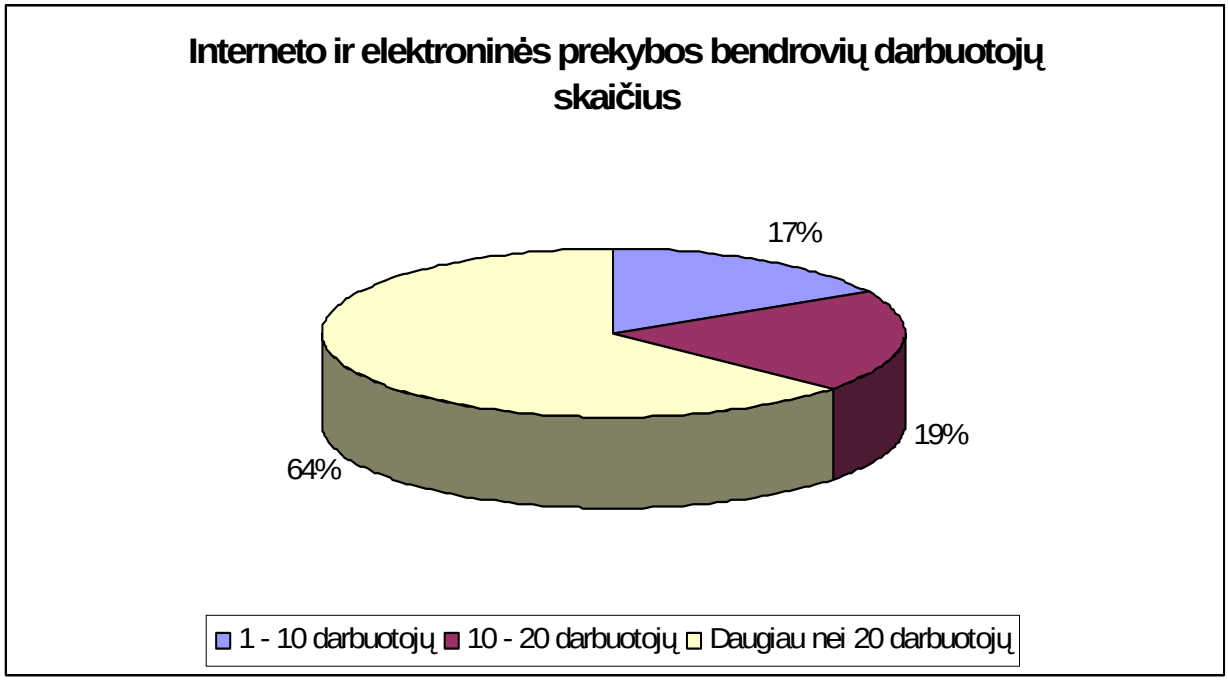
Sektorius	**Organizacijų skaičius iš viso**	**Išsiųstų anketų skaičius**	**Gautų atsakymų skaičius**	**Atsakymų grąža proc.**
Interneto ir elektroninės prekybos bendrovės	300	200	171	86%
Valstybės institucijos	141	130	105	81%

Elektroninės apklausos klausimai buvo formuluojami tikslingai, struktūrizuotai, kad būtų galima nustatyti ne tik bendrąją informaciją apie tyrime dalyvaujančias organizacijas (pvz, organizacijos dydį), bet taip pat ir surinkti svarbius duomenis informacijos saugumo tematika: duomenis apie tai, su kokiais informacijos saugos incidentais organizacijos susiduria, kokios informacijos saugos priemonės organizacijoje naudojamos, kokią žalą organizacijos patiria informacijos saugumo incidentų metu, kaip yra valdomi informacijos saugumo incidentai, dėl kokių priežasčių nėra užtikrinama pakankama informacijos sauga organizacijose. Respondentai taip pat buvo klausiami, ar jų organizacijose dirbama su konfidencialia informacija ir ar darbuotojai yra

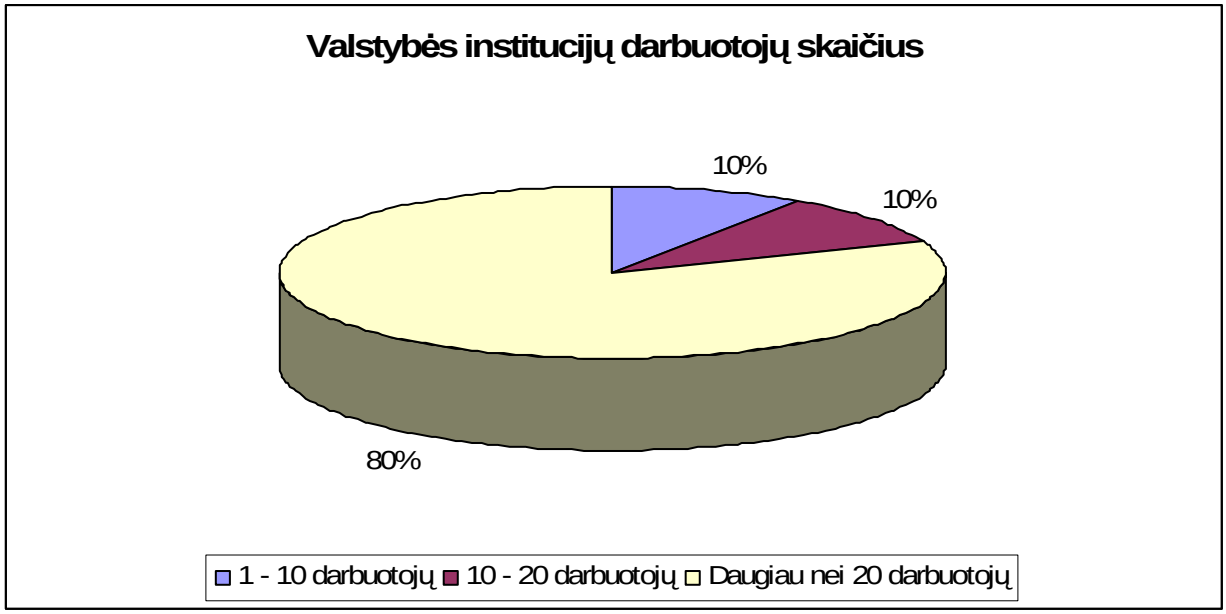
pasirašę konfidencialumo sutartis, taip pat buvo mėginama sužinoti informacijos ir duomenų saugumo specialistų nuomonę apie tai, ar informacija jų organizacijoje yra pakankamai apsaugota. Vienas iš atvirųjų klausimų buvo apie respondentų nuomonę, kodėl reikėtų arba kodėl nereikėtų saugoti informacinio organizacijos turto. Respondentai atsakinėjo į klausimus ir dėl „švaraus stalo“ bei „švaraus ekrano“ politikos jų organizacijoje, ir dėl atsakingų asmenų informavimo apie įvykusius informacijos saugumo incidentus.

Elektroninėje apklausoje dalyvavo įvairių dydžių bendrovių ir institucijų atstovai. Tyrime dalyvavusių bendrovių ir institucijų procentinis paskirstymas pagal jose dirbančių žmonių skaičių pateiktas pirmoje ir antroje diagramoje.

1 diagrama. Tyrime dalyvavusių interneto ir elektroninės prekybos bendrovių darbuotojų skaičius



2 diagrama. Tyrime dalyvavusių valstybės institucijų darbuotojų skaičius



Iš pateiktų rezultatų matome, jog elektroninėje apklausoje dalyvavo už informacijos saugumą pagrinde didelėse (turinčiose daugiau negu 20 darbuotojų) organizacijose atsakingi asmenys. Informacijos saugumo aspektu svarbu pabrėžti, kad didesnėse organizacijose sukaupta ir cirkuliuoja daugiau duomenų ir informacijos, o informacinių procesų ir informacijos saugumo valdymas yra sudėtingesnis ir procesas, reikalaujantis daugiau laiko ir lėšų negu mažesnėse organizacijose.

Visi tyrime dalyvaujantys respondentai, informacinių sistemų, informacijos saugumo specialistai bei už informacijos saugą atsakingi darbuotojai teigė, kad jų organizacijose susiduriama su įvairiais informacijos saugumo incidentais. Taigi, kaip buvo aptarta teorinėje darbo dalyje, informacijos gausa, informacinių resursų perkėlimas į elektroninę erdvę atnešė didelį susirūpinimą informacijos saugumu, konfidencialumo, slaptumo, vientisumo ir prieinamumo užtikrinimu. Atliktas praktinis tyrimas dar kartą įrodė, kad informacija organizacijose nėra pakankamai apsaugota, kad kasdien jai iškyla įvairių grėsmių ir kad šią problemą būtina spręsti.

Vienas iš tyrimo tikslų – nustatyti, su kokiais incidentais susiduriama dirbant su skirtingo pobūdžio informacija viešąjame ir privačiame sektoriuje. Ties šiuo klausimu respondentai turėjo galimybę pažymėti tiek atsakymų, kiek informacijos saugumo incidentų yra patiriama jų organizacijose.

Net 69% tyrime dalyvavusių privačiojo sektoriaus atstovų ir 81% viešojo sektoriaus informacijos saugumo specialistų pažymėjo, jog jų organizacijose nuolat susiduriama su dviem ar daugiau skirtingų informacijos saugumo incidentų.

Prieš analizuojant tyrimo metu gautus respondentų atsakymus, bus apžvelgta, kokias grėsmes informacijai ar organizacijos veiklai gali kelti kiekvienas iš dažniausiai patiriamų informacijos saugos incidentų – t.y. nepageidaujami elektroniniai laiškai, kompiuteriniai virusai, duomenų vagystės, įsilaužimai į kompiuterius bei piktavališki organizacijos darbuotojų veiksmai vietiniame tinkle.

Nepageidaujami elektroniniai laiškai (angl. *spam*), dažniausiai platinami reklaminiais tikslais, Lietuvoje yra draudžiami Reklamos įstatymo ir Elektroninių ryšių įstatymo, kurie nustato, kad tokio pobūdžio reklaminės žinutės gali būti siunčiamos tik su išankstiniu gavėjo sutikimu ar prašymu. Vadinamasis „spam‘as“ yra draudžiamas, nes dažniausiai yra siuntinėjamas be gavėjų sutikimo, reikalauja nemažų laiko ir piniginių sąnaudų siekiant jais atsikratyti. Nepageidaujami elektroniniai laiškai taip pat klaidina gavėjus, pažeidžia jų privatumą ir interesus.

