MYKOLO ROMERIO UNIVERSITETO

STRATEGINIO VALDYMO IR POLITIKOS FAKULTETO

VALDYMO TEORIJOS KATEDRA

STUDENTĖS ARŪNĖS GOGYTĖS

(Viešojo administravimo programa,Veiklos audito specializacija)

ASMENS DUOMENŲ APSAUGOS AUDITAS BIUDŽETINĖSE DUOMENŲ VALDYTOJŲ ORGANIZACIJOSE

Magistro baigiamasis darbas

Darbo vadovė –

lekt. R. Bukaveckienė

Konsultantas –

prof. habil. dr. S. Puškorius

Vilnius, 2006

TURINYS

ĮVADAS

Gyvename informacijos amžiuje, kai nuo informacijos tikslumo, jos pateikimo greičio priklauso daugelio žmonių gyvenimas. Informacija ir jos apdorojimo sparta tapo neatsiejama verslo įmonių, valstybinių įstaigų bei kitų organizacijų dalimi. Tam tikros informacijos turėjimas gali suteikti konkurencinį pranašumą, o jos praradimas - atnešti nuostolių.

Eksponentinis globalinio kompiuterių tinklo augimas (tokio kaip Internetas) sukuria beprecedentį atvejį. Interneto pagalba didžiuliai kiekiai informacijos gali būti perduoti iš vienos šalies į kitą visiškai nepaisant sienų ir ši informacija laisvai prieinama visai visuomenei. Dėl to duomenų apsaugos įstatyminė bazė turi atitikti visuomenės poreikius ir sugebėti atremti šiuos technologijų keliamus iššūkius.

Darbo autorės nuomone asmens duomenų apsauga gali būti suprantama kaip atsakas į šiuolaikinę technologijų raidą. Modernios IT technologijos sąlygojo esminius organizacinius pokyčius daugelyje šiuolaikinės visuomenės gyvenimo sričių. Pavyzdžiui, skaitmeninė telefonija, interneto ir el. pašto paslaugos taip pat pastebimai pakeitė darbo vietos realybę. Neišvengiamai ji taip pat pakeitė ir informacinę *status quo* santykių ne tik tarp valdžios institucijų ir piliečių, vartotojų ir įmonių, bet ir tarp darbdavių ir darbuotojų. Šis faktas yra esminis, nes daugelis Europos valstybių sukūrė gana griežtą teisinį šių santykių režimą[1].

Pasirinkti šią temą paskatino jos naujumas ir aktualumas. Galima teigti, jog duomenų apsaugos sritis yra palyginti nauja Lietuvoje, todėl pastebimas žinių, savo teisių ir pareigų suvokimo trūkumas tiek tarp duomenų subjektų, tiek ir tarp duomenų valdytojų. Asmeninių duomenų didėjantis naudojimas yra naudingas tiek visuomenei, tiek individams. Vis dėl to, bet kuris asmeninių duomenų rinkimas ir naudojimas gali turėti ir neigiamos įtakos. Pavyzdžiui, jeigu duomenys yra laikomi nesaugiai galima pažeisti asmens privatumo laisvę. Su individais susijusi informacija vadinama asmeniniais duomenimis yra renkama ir naudojama įvairiais gyvenimo atvejais. Asmuo pateikia informaciją apie save registruodamasis į biblioteką, pirkdamas sporto abonentą, atidarydamas banko sąskaitą ir t.t. Asmeniniai duomenys gali būti gaunami tiesiai iš individo arba iš jau egzistuojančių duomenų bazių. Duomenų bazėse esantys duomenys gali būti naudojami įvairiems tikslams. Taigi, asmeniniai duomenys, tai bet kokia informacija, kuri identifikuoja asmenį (pavyzdžiui vardas, telefono numeris ar nuotrauka).

[1] Phare programme twinning project no. LT02/IB-JH-02/-03 strengthening administrative and technical capacity of personal data protection. Phare Dvynių projektas // www.ada.lt/images/cms/File/**Pirmieji**%20duomenu%20**apsaugos**%20zingsniai.pdf; prisijungimo laikas: 2006-05-10.

Plečiantis elektroniniam verslui, perduodant informaciją kompiuterių tinklais, vis daugiau naudojama privati informacija, asmens duomenys. Vykdant elektroninių paslaugų procedūras internete, vis aktualesnėmis tampa vartotojų privatumo teisių ir sandorių informacijos apsaugos, privačios informacijos ir asmens duomenų nesankcionuoto vartojimo problemos.