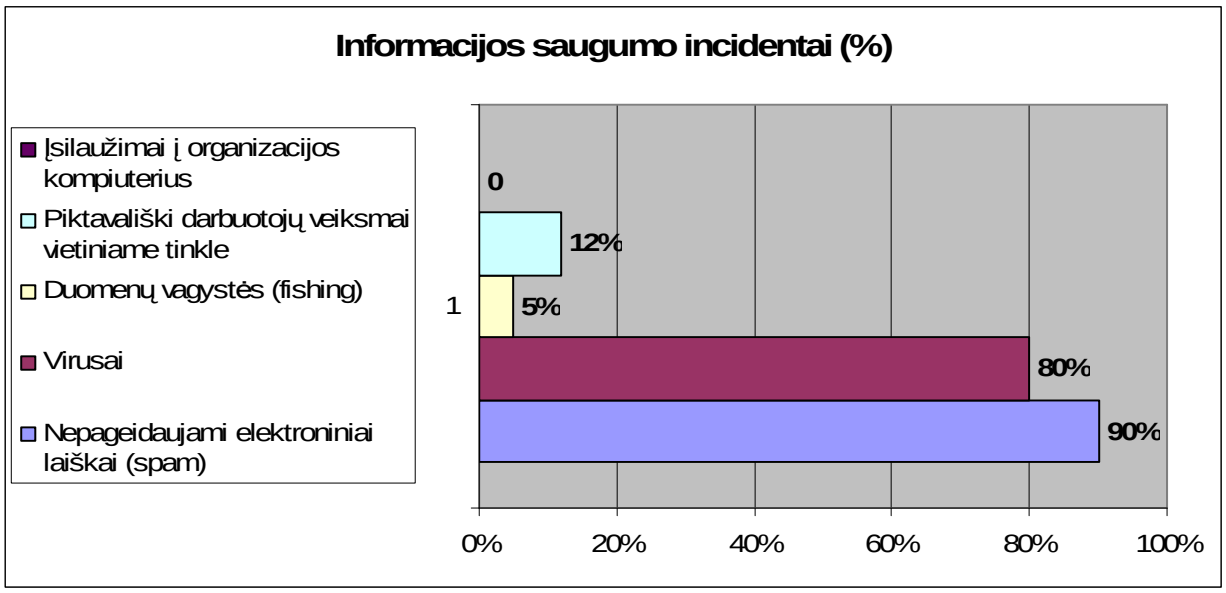
Kompiuteriniai virusai – tai piktavališkos kompiuterinės programos, galinčios daugintis ir plisti internetu iš kompiuterio į kompiuterį. Virusai gali sukelti ypač daug žalingų padarinių: sunaikinti, sugadinti ar persiųsti trečiajam asmeniui kompiuteryje saugomą informaciją. Įvairūs statistiniai tyrimai rodo, kad pasaulyje jau buvo sukurta per milijoną kompiuterinių virusų, o 2008 m. sausį pradėti skaičiuoti dvidešimt tretieji metai nuo pirmojo viruso sukūrimo.

Duomenų vagystė – tai tokia sukčiavimo forma, kai pasinaudojant nepageidaujamais elektroniniais laiškais ar falsifikuotais interneto tinklalapiais siekiama išgauti duomenis apie slaptažodžius, internetinės bankininkystės prisijungimus ar kitą konfidencialią informaciją. Ši sukčiavimo forma nuolat plinta.

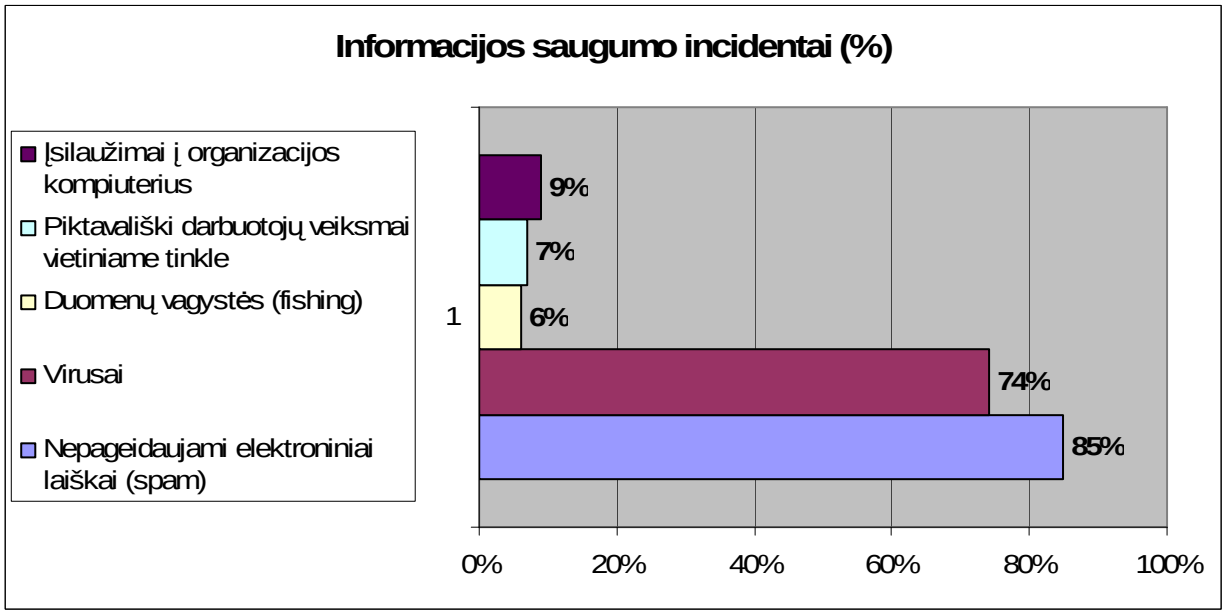
Įsilaužimai į organizacijos kompiuterius gali atnešti ypač didelių nuostolių, nuo kompiuterinės įrangos sugadinimo, iki slaptos informacijos paviešinimo, kuomet gali nukentėti organizacijos reputacija, būti patirtos didelės finansinės išlaidos ir pan.

Viešojo ir privataus sektorių organizacijų kiekis, kurios susiduria su įvairiais informacijos saugumo incidentais, procentiškai pavaizduotas trečioje ir ketvirtoje diagramose.

3 diagrama. Valstybės institucijų, susiduriančių su informacijos saugumo incidentais, skaičius



4 diagrama. Interneto ir eletroninės prekybos bendrovių, susiduriančių su informacijos saugumo incidentais, skaičius



Tyrimo metu gauti rezultatai rodo, jog dažniausiai tiek viešojo sektoriaus, tiek privataus informacijai kylanti grėsmė yra nepageidaujami elektroniniai laiškai (angl. *spam*), kompiuteriniai virusai bei duomenų vagystės.

Tyrimo rezultatai leidžia atlikti pirmuosius sektorių palyginimus: viešąjame sektoriuje dažniau nei privačiame susiduriama su tokiais incidentais, kaip nepageidaujami laiškai ir virusai, duomenų vagysčių atvejų kiekviename iš sektorių pasitaiko beveik vienodai dažnai, o su tokiais drąstiškais incidentais, kaip įsilaužimais į organizacijos kompiuterius, susiduria kas dešimta privati organizacija. Tuo tarpu viešąjame sektoriuje su šiuo incidentu, kaip rodo tyrimo metu surinkti respondentų atsakymai, nesusiduriama.

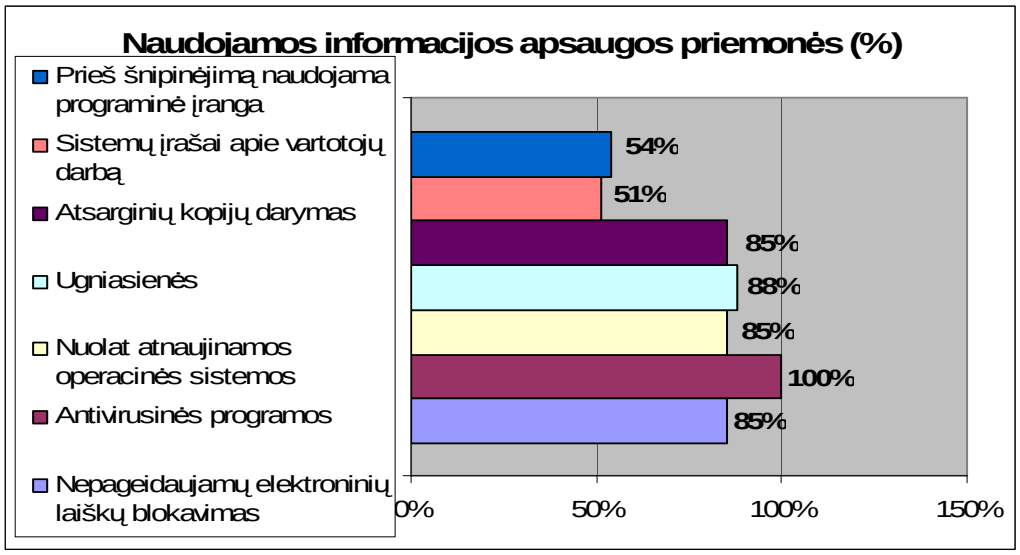
Apklausoje dalyvavę respondentai buvo paprašyti įvardinti ir kitus, tyrimo anketoje nepaminėtus incidentus, dėl kurių kyla grėsmė jų organizacijose naudojamos informacijos saugumui. Viešojo sektoriaus atstovai išskyrė tokias problemas, kaip netyčiniai duomenų sugadinimai, kompiuterių vagystės, bandymai įsilaužti į internetinės svetainės duomenų bazę. Privataus sektoriaus informacijos saugos specialistai paminėjo, jog informacijai kyla grėsmių dėl silpnų slaptažodžių bei vagiamų kompiuterių, ko pasekoje gali būti pasiekta konfidenciali įmonės informacija bei pavagiami slapti verslo duomenys.

Atlikus informacijos incidentų analizę sektoriuose, galima daryti pirmąsias išvadas. Informacijos saugumas kelia vienokių ar kitokių rūpesčių tiek valstybės tarnautojams, tiek verslo žmonėms. Jų informacija pažeidžiama panašiais būdais, naudojamos panašios priemonės prieiti tiek prie viešojo, tiek prie privataus sektoriaus informacijos, galima pastebėti tik nedidelius skirtumus tarp skirtingo viename ir kitame sektoriuje kylančių informacijos saugos incidentų kiekio.

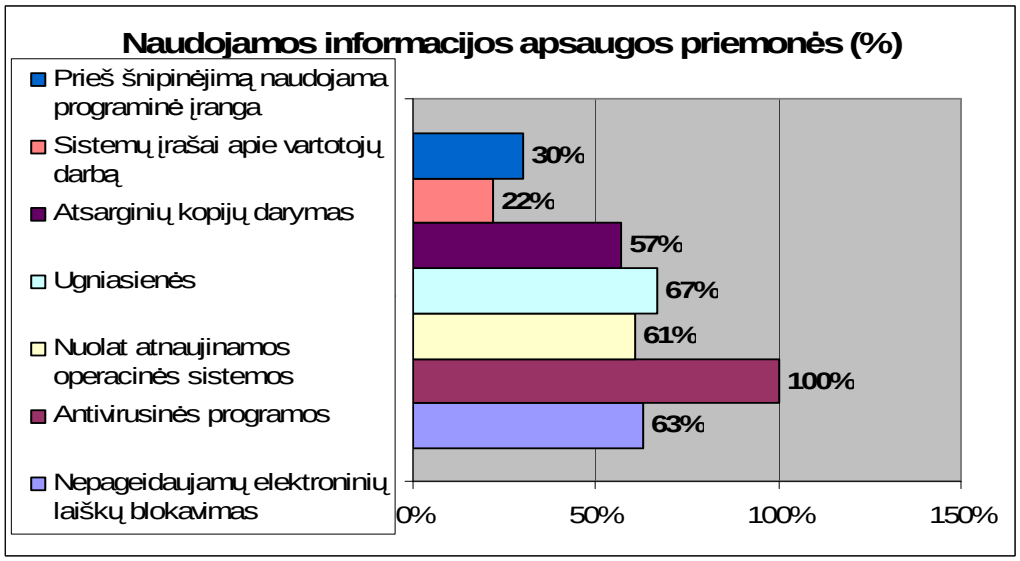
Nustačius svarbiausias informacijai kylančias grėsmes kiekviename sektoriuje, svarbu išsiaiškinti, kokias priemones informacijai apsaugoti naudoja viešojo ir privataus sektoriaus organizacijos, ar priemonės pasirenkamos pagal tai, su kokiomis informacijos saugos grėsmėmis dažniausiai susiduriama. Tik tikslingas ir pakankamas informacijos apsaugos priemonių naudojimas gali užtikrinti pakankamai aukštą informacinio saugumo lygį bei apsisaugoti nuo sunkių padarinių.

Kiekviename sektoriuje naudojamos informacijos apsaugos priemonės pagal jų naudojimo dažnumą pasiskirstė taip, kaip pavaizduota penktoje ir šeštoje diagramose.

5 diagrama. Viešąjame sektoriuje naudojamos informacijos apsaugos priemonės



6 diagrama. Privačiame sektoriuje naudojamos informacijos apsaugos priemonės



Visos tyrime dalyvavusios organizacijos kovoja su informacijos saugumo incidentais pasitelkdamos įvairias informacijos apsaugos priemones. Reikia pastebėti, jog 89% privataus sektoriaus kompanijų informacijos saugumui užtikrinti priemones naudoja kompleksiškai - derina iškart dvi ir daugiau priemonių, taip siekdamos kuo aukštesnio informacijos apsaugos lygio organizacijose. Viešojo sektoriaus organizacijose net 98% analizuotų atvejų informacijos saugumui užtikrinti buvo taikomos dvi ir daugiau informacijos apsaugos priemonių. Organizacijos suvokia, kad vien tik antivirusinės programos, kurias naudoja visos tyrime dalyvavusios organizacijos, negali

užtikrinti pakankamo informacijos saugumo. Grėsmės informaciniam turtui yra labai skirtingo pobūdžio, skirtingas pasekmes sukeliančios, todėl ir tinkamą apsaugos lygį gali užtikrinti tik kompleksiškas įvairiapusiškų informacijos apsaugos priemonių naudojimas ir nuolatinis tobulinimas.

Nustačius incidentus, su kuriais susiduriama viešąjame ir privačiame sektoriuje, bei šiuose sektoriuose naudajamas informacijos apsaugos priemones, toliau bus apžvelgta, ar naudojamos priemonės yra pasirinktos pagal tai, su kokiais incidentais susiduriama ir ar jos gali padėti išvengti ar sumažinti dėl informacijos saugumo incidentų patiriamus nuostolius.

Kaip buvo minėta, viešąjame sektoriuje dažniausiai susiduriama su kompiuteriniais virusais bei nepageidaujamais elektroniniais laiškais. Kovai su virusais visos tyrime dalyvavusios valstybės institucijos naudoja antivirusines programas, kurios aptinka virusus ir apie juos praneša vartotojams, o siekdamos išvengti nepageidaujamų elektroninių laiškų 85% institucijų yra įdiegusios tokių laiškų blokavimo priemones, leidžiančias užblokuoti tam tikrų nepageidaujamų adresatų laiškus.

Kad būtų išvengta sunkių pasekmių, kurias gali sukelti įstaigos darbuotojų piktavališki veiksmai vietiniame tinkle, kas antroje tyrime dalyvavusioje valstybės institucijoje daromi ir saugomi sistemos įrašai apie vartotojų darbą, atliktus pakeitimus, informacijos išsaugojimus, perrašymus ir panašiai. Tokie įrašai suteikia galimybę už informacijos saugumą atsakingiems žmonėms stebėti vartotojų darbą, nustatyti tam tikrų informacijos saugos incidentų kaltininkus, užbėgti už akių sunkesniems nusikaltimams.

Antroje vietoje po antivirusinių programų pagal naudojimo paplitimą viešojo sektoriaus informacinėse sistemose yra ugniasienės (angl. *firewal*), apsaugančios nuo įsibrovėlių bei blokuojančios įtartinų failų įėjimą ir išėjimą. Naudojant antivirusinę programą kartu su ugniasiene, užtikrinamas pakankamai aukštas institucijų informacinių sistemų apsaugos lygis nuo interneto keliamų grėsmių, tokių kaip virusai, duomenų vagystės ir kiti.

Be paminėtų priemonių valstybės institucijose naudojama ir atsarginių kopijų darymo bei nuolatinio operacinių sistemų atnaujinimo praktika (atsargines kopijas daro ir nuolat savo operacines sistemas atnaujina 85% tyrime dalyvavusių valstybės institucijų). Atsarginių kopijų darymo ir saugojimo procesai reglamentuoti teisės aktuose, įtraukti į informacijos saugumo rekomendacijas ir standartus, nes tai viena iš efektyviausių priemonių įvykus informacijos saugumo incidentui atkurti prarastą ar pakeistą informaciją ir greitai grįžti prie įprasto darbo ritmo nepatiriant didesnių nuostolių. Nuolatinis operacinių sistemų atnaujinimas pašalina iš sistemų saugumo spragas ir gerina operacinėse sistemose saugomų duomenų apsaugos lygį. Paprašyti įvardinti kitas informacijos apsaugos priemones, naudojamas viešojo sektoriaus informacijai apsaugoti,

respondentai paminėjo prieigos kontrolės valdymą (kai teisę naudotis tam tikra informacija turi tik autorizuoti asmenys), interneto srautų kontrolės valdymą.

Atlikus trumpą viešajame sektoriuje patiriamų informacijos saugos incidentų ir naudojamų saugos priemonių analizę, buvo nustatyta, kad informacijos apsaugos priemonės valstybės institucijose naudojamos tikslingai ir kompleksiškai, jomis kovojama su realiomis grėsmėmis, taip pat pasitelkiamos papildomos prevencinės priemonės, tokios kaip atsarginių duomenų kopijų darymas, antišnipinėjimo programų diegimas ir panašiai.

Kalbant apie privataus sektoriaus informacijos saugumą, buvo nustatyta, kad nepageidaujami elektroniniai laiškai bei kompiuteriniai virusai kelia didžiausią grėsmę verslo informacijai. Kovai su virusais visos tyrime dalyvavusios organizacijos naudoja įdiegtas antivirusines programas, o nepageidaujamų laiškų blokavimo priemones naudoja ne visos su šia problema susiduriančios organizacijos. Taigi, ši saugumo spraga nėra visiškai užpildyta.

Ugniasienės privataus sektoriaus organizacijose naudojamos tikslingai, nes jose neretai susiduriama su įsibrovimais į įmonių kompiuterius, kuomet kyla didžiulė grėsmė slaptai verslo informacijai. Paprašyti įvardinti kitas, į anketos sąrašą neįtrauktas informacijos apsaugos priemones, privataus sektoriaus atstovai paminėjo dažną priverstinį slaptažodžių pakeitimą prie visų sistemos prieigų, taip pat ir informacinių resursų prieigos kontrolę. Šios priemonės apsaugo informaciją nuo patekimo tretiesiems asmenims į rankas.

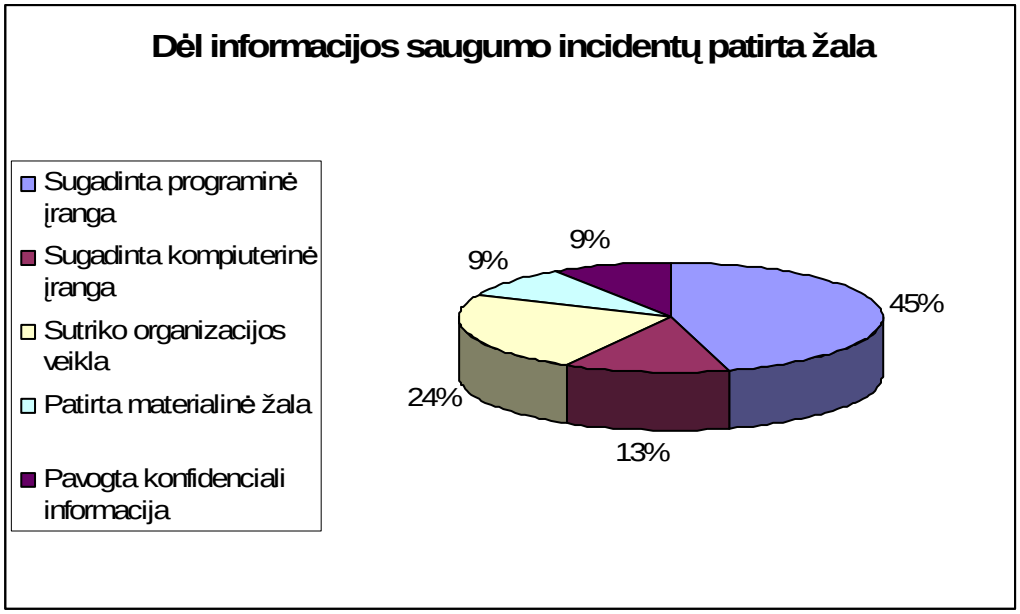
Atlikus bendrąją apžvalgą pastebėta, jog viešojo sektoriaus organizacijos informacijos apsaugos priemones taiko dažniau, kompleksiškiau ir tikslingiau, o privačiame sektoriuje dalis priemonių, atsižvelgus į informacijai kylančias grėsmes, taikomos nors ir tikslingai, tačiau nepakankamai.

Kaip jau buvo aptarta teorinėje darbo dalyje, beveik visi informacijos saugumo incidentai sukelia nemažai organizacijoms juntamų pasekmių – dėl jų gaištamas brangus darbuotojų laikas, sutrinka organizacijos veikla, dažnai patiriami finansiniai nuostoliai, nukenčia organizacijos reputacija. Atliktame tyrime kaip vienas iš iškeltų tikslų buvo išsiaiškinti, ar įmonės patiria žalą dėl vykstančių informacijos saugumo incidentų, kokią žalą patiria daugiausia organizacijų.

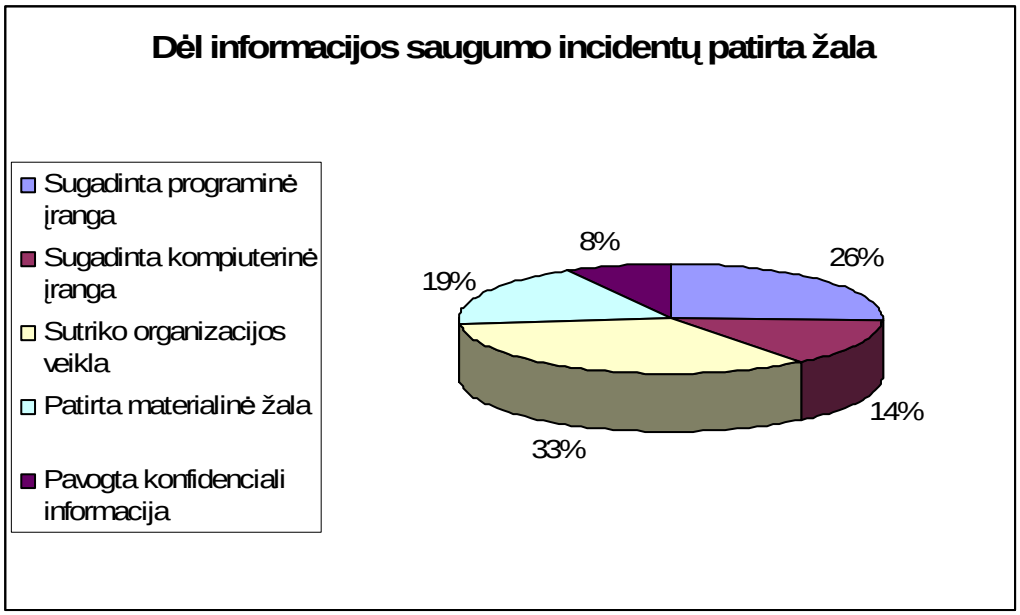
Tyrimo metu nustatyta, kad daugiau kaip pusė viešojo ir privataus sektoriaus organizacijų realios žalos dėl kylančių informacijos saugumo incidentų nepatyrė: žalos nepatyrė 64% viešojo ir 63% privataus sektoriaus organizacijų.

Iš žalą patyrusių organizacijų buvo tokių, kurios deklaravo keletą skirtingų patirtų žalų. Procentiškai žalų patyrusių, skirtingus žalų tipus nurodžiusių organizacijų duomenys pagal sektorius pateikiami sekančiose diagramose.