Galima teigti, jog duomenų apsauga šiuo metu yra aktuali tema. Jos palaikymui ir sustiprinimui reikalingas duomenų apaugos auditas, kuris padėtų nustatyti duomenų saugumo lygį organizacijose ir atskleistų pagrindines problemas.

Šio darbo **tikslas** – atskleisti asmens duomenų apsaugos audito ypatumus.

Darbo uždaviniai:

- Aptarti asmens duomenų apsaugos sampratą bei reikšmę;
- Išanalizuoti teisinę bazę, reglamentuojančią duomenų apsaugą;
- Nustatyti duomenų apsaugos audito formas, metodus ir etapus;
- Ištirti bei įvertinti asmens duomenų apsaugos audito būtinumą ir reikšmę biudžetinėse duomenų valdytojų organizacijose;
- Ištyrus esamą situaciją pateikti išvadas ir pasiūlymus.

Tyrimo objektas – registruoti Lietuvoje biudžetinių įstaigų duomenų valdytojai.

Hipotezė – duomenų valdytojai, neatliekantys duomenų apsaugos audito duomenis valdo neefektyviai ir nesilaikydami duomenų apsaugai keliamų teisinių reikalavimų.

Tyrimo metodika:

Mokslinės literatūros analizė bei pirminių ir antrinių duomenų analizė (dokumentinis tyrimas) programos, statistika, moksliniai darbai, įmonių vidiniai dokumentai, išorinė įmonių informacija pateikta Interneto svetainėse, įvairūs užsienio ir Lietuvos autorių straipsniai panaudoti išsiaiškinant duomenų apsaugos sampratą ir reikšmę, duomenų apsaugos audito sąvoką bei analizuojant teisinę bazę. Dėl temos naujumo ir aktualumo daugiausiai buvo naudojamasi moksliniais straipsniais. Šie tyrimo metodai buvo svarbūs teorinėje darbo dalyje.

Praktinėje tyrimo dalyje *anketavimo metodu* apklausti registruoti biudžetinių organizacijų duomenų valdytojai (išskyrus švietimo įstaigas).

1. DUOMENŲ APSAUGOS AUDITAS

Norint užtikrinti asmeninių duomenų apsaugą labai svarbu kontroliuoti visą procesą susijusį su duomenų rinkimu, judėjimu, archyvavimu ir t.t. Tai padaryti padėtų ir duomenų apsaugos auditas, kurio sąvoką autorė pateikia 1.1. skyrelyje.

Asmens duomenų tvarkymas yra neabejotinai vienas iš svarbiausių šių laikų socialinių reiškinių. Visos šiuolaikinės vidutinės ir didelės įmonės personalo duomenų sistemoms, bazėms kurti, administruoti ir planuoti naudoja kompiuterizuotas asmens duomenų kaupimo, perdavimo ir pan. sistemas. Pvz., ligoninės ir sveikatos draudimo įstaigos kaupia ir tvarko medicininius pacientų duomenis. Bankai ir kitos kredito institucijos kaupia informaciją apie klientų pajamas ir rinką, mokyklos ir universitetai apie savo studentus, policija atlieka pirštų antspaudų, genetinio patikrinimo ar telekomunikacijų kontrolę. Mokesčių institucijos taip pat valdo ir naudoja milžiniškas asmens duomenų bazes, susisteminančias informaciją apie pajamas, darbo vietą, šeimyninį statusą ir pan. Daugelio sričių (sociologinės, istorinės, medicininės) moksliniai tyrimai tiesiogiai priklauso nuo asmens duomenų. Televizija ir spauda nuolat skelbia apie privačių asmenų, politikų, žymių visuomenės veikėjų veiklą. Šie pavyzdžiai – tik dalis asmeninės informacijos panaudojimo. Pastarieji dešimtmečiai atskleidė ir įtvirtino, jog duomenys, informacija, susijusi su privataus asmens gyvenimu, naujosios ekonomikos kontekste tampa preke, turinčia nemenką komercinę vertę.