7 diagrama. Žala, kurią dėl saugumo incidentų patyrė valstybės institucijos



8 diagrama. Žala, kurią dėl saugumo incidentų patyrė interneto ir elektroninės prekybos bendrovės



Nors dėl kilusių informacijos saugumo incidentų žalos patyrė panaši dalis viešojo ir privataus sektoriaus organizacijų, visgi patirta žala skiriasi savo pobūdžiu. Incidentų pasekoje viešasis sektorius dažniausiai atsipirkdavo sugadintos programinės įrangos taisymu ar naujos įsigyjimu – vadinasi, dėl kilusių incidentų būdavo ne tik gaištamas laikas, bet ir patiriami finansiniai nuostoliai, nes reikėdavo skirti lėšų naujai programinei įrangai įsigyti ar sugadintos įrangos (kompiuterinių programų, operacinių sistemų) taisymui. Kas ketvirta žalą patyrusi institucija pabrėžė, kad dėl

kylančių informacijos saugumo incidentų sutriko įprastinė veikla, dėl to mažėjo produktyvumas, buvo vėluojama atlikti tam tikrus darbus ir pan. Materialinę žalą teigė patyrusios 9% tyrime dalyvavusių valstybės institucijų. Paprašyti įvardinti ir kitą dėl informacijos saugumo incidentų patirtą žalą, viešąjame sektoriuje dirbantys informacijos specialistai paminėjo, kad dėl saugumo sutrikimų vėluojama atlikti tam tikrus darbus, kaupiasi ir daugėja darbų.

Kalbant apie privatųjį sektorių, dažniausiai dėl incidentų patiriama žala – komercinės organizacijos veiklos sutrikimas, kuris buvo pastebėtas net trečdalyje tyrime dalyvavusių interneto ir elektroninės prekybos bendrovių. Sutrikus veiklai įmonės gaišta laiką, o laikas – pinigai, todėl galime teigti, kad netiesiogiai, tačiau patiriama ir materialinė žala. Pakankamai dažnai dėl kylančių informacijos saugumo incidentų genda įmonių programinė (26% tirtų atvejų) bei kompiuterinė (14% tirtų atvejų) įranga. Gedimai taip pat kainuoja ne tik daug papaildomo laiko, bet ir pinigų. Tiesioginę materialinę žalą teigia patyrusios beveik kas dešimta tyrime dalyvavusi interneto ir elektroninės prekybos bendrovė. Tarp kitų dėl informacijos saugumo incidentų patiriamų žalų buvo paminėta moralinė žala (įmonės, patyrusios incidentus, dažnai jausdavosi pažeidžiamos ir nesugebančios apsaugoti svarbios verslo informacijos), darbo apimčių dėl kokybės bei saugumo užtikrinimo padidėjimas, taip pat vėlavimai atlikti darbus, klientų lūkesčių nepateisinimai.

Bene pavojingiausias, informacijos saugumo incidentų sąlygojamas procesas, atnešantis ne tik finansinių nuostolių, bet galintis stipriai pakenkti organizacijos reputacijai yra konfidencialios įmonės ar įstaigos informacijos pasisavinimas, su kuriuo susiduria panašus skaičius tiek viešojo, tiek privataus sektoriaus organizacijų.

Apibendrinant šią tyrimo dalį, galima atlikti pastebėjimą, kad nepaisant organizacijose taikomų informacinio turto apsaugos priemonių daugelis organizacijų vis dar patiria žalą dėl incidentų, o žalos pobūdis labai įvairus – nuo veiklos sutrikimų ir kompiuterių gedimų, iki konfidencialių duomenų vagysčių.

Įvairių priemonių informacijos saugumui užtikrinti naudojimas negali garantuoti šimtaprocentinio saugumo. Kaip jau buvo kalbėta teorinėje šio darbo dalyje, labai svarbus yra ir saugumo incidentų valdymas, už informacijos saugą organizacijoje atsakingų asmenų skyrimas, nes tai padeda ne tik kovoti su kylančiomis grėsmėmis ir patiriamais incidentais, tačiau ir išvengti jų ateityje.

Taigi, informacijos saugumo incidentai gali būti valdomi įvairiai – organizacijoje juos valdyti gali būti paskirtas tas pats asmuo, kuris valdo informacines sistemas, taip pat šią funkciją atlikti gali informacijos saugos įgaliotinis, apie kurį plačiau rašyta buvo teorinėje dalyje, ar CERT, t.y. kompiuterinių incidentų valdymo (angl. *Computer Emergency Response Team*) grupė. Informacijos saugumo incidentų valdymas dažniausiai apibrėžiamas organizacijos informacijos saugos politikoje,

nuostatuose ar taisyklėse, tačiau ne kiekviena organizacija jas turi. Vienas iš atlikto tyrimo tikslų buvo pasigilinti į informacijos saugumo problemą incidentų valdymo aspektu, nustatyti, ar organizacijos turi informacijos saugumo politikas, kaip valdo incidentus.

Apklausus viešojo ir privataus sektoriaus informacijos saugos specialistus, paaiškėjo, kad kas dešimtoje tyrime dalyvavusioje valstybės institucijoje ir net kas penktoje interneto ir elektroninės prekybos įmonėje nėra vykdoma informacijos saugumo politika. Tokių organizacijų skaičius pateikiamas sekančioje lentelėje:

2 lentelė. Organizacijų skaičius, kuriose nėra vykdoma informacijos saugumo politika

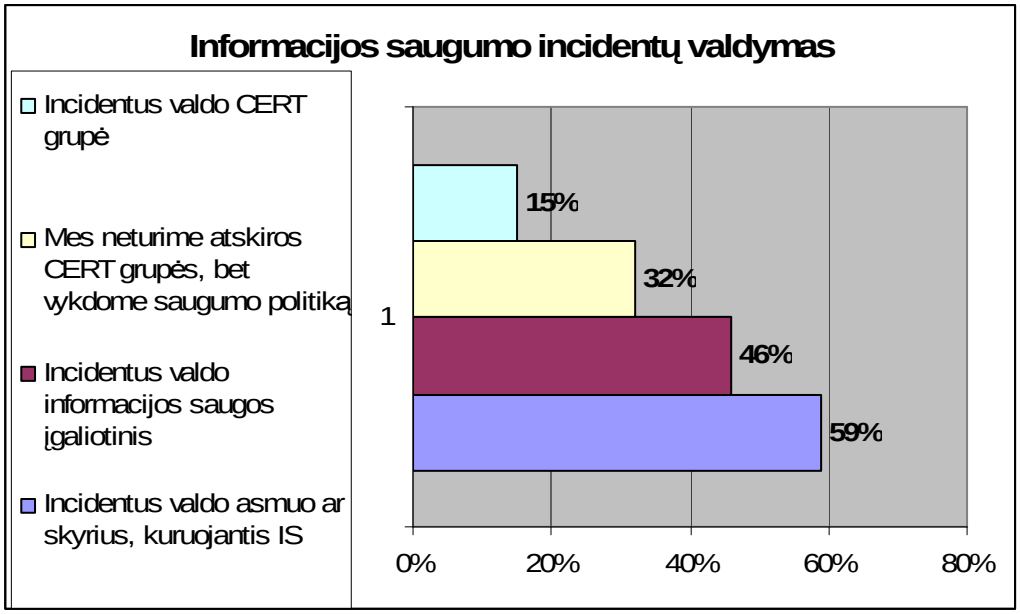
Sektorius	**Nėra vykdoma informacijos saugumo politika (org. skaičius/%)**
Viešasis sektorius	11 organizacijų (t.y. 10% apklaustųjų)
Privatus sektorius	34 organizacijos (t.y. 20% apklaustųjų)

Toks didelis procentas informacijos saugumo politiką vykdančių viešojo sektoriaus organizacijų liudija, kad saugumu šiose įstaigose rūpinamasi labiau negu privataus sektoriaus bendrovėse. Remiantis teorine darbo dalimi galime daryti prielaidą, kad tokius skaičius sąlygoja griežtas informacijos saugumo srities reglamentavimas viešojo sektoriaus organizacijose, kuriose privaloma ne tik skirti ypatingą dėmesį informacinio turto apsaugojimui, bet taip pat nuolat vykdyti saugumo politiką, skatinti darbuotojų sąmoningumą šiuo klausimu bei rodyti pavyzdį kitiems rinkos dalyviams.

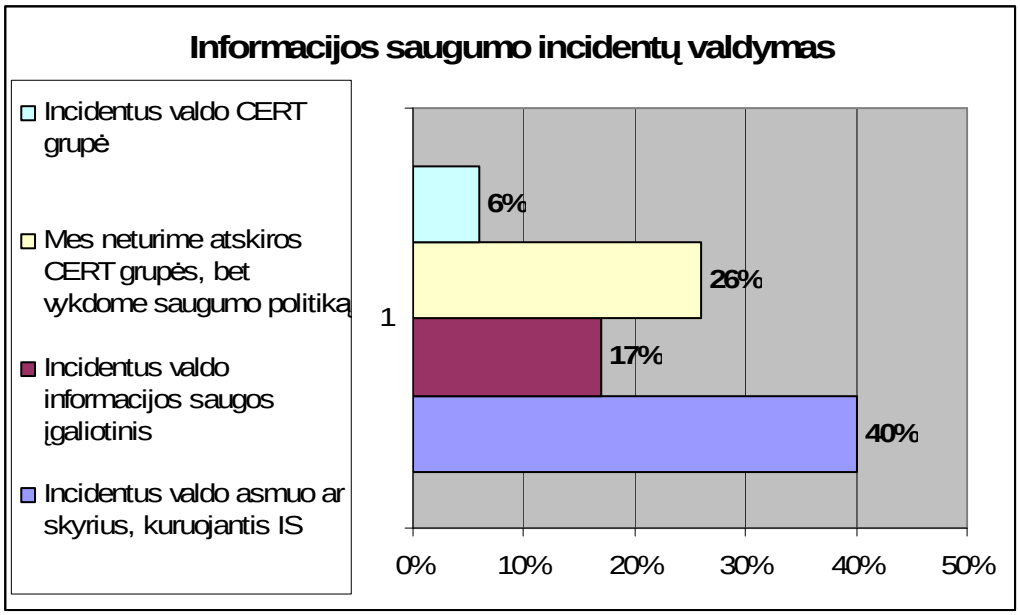
Dalis tyrime dalyvavusių viešojo ir privataus sektoriaus organizacijų nurodė, kad jų informacijos saugumu rūpinamasi keliais būdais – tai daro saugos įgaliotiniai arba informacines sistemas kuruojantis personalas, kompiuterinių nusikaltimų valdymo padaliniai, kartais šia sritimi rūpinasi visi išvardinti subjektai drauge.

Organizacijų, vykdančių informacijos saugumo politiką ir valdančių informacijos saugos incidentus, atsakymai į klausimą „Kaip Jūsų organizacijoje valdomi informacijos saugos incidentai?“ pasiskirstė sekančiai:

9 diagrama. Informacijos saugumo incidentų valdymas viešojo sektoriaus organizacijose



10 diagrama. Informacijos saugumo incidentų valdymas privataus sektoriaus organizacijose



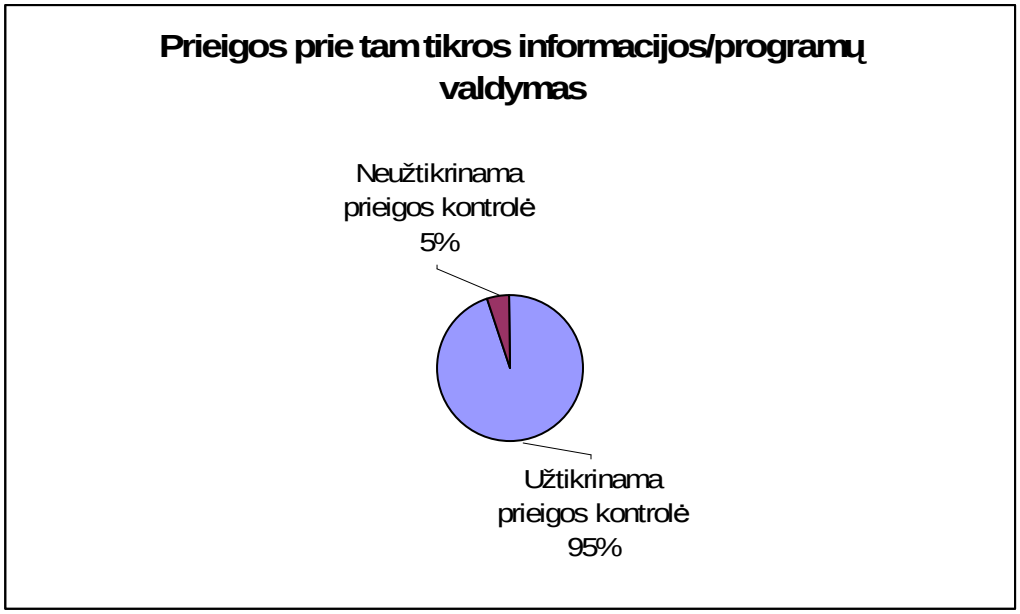
Atlikus informacijos saugumo incidentų valdymo priemonių palyginimą, pastebėta, kad informacijos saugumo incidentai viešojo sektoriaus organizacijose valdomi geriau – skiriami už tai atsakingi informacijos saugos įgaliotiniai (beveik pusėje tirtų atvejų), kartu su jais incidentus dažnai tiria ir už informacines sistemas atsakingi skyriai ar asmenys. 15% tyrime dalyvavusių viešųjų organizacijų atstovų pažymėjo, jog saugumo incidentai jų institucijose valdomi CERT grupių –

specializuotų reagavimo į informacijos saugumo incidentus padalinių, kurių pagrindinis tikslas yra operatyviai reaguoti į saugumo incidentus bei koordinuoti jų šalinimo veiksmus. Privačiame sektoriuje tuo tarpu vos kas dvidešimta organizacija turi tokias grupes ir patiriamų informacijos saugumo incidentų valdymą dažniausiai patiki skyriui ar asmeniui, atsakingam už informacines sistemas. Taigi, informacijos saugumo incidentų valdymui daugiau dėmesio skiriama viešąjame sektoriuje, kur yra sukurta daug specialių šią sritį kuruojančių pareigybių, kurias užima profesionalūs ir patyrę informacinio saugumo specialistai.

Beveik kiekviena šiuolaikinė organizacija, nesvarbu viešąjame ar privačiame sektoriuje dirbanti, savo veikloje naudoja slaptą bei konfidencialią informaciją. Tai pažymėjo 80% tyrime dalyvavusių privataus sektoriaus atstovų ir 61% valstybės institucijoje dirbantis informacijos saugumo specialistas. Tokiai informacijai apsaugoti naudojamos konfidencialumo sutartys. Jas pasirašo visi su konfidencialia informacija dirbantys tyrime dalyvavusių valstybės institucijų darbuotojai, tuo tarpu privataus sektoriaus – vos 74% su tokio pobūdžio informacija dirbantys asmenys. Apžvelgus darbą su slapta ir konfidencialia informacija viešąjame sektoriuje reglamentuojančius teisės aktus, buvo galima tikėtis, kad konfidencialumo sutartys bus pasirašomos visose su konfidencialia informacija dirbančiose valstybės institucijose. Privačiame sektoriuje situacija šiuo aspektu yra kiek kitokia – konfidencialumo sutartys yra viena iš rekomenduojamų priemonių slaptos informacijos apsaugojimui, dėl vienokių ar kitokių priežasčių šios sutartys pasirašomos ne visose įmonėse, kuriose naudojama slapta ar konfidenciali informacija. Apibendrintai galime teigti, kad konfidenciali informacija geriau yra apsaugota viešąjame sektoriuje.

Dar viena priemonė, galinti padėti išvengti nemalonių dėl informacijos saugumo incidentų kylančių pasekmių yra prieigos prie organizacijoje naudojamų informacijos resursų valdymas. Ši priemonė užtikrina, kad tam tikra informacija ar kompiuterinės programos organizacijoje prieinamos tik tiems asmenims ar asmenų, kurie yra įgalioti ir kuriems tokia informacija yra būtina jų pareigų vykdymui. Atlikus elektroninę informacijos specialistų apklausą paaiškėjo, jog prieigos kontrolės priemonė plačiau naudojama viešąjame (95% tirtų institucijų) negu privačiame (76%) sektoriuje. Net kas penktoje privačioje organizacijoje informacija, duomenimis ar kompiuterinėmis programomis gali naudotis visi įmonės darbuotojai. Tai iliustruoja sekančios dvi diagramos.

11 diagrama. Prieigos prie tam tikros informacijos valdymas valstybės institucijose



12 diagrama. Prieigos prie tam tikros informacijos valdymas interneto ir elektroninės prekybos bendrovėse

Vartotojų prieigos prie tam tikrų duomenų ir informacijos teisių valdymas yra viena labiausiai paplitusių organizacinių informacijos apsaugojimo priemonių. Dažnai įmonės vykdo ir vadinamąją „švaraus stalo“ bei „švaraus ekrano politiką“, kai ne darbo metu visa jautri informacija yra užrakinama, kompiuterinės programos išjungiamos, svarbūs dokumentai saugomi seifuose ir pan. Iš tyrime dalyvavausių valstybės institucijų „švaraus stalo politiką“ vykdo daugiau kaip pusė (t.y.

56%), o kalbant apie privataųjį sektorių – vos 28% tyrime dalyvavausių organizacijų. Išvada – jautrios ir svarbios informacijos apsaugai vienu paprasčiausiu ir pigiausiu būdu – laikantis tvarkos ir paliekant informaciją saugiai užrakintą – viešąjame sektoriuje skiriama daugiau dėmesio nei privačiąjame.

Norint tobulinti jau įdiegtas ir taikomas informacijos apsaugos priemones ir ateityje išvengti sunkių informacijos saugumo incidentų sukeltų padarinių, būtina nuolat tirti informacijos saugumo incidentus. Incidentų tyrimus atlieka už tai atsakingi asmenys, tai ilgas ir sudėtingas procesas, reikalaujantis ne tik už informacijos saugumą atsakingų darbuotojų atidumo, bet ir visų su informacija dirbančių organizacijos narių dėmesio. Kad incidentai būtų sėkmingai tiriami, svarbu, kad darbuotojai ne tik galėtų juos atpažinti, bet taip pat ir skubiai informuoti apie įvykusius incidentus atsakingus asmenis. Tai padėtų išvengti sunkesnių padarinių, sutrumpinti dėl incidentų prarandamą brangų darbo laiką, imtis didesnių saugumo priemonių. Todėl organizacijos vadovybė turėtų įpareigoti savo darbuotojus apie incidentus pranešti už informacijos saugą atsakingam personalui – informacinių sistemų skyriui, informacijos saugos įgaliotiniui ar reagavimų į kompiuterinius incidentus grupės nariams. Tačiau šią atsakingų už incidentus darbuotojų informavimo praktiką taiko ne visos tyrime dalyvavusios organizacijos – vėlgi priemonė labiau paplitusi viešojo sektoriaus organizacijose (78% tirtų atvejų darbuotojai yra įpareigoti pranešti apie įvykusį incidentą atsakingiems asmenims) negu privataus (54% tirtų atvejų). Iš šių rezultatų galima spręsti, kad informacijos incidentų analizei viešąjame sektoriuje skiriama daugiau dėmesio. Incidentų, jų priežasčių bei pasekmių analizė gali būti traktuojama kaip dar viena informacijos apsaugos priemonė, nes ji padeda išvengti panašių nutikimų ateityje.

Nustačius pagrindinius incidentus, su kuriais susiduria viešojo ir privataus sektoriaus darbuotojai, taip pat dažniausiai naudojamas informacijos saugos priemones, aptarus incidentų valdymą, darbą su konfidencialia informacija, atlikus bendrus palyginimus ir išvadas, tyrimo dalyvių buvo paprašyta ir išsakyti savo, kaip informacijos saugumo specialistų, nuomonę apie informacijos apsaugą jų organizacijose. Nuo žmonių, atsakingų už šią sritį organizacijoje, priklauso labai didelė dalis darbo kovojant su infomacijos saugumo problemomis, todėl kritiškas jų požiūris į jų pačių organizacijų saugumo padėtį verčia ieškoti naujų sprendimų, taikyti vis daugiau ir įvairesnių priemonių, kad būtų pasiektas aukštas informacinio saugumo lygis. Tyrimo metu nustatyta, kad palankiau organizacijos informacijos apsaugą vertina viešojo sektoriaus atstovai – 61% jų mano, kad informacija yra apsaugota gerai, likę – kad nepakankamai, tačiau nė vienas neatsakė, kad informacija apsaugota blogai. Privačiame sektoriuje taip teigiančių buvo – blogą informacijos apsaugojimą jų organizacijoje deklaravo 7% respondentų, 52% manė, kad informacija

apsaugota gerai, likę – kad nepakankamai. Sprendžiant iš tyrimo rezultatų galime teigti, kad iš tiesų informacinis turtas viešojo sektoriaus organizacijose yra saugesnis.

Vienas iš atvirųjų tyrimo klausimų buvo skirtas sužinoti informacijos saugumo specialistų nuomonę apie tai, kodėl informaciją reikia saugoti. Į šį klausimą sau turėtų atsakyti kiekvienas, dirbantis su informacija. Apsaugos būtinybė buvo motyvuojama labai įvairiai, pagrindiniai motyvai, kodėl būtina saugoti informaciją, pateikiami 3 lentelėje:

3 lentelė. Priežastys, kodėl būtina saugoti informaciją, kurias nurodė viešojo ir privataus sektoriaus organizacijos

Viešasis sektorius	**Privatusis sektorius**
• kad išvengtumėme nuostolių;	• nes apsauga padeda apginti savo ir klientų interesus;
• būtina vadovautis asmens duomenų apsaugos įstatymu;	• nes informacija kainuoja;
• reglamentavus informacijos saugumą stiprėja vidaus kontrolė;	• informacija yra organizacijos turtas ir nuosavybė;
• nes tokios yra bendros saugumo rekomendacijos;	• informacijos apsauga užtikrina finansinį saugumą;
• kad nenukentėtų įmonės politika;	• nuo to priklauso, kaip patenkinami klientai, jų konfidencialumas;
• nes informacija - tai turtas, todėl sukuria motyvaciją juo pasinaudoti, sugadinti, piktnaudžiauti ir pan.	• kad įmonė nepatirtų bankroto;
• nes informacijos sauga yra viena iš pagrindinių problemų šiuolaikinėje visuomenėje;	• kad ji nebūtų panaudota trečiųjų asmenų;
• nes privalu laikytis įstatymų;	• nes informacija - tai turtas;
• informacija - turtas, o turtą reikia saugoti;	• kad būtų išvengta finansinių nuostolių;
• informacijos konfidencialumas įpareigoja ją saugoti;	• nes informacija yra organizacijos turtas ir darbo pagrindas;
• nes didelė dalis informacijos yra viešai neskelbtina, būtina nepertraukiamam ir kokybiškam organizacijos darbui.	• būtina užtikrinti, kad informacija nepakliūtų į svetimas rankas ir nepadarytų žalos organizacijai.

Iš pateiktų atsakymų matyti, kad kai kurie motyvai sutampa – tiek viešojo, tiek privataus sektoriaus atstovai teigė, kad informacija yra turtas ir organizacijos nuosavybė, jos gavimu, apdorojimu, perdavimu, saugojimu yra paremta daugelio įmonių veikla. Dauguma viešojo sektoriaus atstovų apsaugos būtinybę motyvavo tuo, kad ši sritis yra reglamentuota įstatymais, o įstatymų privalu laikytis. Daugelis respondentų, dirbančių viešąjame sektoriuje, pastebėjo ir tai, kad

užtikrinus saugų, nepertraukiamą informacinių sistemų darbą organizacijoje, stiprėja ir vidaus procesų kontrolė. Privataus sektoriaus atstovai, kaip ir buvo tikėtasi, saugumo būtinybę motyvuoja pagrinde finansais, informacinį saugumą netgi prilygina finansiniam saugumui ir stabilumui. Taip pat dažnai buvo minima, kad informacija turi būti apsaugota ir nepatekti konkurentams bei trečiosioms šalims į rankas, nes jau teorinėje dalyje buvo kalbėta apie tai, kad saugi verslo informacija ir įvairios komercinės paslaptys dažnai užtikrina konkurencinį pranašumą šiuolaikiniame verslo pasaulyje.