Pasaulyje vis didėja susirūpinimas nevaldomais asmeniniais duomenimis. Steigiamos institucijos padedančios prižiūrėti šį sudėtingą ir nenumaldomu greičiu plintanti procesą. Vyksta konferencijos, diskusijos, priimami teisiniai aktai. 2005 metų rugsėjo mėnesį susirinkę į Montreux 27-ąją Tarptautinę konferenciją duomenų Apsaugos ir Privatumo Įgaliotiniai pritarė skatinti duomenų apsaugos principų visuotinumo pripažinimą ir priėmė Montreux deklaraciją „Asmens duomenų apsauga ir privatumas globalizuotame pasaulyje: visuotinė teisė gerbti įvairovę". Šia deklaracija įgaliotiniai apibrėžė 17 pagrindinių duomenų apsaugos principų. Be to, siekdami stiprinti šiuos principus įgaliotiniai sieks bendradarbiavimo su įvairiomis valstybinėmis organizacijomis bei susitarė[2]:

a. ypač sustiprinti informacijos apsikeitimą, priežiūros veiklos koordinavimą, bendrų standartų kūrimą, informacijos, susijusios su veikla ir šios konferencijos rezoliucijomis, sklaidą;

[2] Montreux deklaracija // www.ada.lt/images/cms/File/ Montre_deklaracija_doc.0922%20(1).doc; prisijungimo laikas: 2006-05-10.

b. skatinti bendradarbiavimą su šalimis, kuriose kol kas nėra nepriklausomų duomenų apsaugos priežiūros institucijų;
c. skatinti informacijos apsikeitimą su tarptautinėmis nevyriausybinėmis organizacijomis sprendžiančiomis duomenų apsaugos ir privatumo klausimus;
d. bendradarbiauti su organizacijų duomenų apsaugos pareigūnais;
e. sukurti nuolatinį tinklapį, ypač dėl informacijos ir išteklių bendro valdymo.

Visos organizacijos besirūpinančios duomenų apsauga ir saugia informacija Lietuvoje gali įsidiegti ISO/IEC 17799:2005 standartą, kurio neoficialus vertimas pateiktas 1 priede. Be to, įgyvendinant pagal ši standartą parinktas priemones, reikėtų naudotis ir detalesniais, techniniais atskirų sričių standartais ar metodikomis, kaip pavyzdžiui IT saugumo „techninis" standartas ISO/IEC 13335.

Apibendrintai galima teigti, jog duomenų apsauga yra šiuolaikinės visuomenės, sparčiai besikeičiančių technologijų padarinys. Organizacija, norinti užtikrinti duomenų apsaugą turėtų turėti atsakingą už duomenų apsaugą darbuotoją bei reguliariai atlikti duomenų apsaugos auditą.

1.1. Duomenų apsaugos audito samprata ir reikšmė

Lietuvoje duomenų apsaugos priežiūra ir plėtojimas yra glaudžiai susijęs su Vyriausybės strateginiais tikslais (prioritetais) – stiprinti Lietuvos įtaką formuojant Europos Sąjungos ekonominę politiką ir sprendimus šaliai aktualiais klausimais ir siekti dalyvauti euro zonoje, plėtoti informacinę ir žinių visuomenę, skatinti visuomenės teisinį švietimą.

Dauguma autorių sutaria, kad užtikrinti duomenų saugumą reiškia užtikrinti jos KONFIDENCIALUMĄ (angl.*Confidentiality)*, VIENTISUMĄ (angl. *Integrity)* ir PRIEINAMUMĄ (angl. *Availability)*[3].

Galima teigti, jog konfidencialumas - tai saugumo principas, užtikrinantis, kad su informacija galės susipažinti tik tie asmenys, kurie turi teisę su ja susipažinti, ji nebus tyčia ar netyčia atskleista kitiems asmenims. Konfidencialumo pažeidimas - informacijos tyčinis ar netyčinis atskleidimas pašaliniams asmenims.

Vientisumas (integralumas) – tai saugumo principas, užtikrinantis, kad informacinės sistemos ir jose saugoma informacija nebus pakeista nesankcionuotu būdu, kitaip sugadinta arba visiškai prarasta. Vientisumo pažeidimas - nesankcionuotas informacinės sistemos konfigūracijos ar jose saugomos informacijos pakeitimas arba praradimas (dalinis arba visiškas), įvykęs dėl tyčinių ar

[3] A. Jankūnas, A. Klibas. Informacijos technologijos. Vilnius, Verslo žinios, 2005. P. 60.

netyčinių veiksmų. Šis saugumo principas - šiek tiek sudėtingesnis, nes susijęs ne tik su kompiuteriuose saugoma informacija, bet ir su pačiomis informacinėmis sistemomis. Pavyzdžiui, nesankcionuotas duomenų bazės ar kitų dokumentų įrašų pakeitimas, informacijos sugadinimas. Tai gali būti padaryta tiek tyčia, norint pakenkti arba siekiant naudos, tiek netyčia - dėl nežinojimo ar žmogiškos klaidos. Taip pat informacija gali būti sugadinta ir dėl kompiuterių gedimų ar virusų.