Kiekybinio tyrimo metu nustačius pagrindinius skirtumus tarp viešojo ir privataus sektoriaus informacinio saugumo srityje, teorinėje ir praktinėje darbo dalyje konstatavus, kodėl reikia saugoti informaciją, liko neatsakytas dar vienas labai svarbus klausimas – kokios priežastys trukdo tinkamai spręsti informacijos saugumo problemas šiuolaikinėje organizacijoje? Į šį klausimą atsakymų ieško daugelio saugumo tema parašytų straipsnių autoriai. Surengtos kiekybinės apklausos dalyviai – tiek privataus, tiek viešojo sektoriaus atstovai – buvo panašios nuomonės šiuo klausimu. 58% viešojo sektoriaus atstovų ir 61% privačiame sektoriuje dirbantis respondentas pastebėjo, kad tinkamai informacijos saugumu rūpintis trukdo gerų šios srities specialistų trūkumas. Atsakingais už informacijos saugą, vieną iš esminių ir sėkmingam organizacijos darbui būtinų faktorių, turi būti skiriami kompetetingi, patyrę darbuotojai, turintys ne tik praktinių, bet ir teorinių šios srities žinių. Daudelis organizacijų vadovų pasitiki savo už informacines technologijas, sistemos ir informacijos saugą atsakingais darbuotojais ir šie dažniausiai formuoja poreikius bei reikalavimus informacijos apsaugos priemonėms. Deja tikrai ne visos organizacijos gali pasigirti kompetetingais šios srities darbuotojais, kurie gerai suvoktų informacinio saugumo srities subtilybes ir, kas yra svarbiausia, gebėtų turimas žinias gerai pritaikyti.

Tačiau tai nėra vienintelė priežastis, dėl kurios informacijos saugumas daugelyje organizacijų nėra pilnai užtikrintas. Daugelis vis dar nemano, kad tai sritis, į kurią vertėtų investuoti ar skirti pernelyg didelį dėmesį – net 38% valstybės institucijų informacijos saugos specialistų ir 45% jų kolegų iš privataus sektoriaus teigė, kad šiai sričiai organizacijose nėra skiriama pakankamai lėšų. Nepakankamas lėšų informacijos saugumui užtikrinti skyrimas tik dar kartą įrodo, kad dauguma organizacijų vis dar nesuvokia informacinio turto vertės ir yra siejamas su nepakankamai rimtu požiūriu į šią sritį. Juk daugelis kompanijų ar įstaigų vadovų informacijos apsaugą laiko antraeiliu dalyku, kurio investicijos neatsiperka.

3.3. Tyrimo išvados

Šiame darbe buvo iškelta informacijos ir informacinio turto saugos problema, kuri teorinėje darbo dalyje buvo aprašyta įvairių literatūros šaltinių pagalba, o praktinėje dalyje – įrodyta įvykdyto kiekybinio tyrimo metu. Buvo nustatyta, kad saugos problema egzistuoja tiek viešąjame, tiek privačiame sektoriuje, kad informaciniam turtui nuolat kyla įvairių grėsmių, kurių pasekoje vyksta saugumo incidentai bei patiriama tiek finansinė, tiek moralinė žala.

Informacijos saugos problemą organizacijose, veikiančiose privačiame ir viešąjame sektoriuje, sąlygoja daugelis veiksnių – tai ir naudojamos arba nenaudojamos informacijos apsaugos priemonės, vykdomos ar nevykdomos saugos politikos, požiūris į informacinį turtą ir jo apsaugos problematiką, šios srities specialistų trūkumas ir daugelis kitų. 4 lentelėje pateikiamos tyrimo metu identifikuotos pagrindinės viešąjame ir privačiame sektoriuje egzistuojančios informacijos saugos problemos, taip pat galimos jų priežastys bei galimi šių problemų sprendimo būdai.

4 lentelė. Identifikuotų informacijos saugos problemų sprendimo būdai viešąjame sektoriuje

Egzistuojanti problema	**Galimos problemos priežastys**	**Problemos sprendimas**
Viešasis sektorius		
1. Nuolat susiduriama su įvairiais informacijos saugumo incidentais.	1. Skiriama per mažai dėmesio, lėšų ir pastangų pakankamam informacijos saugos lygiui užtikrinti.	1. Didesnis vadovybės ir kiekvieno darbuotojo dėmesys saugumo problemai, pakankamas lėšų informacijos saugumo priemonėms įsigyti skyrimas, atsakingų darbuotojų skyrimas, saugumo politikos tikslų siekimas.
2. Didžiausia grėsmę informacijos saugumui kelia nepageidaujami elektroniniai laiškai ir kompiuteriniai virusai.	2. Nepakankamas antivirusinių programų ir nepageidaujamų elektroninių laiškų blokavimo programų diegimas.	2. Nuolatinis antivirusinių pogramų ir spam blokavimo programų atnaujinimas ir diegimas visuose organizacijos kompiuteriuose.
3. Duomenų vagystės.	3. Nepakankamai kontroliuojama prieiga prie informacijos resursų, nepakankamai diegiamos ugniasienės, nepatikimi darbuotojai, nesaugus tinklas.	3. Griežtesnė prieigos kontrolė, ugniasienių diegimas, atsarginių kopijų darymas, vidinio ir išorinio tinklo apsauga, patikimų darbuotojų samdymas, konfidencialumo sutarčių sudarymas.
4. Pasitaikantys netyčiniai duomenų sugadinimo ir kompiuterių vagysčių atvejai.	4. Nepakankamai atidūs darbuotojai, neužtikrinta fizinė informacinio turto apsauga.	4. Darbuotojų atidumo ir kruopštumo ugdymas, aukšto fizinio informacijos saugumo lygio užtikrinimas, atsarginių kopijų darymas.
5. Kas dešimtoje institucijoje nėra vykdoma informacijos saugumo politika.	5. Neįvertinama informacijos saugumo problema ir grėsmės bei rizikos informaciniam turtui.	5. Informacijos rizikų vertinimas, saugumo politikos ir tikslų nusistatymas.

6. Nepakankamai vykdoma "švaraus stalo" ir "saugaus ekrano" politika.	6. Nepakankamas darbuotojų sąmoningumas informacijos saugumo klausimu, nepakankamas organizacinių ir techninių priemonių diegimas.	6. Nuolatinis darbuotojų sąmoningumo skatinimas, platesnis organizacinių bei techninių priemonių taikymas.
7. Nepakankamas už informacijos saugą atsakingų darbuotojų informavimas apie vykstančius saugumo incidentus.	7. Nepakankamas arba ne visų darbuotojų supažindinimas su reikalavimu informuoti atsakingus asmenis apie saugumo incidentus.	7. Organizacijos darbuotojų supažindinimas su reikalavimu informuoti atsakingus asmenis apie vykstančius informacijos saugumo incidentus. Darbuotojų sąmoningumo skatinimas.
8. Gerų informacijos saugos specialistų trūkumas.	8. Nepakankamas informacijos saugos specialistų ruošimas, mažos investicijos į saugos specialistų kvalifikacijos kėlimo kursus, įvairius apmokymus.	8. Nuolatinis saugos specialistų tobulinimas siunčiant į kvalifikacijos kėlimo kursus, gerų specialistų paieška.
9. Nepakankamas lėšų informacijos apsaugai užtikrinti skyrimas.	9. Informacinio turto grėsmių neįvertinimas, nepakankamas vadovybės sąmoningumas informacijos saugos atžvilgiu.	9. Informacijos grėsmių ir pažeidžiamumų įvertinimas, realios padėties informacijos saugumo srityje suvokimas.

5 lentelė. Identifikuotų informacijos saugos problemų sprendimo būdai privačiame sektoriuje

Egzistuojanti problema	**Galimos problemos priežastys**	**Problemos sprendimas**
Privatus sektorius		
1. Dažnai susiduriama su įvairiais informacijos saugumo incidentais.	1. Skiriama per mažai dėmesio, lėšų ir pastangų pakankamam informacijos saugos lygiui užtikrinti.	1. Didesnis dėmesys informacijos saugumo problemai, pakankamas lėšų informacijos saugumo priemonėms įsigyti skyrimas, atsakingų darbuotojų skyrimas, saugumo politikos organizacijoje įvedimas ir įgyvendinimas..
2. Didžiausia grėsmę informacijos saugumui kelia nepageidaujami elektroniniai laiškai, kompiuteriniai virusai ir duomenų vagystės.	2. Nepakankamas organizacinių, techninių ir fizinių informacijos apsaugos priemonių diegimas.	2. Nuolat kompleksiškai diegti ir atnaujinti organizacines, technines ir fizines informacijos apsaugos priemones.
3. Į kas dešimtos organizacijos informacinį turtą kėsinamasi įsilaužus į organizacijos kompiuterius.	3. Nepakankamai apsaugotas tinklas, nepakankamas ugniasienių ir kitų priemonių diegimas.	3. Priemonių, užtikrinančių organizacijos informacinių sistemų ir tinklo apsaugą, diegimas bei nuolatinis informacijos rizikos vertinimas.
4. Silpni slaptažodžiai, kontroliuojant prieigą prie tam tikros informacijos ir duomenų.	4. Nepakankama slaptažodžių kontrolė.	4. Griežtesnės slaptažodžių kontrolės įvedimas, ypatingą dėmesį atkreipiant į jų ilgį, keitimo periodiškumą, tvarkymą.
5. Nepakankamas apsaugos nuo nepageidaujamų elektroninių laiškų užtikrinimas.	5. Ne visose organizacijose, kuriose susiduriama su nepageidaujamais elektroniais laiškais, diegiamos tokių laiškų blokavimo priemonės.	5. Kova su nepageidaujamais elektroniniais laiškais diegiant jų blokavimo programas, pavojingų laiškų turinio neatidarymas ir trynimas.

6. Nepakankamai tikslingas ir komplesiškas informacijos apsaugos priemonių diegimas.	6. Neįvertinamos realios informacijos grėsmės ir pažeidžiamumai, pernelyg pasitikima turimomis informacijos apsaugos priemonėmis, nors jos ir negali užtikrinti pakankamai aukšto informacijos apsaugos lygio.	6. Priemonių, skirtų kovoti su kylančiais incidentais ir esančiomis grėsmėmis skyrimas, tikslingas ir kompleksiškas apsaugos priemonių diegimas.
7. Dėl nuolat vykstančių informacijos saugumo incidentų organizacijos patirią žalą - moralinę, finansinę ir kt.	7. Neužtikrinamas pakankamas informacinio turto apsaugos lygis, dėl to nuolat patiriami įvairūs nuostoliai.	7. Apsaugos priemonių kompleksinis taikymas, leisiantis užtikrinti pakankamai aukštą informacijos apsaugos lygį ir išvengti nuolatinių nuostolių.
8. Net kas penktoje organizacijoje nėra vykdoma informacijos saugos politika.	8. Organizacijos nesuvokia rizikų ir grėsmių, kylančių organizacijoje cirkuliuojančiai informacijai.	8. Atlikus rizikų ir informacijos pažeidžiamumų analizę nusistatyti informacijos saugos tikslus, nuostatas ir politikas bei jas įgyvendinti.
9. Nepakankamas informacijos saugumo incidentų valdymas ir kontrolė.	9. Už saugumo incidentus atsakingų darbuotojų trūkumas, incidentų keliamų grėsmių neįvertinimas.	9. Už informacijos saugą atsakingo personalo skyrimas, saugumo politikos vykdymas, ypatingą dėmesį skiriant saugumo incidentų valdymui bei kontrolei.
10. Nepakankamai apsaugota konfidenciali organizacijų informacija.	10. Pernelyg pasitikima organizacijos darbuotojais ir nepakankamai pasirašomos konfidencialumo sutartys.	10. Visose organizacijose, kuriose dirbama su konfidencialia informacija, turi būti pasirašomos konfidencialumo sutartys, numatančios atsakomybę už konfidencialios informacijos paviešinimą.
11. Nepakankamas prieigos kontrolės prie informacinių resursų valdymas.	11. Nepakankamas grėsmių, kurios gręsia nekontroliuojant prieigos prie informacijos ir duomenų, įvertinimas. Pernelyg didelis pasitikėjimas organizacijos darbuotojais.	11. Kontrolė, kas ir dėl kokių tikslų naudojasi organizacijos informacija. Slaptažodžių sistemos diegimas.
12. Nepakankamai vykdoma "švaraus stalo" ir "saugaus ekrano" politika.	12. Nepakankamas darbuotojų sąmoningumas informacijos saugumo klausimu, nepakankamas organizacinių ir techninių priemonių diegimas.	12. Nuolatinis darbuotojų sąmoningumo skatinimas, platesnis organizacinių bei techninių priemonių taikymas.
13. Nepakankamas už informacijos saugą atsakingų darbuotojų informavimas apie vykstančius saugumo incidentus.	12. Nepakankamas arba ne visų darbuotojų supažindinimas su reikalavimu informuoti atsakingus asmenis apie saugumo incidentus.	12. Organizacijos darbuotojų supažindinimas su reikalavimu informuoti atsakingus asmenis apie vykstančius informacijos saugumo incidentus. Darbuotojų sąmoningumo skatinimas.
14. Gerų informacijos saugos specialistų trūkumas.	14. Nepakankamas informacijos saugos specialistų ruošimas, mažos investicijos į saugos specialistų kvalifikacijos kėlimo kursus, įvairius apmokymus.	14. Nuolatinis saugos specialistų tobulinimas siunčiant į kvalifikacijos kėlimo kursus, gerų specialistų paieška.
15. Nepakankamas informacijos saugumo problemos įvertinimas.	15. Neįvertinama, jog informacinis turtas yra brangesnis už materialųjį ir gali suteikti pranašumų konkurencinėje kovoje.	15. Didesnis dėmesys informaciniam turtui kaip konkurencinei priemonei ir kaip visam kitam organizacijos turtui.

Apibendrinant tyrimo rezultatus galima pastebėti, jog privataus sektoriaus organizacijose buvo identifikuota beveik du kartus daugiau problemų nei viešojo sektoriaus organizacijose, tačiau problema, kaip užtikrinti tinkamą informacijos apsaugos lygį, egzistuoja visose organizacijose, neatsižvelgiant į jų veiklos sektorių. Visgi pagrindinės problemos prasideda tada, kuomet nesuvokiama arba neįvertinama informacijos ir informacinio turto nauda bei teikiami pranašumai, kuomet saugumui neskiriama dėmesio nei vadovybės, nei eilinių darbuotojų lygmeniu. Informacijos sauga organizacijose turi būti užtikrinama įvairiomis priemonėmis, jas pasirenkant pagal egzistuojančias rizikas ir grėsmes, o dirbti saugios informacijos labui turi kiekvienas – ir informacijos bei duomenų saugos specialistas, ir informacinių sistemų kuratorius, taip pat organizacijų vadovai bei kiekvienas organizacijos darbuotojas. Kaip jau buvo ne kartą minėta – informacijos saugumas yra nuolatinis procesas, reikalaujantis kasdienės priežiūros, vis modernesnių priemonių ir vis didesnių pastangų.

IŠVADOS

Šio magistrinio darbo tema – „Informacijos sauga viešąjame ir privačiame sektoriuje“. Informacijos ir duomenų apsauga yra vienas aktualiausių klausimų šiandieniniame informacijos ir naujausių technologijų pasaulyje, su kuriuo susiduria daugelis tiek viešąjame, tiek privačiame sektoriuje dirbančiųjų.

Šiuo metu visuomenėje vykstantys informaciniai procesai be naujų galimybių atnešė ir problemų, kurių viena svarbiausių – informacijos apsaugos problema. Kasdieniniame darbe organizacijos naudoja įvairiausius informacijos šaltinius, informaciją ne tik gauna, bet nuolat su ja dirba, perduoda, saugo ar sunaikina. Šiame informacijos cikle priklausomai nuo organizacijos veiklos sričių informaciniam turtui iškyla įvairiausių pavojų, grėsmių ir rizikų. Todėl kylančių pavojų įvairiapusiškumas verčia susimąstyti, kad informacijai apsaugoti neužtenka tik įdiegti tam tikras kompiuterines programas. Aukštam informacijos saugos lygiui užtikrinti reikia kompleksiškai taikyti įvairiausias priemones, nuolat jas peržiūrėti ir tobulinti.

Atlikus literatūros informacijos saugumo tematika analizę, kiekybinio tyrimo metu ištyrus ir nustačius pagrindines informacijos saugos tendencijas viešąjame ir privačiame sektoriuje, buvo prieita prie tokių išvadų:

- Informacijos saugumo problema egzistavo ir seniau, telefono, telegrafo sistemose, tačiau didžiąją dalį informacijos perkėlus į elektroninį erdvę ji tapo ypač opi ir aktuali. Šios problemos egzistavimas buvo įrodytas tiek įvairių literatūros šaltinių, rinkos tyrimų bei teisės aktų analizėje, tiek atliktame kiekybiniame tyrime – informacijos ir informacijos saugos specialistų apklausoje;
- Remiantis šiame darbe iškelta informacijos apsaugos problema, kuri buvo įrodyta tiek praktinėje, tiek teorinėje darbo dalyje, buvo nustatyta, kad aukštam informacijos saugos lygiui užtikrinti neužtenka tik paparasčiausių apsaugos priemonių, o būtina kompleksiškai taikyti ne tik technines, bet ir fizines bei organizacines apsaugos priemones;
- Darbo metu buvo nustatyta, kad informacijos ir informacinios turto saugumas organizacijai suteikia konkurencinį pranašumą, geresnį pelningumą, garantuoja teisinę atitiktį, padeda išsaugoti gerą organizacijos įvaizdį;
- Teisinių aktų analizės metodu teorinėje darbo dalyje buvo nustatyta, kad informacijos saugumo sritis viešąjame sektoriuje, skirtingai nei privačiąjame, yra stipriai teisės aktais reglamentuota sritis, o vienas pagrindinių šių teisės reikalavimų viešosioms organizacijoms

yra už informacijos saugą atsakingų darbuotojų skyrimas, ypač palengvinantis informacijos saugos politikos organizavimą įstaigoje;

- Privataus sektoriaus organizacijose, kaip parodė literatūros šaltinių analizė, informacinis turtas sudaro didžiąją dalį pačių organizacijų vertės, įvairios komercinės paslaptys ir konfidenciali informacija leidžia privačioms organizacijoms tinkamai konkuruoti bei varžytis konkurencingame verslo pasaulyje bei išsikovoti lyderio pozicijas;
- Privataus sektoriaus informacijos ir duomenų saugumas, nors ir ne taip plačiai kaip viešojo, reglamentuotas teisės aktais ir nutarimais, kuriuose įpareigojama saugoti konfidenciali organizacijos informacija, komercines bei technologines įmonės paslaptis, be leidimo ar netinkamai nenaudoti asmens duomenų, nepažeisti galiojančių autorių ir gretutinų teisių;
- Atlikus kiekybinį tyrimą buvo patvirtinta darbo pradžioje iškelta hipotezė, kad informacijos apsaugos problema egzistuoja tiek privataus, tiek viešojo sektoriaus organizacijose, kuriose nuolat susiduriama su informacijos saugumo incidentais, o didžiausią grėsmę abiejų sektorių informacijos saugumui kelia nepageidaujami elektrininiai laiškai, kompiuteriniai virusai ir duomenų vagystės.
- Tyrimo metu nustatyta, kad visos organizacijos vienokiomis ar kitokiomis priemonėmis kovoja su informacijos saugumo incidentais. Tačiua viešojo sektoriaus organizacijose informacijos apsaugojimo priemonės naudojamos kompleksiškiau ir tikslingiau nei privačiojo, atsižvelgdamos į realias kylančias grėsmes;
- Tiek teorinėje darbo dalyje, tiek atlikto kiekybinio tyrimo metu buvo nustatyta, kad dauguma tiek viešojo, tiek privataus sektoriaus organizacijų patiria vienokią ar kitokią (nuo moralinės iki finansinės) žalą dėl nuolat kylančių informacijos saugumo incidentų;
- Praktinio tyrimo metu buvo atsakyta į darbo pradžioje kilusį klausimą apie tai, ar skirtingas viešojo ir privataus sektoriaus informacijos saugumo srities reglamentavimas įtakoja skirtingą praktinį informacijos apsaugos lygį organizacijose. Viešosiose organizacijose informacijos saugumui skiriamas didesnis dėmesys ir rūpestis, nes čia privaloma ne tik skirti ypatingą dėmesį informacinio turto apsaugojimui, bet ir nuolat vykdyti informacijos saugos politiką, skatinti darbuotojų sąmoningumą šiuo klausimu ir pan.

Galima teigti, kad teisinis reglamentavimas yra viena veiksmingiausių priemonių užtikrinant informacijos saugumą. Tyrimo metu surinkti duomenys įrodė, kad toje organizacija, kurioje egzistuoja informacijos saugumo politika, visiems darbuotojams yra paskelbtos saugumo taisyklės, kurioje dirba už informacijos saugą paskirti asmenys, patiria mažiau žalos, praranda mažiau laiko informacijos saugumo incidentų padarinių likvidavimui.

Taigi, šio darbo metu buvo nustatyta, kad informacijos saugumo problema yra aktuali šiuolaikinėje visuomenėje, taip pat ji neaplenkia ir viešojo bei privataus sektoriaus organizacijų, kurios nulat susiduria su įvairiomis informacijos saugumo grėsmėmis, todėl yra priverstos imtis kompleksiškų priemonių informacijos saugai užtikrinti. Galima teigti, kad darbo pradžioje iškelta hipotezė yra teisinga.

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS

1. ABRAITIS, Vaidotas Blažiejus. *Informacijos privatumas ir sauga Lietuvos internete* [interaktyvus]. [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: <http://www.leidykla.vu.lt/inetleid/inf-mok/23/str2.html>.
2. ALLEN, H. Julia. *The Art of Information Security Governance* [interaktyvus]. Carnegie Mellon University, 24 February 2008 [žiūrėta 2008 m. kovo 2 d.]. Prieiga per internetą: <http://www.cert.org/archive/pdf/QISF_Allen_022408.pdf>.
3. BALTIC CONSULTING GROUP. *Įmonės informacija – nesaugomas turtas* [interaktyvus]. 2007 m. gruodžio 25 d. [žiūrėta 2008 m. kovo 2 d.]. Prieiga per internetą: <http://www.elektronika.lt/articles/computers/10073/>.
4. E-SAUGUMAS. *Bendroji informacija* [interaktyvus], [žiūrėta 2008 m. kovo 10 d.]. Prieiga per internetą: <http://www.esaugumas.lt/index.php?-2028849800>.
5. EUROPOS KOMISIJA. *Komisijos komunikatas Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų ir regionų komitetui. Saugio informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“* [interaktyvus]. Briuselis, 2006 m. gegužės 13 d. [žiūrėta 2007 m. gruodžio 18 d.]. Prieiga per internetą: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:LT:HTML>.
6. GIEDRAITIS, Vilius. *Informacijos apsaugos kompiuterių tinkluose problemos*. Iš *Informacijos mokslai*, 1998, Nr. 9, p. 103 - 106.
7. LIETUVOS RESPUBLIKOS KONKURENCIJOS TARYBA. *Lietuvos Respublikos konkurencijos įstatymas* [interaktyvus]. Vilnius, 1999 m. kovo 23 d., Nr. VIII – 1099 [žiūrėta 2008 m. kovo 12 d.]. Prieiga per internetą: <http://www.konkuren.lt/konkurencija/istatymas/htm>.
8. LIETUVOS RESPUBLIKOS SEIMAS. *Lietuvos Respublikos elektroninės prekybos įstatymas* [interaktyvus], [žiūrėta 2008 m. kovo 12 d.]. Prieiga per internetą: <http://www3.lrs.lt/docs3/kad4/W3_VIEWER.ViewDoc-p_int_tekst_id=7680&p_int_tv_id=855&p org=0.htm>.
9. LIETUVOS RESPUBLIKOS SEIMAS. *Lietuvos Respublikos akcinių bendrovių įstatymas* [interaktyvus]. Vilnius, 2000 m. liepos 13 d., Nr. VIII – 1835 [žiūrėta 2008 m. kovo 17 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=224405> .
10. LIETUVOS RESPUBLIKOS SEIMAS. *Lietuvos Respublikos darbo kodeksas* [interaktyvus]. Vilnius, 2002 m. birželio 4 d., Nr. IX – 926 [žiūrėta 2008 m. sausio 11 d.]. Prieiga per internetą: <http://www.skelbimas.lt/istatymai/darbo_kodeksas.htm>.