Prieinamumas – tai principas, kuriuo remiantis reikiami informacinių sistemų resursai reikiamu metu yra prieinami įgaliotajam naudotojui. Šis terminas dar verčiamas kaip „pasiekiamumas“, „veiksmingumas“ arba „darbingumas“, tačiau nė vienas iš lietuviškų terminų visiškai neatspindi angliško *availability*. Prieinamumo pažeidimas - pilnas arba dalinis informacinės sistemos darbingumo pažeidimas, dėl kurio informacija ir sistemos resursai tampa nepasiekiami visiems arba daliai jos naudotojų.

Apibendrintai galima teigti, jog bet kurį saugumo pažeidimą galima priskirti vienam arba keliems iš trijų aprašytų tipų.

Svarbi problema, susijusi su kompiuteriniu informacijos apdorojimu, yra didelis tokios informacijos pažeidžiamumas bei didesnės galimybės pažeisti informacijos saugumą, pavogti, sunaikinti arba pakeisti duomenis.

Pasak O. Liskovo įvairiuose informacijos ar duomenų apsaugos žinynuose, bei vadovuose duomenų apsauga įvardinama įvairiai, tačiau visuose jų pabrėžiami trys pagrindiniai duomenų apsaugą reglamentuojantys lygiai[4]:

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

Administracinio – techninio saugumo lygis daug kur dar vadinamas administraciniu ir organizaciniu saugumu. Administracinis-techninis saugumas traktuojamas kaip techninių priemonių organizavimas, siekiant užtikrinti kompiuterinėse (ir ne tik) laikmenose saugomą informaciją. Šiam lygiui galime priskirti tokias priemones, kaip saugumo politikos nuostatas, kurios aiškiai apibrėžia, kokia informacija yra saugoma, o kokia ne. Šiam lygiui priklauso ir apsaugos organizavimas techninėmis priemonėmis. Tai ugniasienių įdiegimas bei antivirusinės programinės įrangos įdiegimas įmonės kompiuterinėse sistemose ir jos nustatymas. Duomenų šifravimo priemonės taip pat yra svarbi duomenų apsaugos priemonė.

[4] Liskovas O. Duomenų apsauga elektroninėje komercijoje // http://www.esecurity.lt/article/1145.html; prisijungimo laikas 2006-03-26.

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

Fiziniam saugumui priskiriami metodai, skirti apsaugoti aparatines ir kompiuterinės technikos ryšių priemones nuo nelaukiamo fizinio pašalinių jėgų poveikio. Tokioms jėgoms galime priskirti stichines nelaimes, techninius gedimus, dėl kurių galimas svarbių duomenų sugadinimas ar sunaikinimas.

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

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

Šiuo metu Europoje tik dvi šalys turi veikiančią duomenų apsaugos audito sistemą. Jau 1984 metais Duomenų Apsaugos Aktą priėmusi ir 1998 metais jį atnaujinusi *Didžioji Britanija* bei *Vokietija*, kuri vykdo duomenų apsaugos auditą pagal Federalinį Duomenų Apsaugos Aktą. Galima teigti, jog šiuo metu vis daugiau šalių kreipia dėmesį į duomenų apsaugą, todėl duomenų apsaugos audito reikšmė vis didėja.

Labai svarbu žinoti, kaip yra suprantama duomenų apsaugos audito ir kitos su juo susijusios sąvokos. Lietuvos Respublikoje dar nėra termino duomenų apsaugos auditas, todėl autorė darbe naudos Didžiojoje Britanijoje priimta duomenų apsaugos audito sąvoką.

Pagal buvusią Didžiosios Britanijos duomenų apsaugos komisarę duomenų apsaugos auditas tai „sisteminis ir nepriklausomas patikrinimas, parodantis ar asmeniniai duomenys tvarkomi

pagal organizacijos apsaugos politiką ir procedūras ir ar šie veiksmai atitinka Duomenų Apsaugos Akto reikalavimus“[5].

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (toliau tekste ADTAĮ) yra nustatyta, jog asmens duomenys tai - bet kuri informacija, susijusi su fiziniu asmeniu - duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.

Galima teigti, jos informacinėje visuomenėje duomenų apsaugos auditas labai svarbus ginant asmenines žmogaus teises ir apsaugant jas nuo neteisėto panaudojimo. D. Baker išskiria 4 pagrindinius duomenų apsaugos audito tikslus[6]:

- Nustatyti duomenų apsaugos atitikimą Duomenų Apsaugos Akto reikalavimams;
- Nustatyti atitikimą pačios organizacijos duomenų apsaugos sistemai;
- Nustatyti duomenų apsaugos sistemoje galimas spragas ir silpnybes;
- Pateikti duomenų apsaugos įvertinimą.

Pagal ISACA organizacijos pateiktą prezentaciją yra išskiriama daug daugiau duomenų apsaugos audito tikslų, t.y[7].:

- Patikrinti ar duomenys yra surenkami ir naudojami teisingai, nenusižengiant įstatymams ir nustatytiems tikslams;
- Užtikrinti kokybę, t.y. užtikrinti, kad duomenys yra tikri, pilni ir atnaujinami, pakankami ir aktualūs;
- Užtikrinti išsaugojimą – t.y. patikrinti ar duomenys šalinami ir trinami laiku ir pagal nustatytas procedūras;
- Paruošti duomenų apsaugos rašytines procedūras, jei tokių nėra (pvz. gidus);
- Palyginti naudojamą apsaugą su asmens laisvėmis ir teisėmis;
- Suderinti duomenų apsaugos teisinę bazę su kitais teisiniais aktais.

Taigi, galima teigti, jog šiuo metu dar nėra tiksliai apibrėžtų duomenų apsaugos audito tikslų, ir jie priklauso nuo organizacijos, nuo auditoriaus suvokimo apie duomenų apsaugą, nuo auditui skirto laiko. D. Barker pristatyti audito tikslai yra oficialūs, jie atskleisti ir Duomenų apsaugos audito gidę, kurį sudarė duomenų apsaugą prižiūrinti institucija Didžiojoje Britanijoje.

[5] Barker D. Duomenų apsaugos auditas. Tarptautinės konferencijos E-verslas ir duomenų apsauga medžiaga. Vilnius: Expozona , 2005. P. 146.
[6] Ten pat. P. 152.
[7] Data protection auditing // www.isacalondon.org/presentations/ISACA%20Data%20 Protection %20Auditing.ppt; prisijungimo laikas 2006-05-25.

Autorės nuomone kiekvienas auditorius atlikdamas duomenų apsaugos auditą turėtų kelti tokius tikslus:

- Patikrinti ar organizacijoje yra formali (t.y. dokumentuota ir nuolat atnaujinama) duomenų apsaugos sistema;
- Patikrinti ar organizacijos darbuotojai įtraukti į duomenų apsaugą;
- Patikrinti ar duomenų apsaugos sistema veikia organizacijoje ir yra efektyvi.

Norint užtikrinti tikslų pasiekimą duomenų apsaugos auditorius turi vadovautis duomenų apsaugos principais. Pagal D. Barker yra tokie pagrindiniai duomenų apsaugos audito principai:

- Duomenų apsaugos auditą atlieka nepriklausomi apmokyti auditoriai;
- Duomenų apsaugos auditas yra sisteminis tyrimas;
- Atliekant auditą turi būti naudojamos visos nustatytos procedūros;
- Atliktas auditas įforminamas audito ataskaitoje[8].

Be to, atliekant duomenų apsaugos auditą, labai svarbu atkreipti dėmesį į tai ar[9]:

- Organizacijoje yra žmogus atsakingas už duomenų apsaugą;
- Kiekvienas organizacijos narys dirbantis su asmeniniais duomenimis supranta, jog jis yra atsakingas už teisingą asmeninių duomenų panaudojimą;
- Kiekvienas savo darbe naudojantis asmeninius duomenis yra apmokytas teisingai naudotis šiais duomenimis;
- Kiekvienas darbuotojas dirbantis su asmeniniais duomenimis yra prižiūrimas;
- Bet kuris asmuo, norintis gauti asmeninę informaciją žino kaip tai padaryti;
- Asmeninių duomenų užklausimai ir atsakomi nedelsiant ir paslaugiai;
- Asmeninių duomenų laikymo ir saugojimo metodai yra aiškiai aprašyti;
- Reguliarus peržiūrėjimas ir auditas yra atliekamas tokiu pat būdu kaip ir asmeninių duomenų valdymas;
- Asmeninės informacijos apdorojimo, laikymo ir valdymo metodai yra reguliariai vertinami;
- Asmeninių duomenų laikymas yra reguliariai vertinamas.