11. LIETUVOS RESPUBLIKOS SEIMAS. *Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas* [interaktyvus]. Vinius, 1996 m. birželio 11 d., Nr. I – 1374 [žiūrėta 2008 m. kovo 15 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=231799>.
12. LIETUVOS RESPUBLIKOS SEIMAS. *Autorių teisių ir gretutinių teisių įstatymas* [interaktyvus]. Vilnius, 1999 m. gegužės 18 d., Nr. VIII – 1185 [žiūrėta 2008 m. kovo 15 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=207199>.
13. LIETUVOS RESPUBLIKOS SEIMAS. *Lietuvos Respublikos elektroninių ryšių įstatymas* [interaktyvus]. Vilnius, 2004 m. birželio 5 d. [žiūrėta 2008 m kovo 19 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=232036>.
14. LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJA. *Rizikos analizės vadovas* [interaktyvus]. 2005 m., ISBN 5-415-01827-1. [žiūrėta 2008 m. vasario 25 d.]. Prieiga per internetą: <http://www.vrm.lt/fileadmin/Padaliniu_failai/ Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf>.
15. LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJA. *Informacijos sauga valstybės institucijų ir įstaigų darbuotojams* [interaktyvus]. 2005 m. [žiūrėta 2008 m. kovo 22 d.]. Prieiga per internetą: <http://web.esaugumas.lt/VRM/pdf/12_skyrius.pdf>.
16. LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJA. *Rizikos analizės atsakaita* [interaktyvus]. 2006 m. [žiūrėta 2008 m. sausio 12 d.]. Prieiga per internetą: <http://www.vrm.lt/uploads/media/Rizikos_analizes_ataskaita.pdf>.
17. LIETUVOS RESPUBLIKOS VYRIAUSYBĖ. *Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo* [interaktyvus]. Vilnius, 2001 m. gruodžio 22 d., Nr. 1625 [žiūrėta 2008 m. kovo 22 d.]. Prieiga per internetą: <http://www.ivpk.lt/teises_aktai/files/22.pdf>.
18. LIETUVOS STANDARTIZACIJOS DEPARTAMENTAS. *Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 17799:2005). Lietuvos standartas*. 2006 m., p. 7 – 54.
19. LUČINSKIJ, Miroslav. *Duomenų saugos pradmenys*. Kaunas, 2007 m., p. 18 – 19.
20. LUČIŪNAS, Audrius. *Informacijos apsaugos brandos lygiai* [interaktyvus]. 2007 m. spalio 8 d. [žiūrėta 2008 m. kovo 1 d.]. Prieiga per internetą: <http://www.informacijosapsauga.lt/uncategorized/informacijos-apsaugos-brandos-lygiai/>.
21. MATELIS, Stasys. *Intelektualios informacijos apsauga įmonėse* [interaktyvus]. [žiūrėta 2008 m. kovo 11 d.]. Prieiga per internetą: <http://www.esecurity.lt/article/1322.html>.

22. MIKALAJŪNIENĖ, Edita. *Asmens duomenų apsauga tiesioginėje rinkodaroje* [interaktyvus]. [žiūrėta 2008 m. sausio 22 d.]. Prieiga per internetą: <http://www.ada.lt/images/cms/File/pranesimas_rinkodara.doc>.
23. RYŠIŲ REGULIAVIMO TARNYBA. [interaktyvus]. [žiūrėta 2008 m. kovo 2 d.]. Prieiga per internetą: <http://www.rrt.lt/>.
24. ŠERPENSKAS, Eimantas. *Informacijos apsauga Lietuvoje*. Iš *Informacijos mokslai*. 2001 m., Nr. 18, p. 110 – 115.
25. ŠIMKŪNAS, Mindaugas. *Komercinės paslaptys – konkurencinio pranašumo priemonė* [interaktyvus]. 2004 m. balandžio 22 d. [žiūrėta 2008 m. vasario 28 d.]. Prieiga per internetą: <http://www.verum.lt/view.php?id=149&lg=LT>.
26. *Valstybės žinios. Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos*. Vilnius, 2006 m. birželio 22 d., Nr. 70-2575.
27. *Valstybės žinios. Informacinių technologijų saugos atitikties vertinimo metodika*. Vilnius, 2004 m. gegužės 14 d., Nr. 80-2855.
28. *Valstybės žinios*. *Dėl Elektroninės informacijos saugos koordinavimo komisijos sudarymo ir jos nuostatų patvirtinimo*. Vilnius, 2006 m. gruodžio 16 d., Nr. 137-5224.
29. VENČKAUSKAS, Algimantas. *Įmonės informacinės saugos efektyvumo vertinimas*. Iš *Informacijos mokslai*. 2003 m., nr. 26, p. 91 - 93.
30. VENCKAUSKAS, Algimantas, ŠERPENSKAS, Eimantas. *Grupinio darbo sistemų saugumo problemos.* Iš *Informacinės technologijos‘ 99.* Kaunas, 1999 m., p. 67 – 69.
31. ŽIOBIENĖ, Edita. *Informacijos apie privatų asmens gyvenimą apsauga.* Vilnius, 2003 m., p. 12 – 49.

1 priedas – kiekybinio tyrimo anketos pavyzdys

1. Kur Jūs dirbate?
a) privačiame sektoriuje
b) viešąjame sektoriuje
2. Koks Jūsų organizacijos dydis?
a) 1 – 10 darbuotojų
b) 10 – 20 darbuotojų
c) Daugiau negu 20 darbuotojų
3. Ar Jūsų organizacijoje susiduriama su informacijos saugumo incidentais?
a) taip
b) ne
4. Su kokiais išvardintais informacijos saugumo incidentais susiduriama Jūsų organizacijoje?
a) kompiuteriniais virusais
b) nepageidaujamais elektroniniais laiškais (angl. spam)
c) duomenų vagystėmis (angl. fishing)
d) įsilaužimais į įmonės kompiuterius
e) įmonės darbuotojų piktavališkais veismais vietiniame tinkle
5. Su kokiais incidentais, kurie nebuvo paminėti, susiduriama taip pat?
6. Kokios iš žemiau išvardintų priemonių naudojamos Jūsų organizacijoje informacijos saugumui užtikrinti?
a) nuolat atnaujinamos operacinės sistemos
b) antivirusinės programos
c) programinė įranga prieš šnipinėjimo programas
d) nepageidaujamų elektroninių laiškų blokavimo priemonės
e) užkardos (angl. firewall)
f) daromos atsarginės duomenų kopijos
g) saugomi sistemos įrašai apie vartotojų darbą
7. Kokias priemones, kurios nebuvo paminėtos, naudojate taip pat?
8. Žala, kurią Jūsų organizacija patyrė dėl iškilusių informacijos saugumo incidentų?
a) sugadinta programinė įranga
b) sugadinta kompiuterinė įranga
c) sutriko organizacijos veikla
d) organizacija patyrė materialinę žalą
e) buvo pavogti konfidencialūs duomenys
f) organizacija žalos nepatyrė
9. Kokios žalos, be išvardintos, organizacija patyrė dar?
10. Kaip Jūsų organizacijoje valdomi informacijos saugumo incidentai?
a) incidentus valdo CERT (kompiuterinių incidentų tyrimo) grupė
b) mes neturime atskiros CERT grupės, tačiau vykdome informacijos saugos politiką
c) mūsų organizacijoje dirba informacijos saugo įgaliotinis, užsiimantis visais informacijos saugumo klausimais
d) informacijos saugumo incidentus valdo asmuo, kuruojantis informacines sistemas
e) mūsų organizacijoje nėra vykdoma informacijos saugumo politika
11. Ar Jūsų organizacijoje dirbama su konfidencialia informacija?
a) taip
b) ne
12. Ar su konfidencialia informacija dirbantys asmenys pasirašo konfidencialumo sutartis?

a) taip
b) ne

13. Ar Jūsų organizacijoje užtikrinta, kad prie tam tikros informacijos prieitų tik tam įgaliojimų turintys asmenys?

a) taip
b) ne

14. Kaip manote, informacija Jūsų darbovietėje yra:

a) gerai apsaugota
b) nepakankamai apsaugota
c) visiškai neapsaugota

15. Kodėl, Jūsų nuomone, reikia saugoti informaciją?

16. Ar Jūsų organizacijoje laikomasi „švaraus stalo“ politikos?

a) taip
b) ne

17. Ar Jūsų organizacijoje dirbantys asmnenys yra įpareigoti pranešti apie vykstančius informacijos saugumo incidentus už tai atsakingiems darbuotojams?

a) taip
b) ne

18. Kokios priežastys, Jūsų nuomone, trukdo spręsti informacijos saugumo problemas?

a) šios srities specialsitų trūkumas
b) infprmacijos sauga nėra laikoma problema, kurią reikėtų spręsti
c) per mažos informacijos saugumui skiriamos lėšos.

„INFORMATION SECURITY IN PUBLIC AND PRIVATE SECTOR“

INDRĖ SELSKAITĖ

(SUMMARY)

At present the information and data has become a very important product and has achieved higher value than ever before. The age of information has brought not only new opportunities and possibilities, but also new problems – first of all information security problems.

The object of this master work is information and information property. The main aim of this work is to analyse and describe the information security problem in private and public sector. Tasks, which helped to achieve the main aim, were to find out the information security necessity, to look over the main security problems in private ant public organizations, also to analyse the security means and security politics.

With a help of methods of documentary and scientific literature analysis, bibliographic method and quantitative survey was established, that the security problem really exists and has to be solved as soon as possible, because of the information security incidents the organizations experience large losses and damages every day.

The urgency of information and data security problem was proofed while analysing scientific literature, reviewing researches, also while doing the quantitative research and questioning the information and data security specialist, that are working in public and private organizations, about security problems in their organizations.

Every organization, does not matter in which sector working, is using a lot of different information in her daily work. Depending on their activities the organizations have a various threats and risks. To ensure the high level of information security the public and private organizations needs to apply not only technical, but also organizational and physical means of security.

In contemporary society the information security problem is getting more and more attention. Regardless of this fact there exist not a lot of organizations, which can claim a high information security level.

After quantitative research it became clear, that the information security problem is sorer and bigger in the private (business) sector. Business organizations more often are facing different information security threats and suffering larger damages than the public organizations. The information security means in private organizations are applied not as complex and purposeful as in the public organizations. Besides that the business organizations understands not so good the importance of information resources and appraises not totally the advantage, which can give the information and data.

In research were established different incidents of information security, which are happening in public and private sector. Also were identified different information security means, which are similar in both sectors. The motives why the information should be protected were different: in private sector because of financial reasons, and in the public sector because that is a requisition of law statements. The results of the research let to assert, that the law regulation of the information and data security is one of the most effective means to protect the information property.