Šiuo metu Lietuvoje asmens duomenų apsaugą reglamentuoja Asmens Duomenų Teisinės Apsaugos Įstatymas (ADTAĮ)[10], taigi atliekant duomenų apsaugos auditą Lietuvoje reikėtų

[8] Barker D. Duomenų apsaugos auditas. Tarptautinės konferencijos E-verslas ir duomenų apsauga medžiaga. Vilnius: Expozona , 2005. P. 153.
[9] Data protection policy // www.wales.nhs.uk/sites3/documents/49/15DPA.pdf; prisijungimo laikas 2006-05-10.

vadovautis ne Didžiojoje Britanijoje priimtu Duomenų Apsaugos Aktu, o minėtuoju įstatymu. Be to, Lietuva jau nuo 2004 metų yra Europos Sąjungos narė, todėl joje galioja ir Europos Sąjungos teisiniai aktai bei reikalavimai [11].

Lietuvoje galiojantis ADTAĮ įstatymas duomenų saugumą apibūdina taip[12]:

1. Duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytiniame ar jam prilygintos formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.);
2. Duomenų valdytojas pats tvarko asmens duomenis ir (ar) įgalioja duomenų tvarkytoją. Jei duomenų valdytojas įgalioja duomenų tvarkytoją tvarkyti asmens duomenis, jis privalo parinkti tokį duomenų tvarkytoją, kuris garantuotų reikiamas technines ir organizacines duomenų apsaugos priemones ir užtikrintų, kad tokių priemonių būtų laikomasi;
3. Duomenų valdytojas, įgaliodamas duomenų tvarkytoją tvarkyti asmens duomenis, nustato, kad duomenys turi būti tvarkomi tik pagal duomenų valdytojo nurodymus;
4. Duomenų valdytojo ir duomenų tvarkytojo, nesančio duomenų valdytoju, santykiai turi būti reglamentuojami rašytine sutartimi, išskyrus atvejus, kai tokius santykius nustato įstatymai ar kiti teisės aktai;
5. Duomenų valdytojo, duomenų tvarkytojo ir jų atstovų darbuotojai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį, jei šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams.

Aukščiau cituotoje įstatymo dalyje dažnai minimi duomenų valdytojo ir duomenų tvarkytojo terminai, būtina apibrėžti šias dvi sąvokas. Pagal minėtąjį įstatymą, duomenų valdytojas - juridinis ar fizinis asmuo, kuris vienas arba drauge su kitais nustato asmens duomenų tvarkymo

[10] plačiau apie įstatymą 1.2.2. skyrelyje
[11] plačiau 1.2. skyriuje
[12] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios 2003, Nr. 15 - 597.

tikslus ir priemones. Jeigu duomenų tvarkymo tikslus nustato įstatymai ar kiti teisės aktai, tai duomenų valdytojas ir (ar) jo skyrimo tvarka gali būti nustatyti tuose įstatymuose ar kituose teisės aktuose. O duomenų tvarkytojas tai – juridinis ar fizinis (kuris nėra duomenų valdytojo darbuotojas) asmuo, duomenų valdytojo įgaliotas tvarkyti asmens duomenis. Duomenų tvarkytojas ir (ar) jo skyrimo tvarka gali būti nustatyti įstatymuose ar kituose teisės aktuose[13].

Apibendrinant aukščiau pateiktas duomenų saugumo sąlygas, sąvokas ir principus galima teigti, jog susipažinti su asmens duomenimis turi būti leidžiama tik ribotam asmenų skaičiui. Turi būti pateikti aiškūs (techniniai ir organizaciniai) nurodymai dėl to, kuris asmuo gali susipažinti su kokiais duomenimis. Jeigu į patalpas, kuriuose saugomi asmeninai duomenys, gali patekti kiti asmenys, turi būti nustatyta, kad šie asmenys neturi galimybės pažiūrėti į monitorius ar atspausdintą tokiu būdu gaunamą informaciją; kitaip tariant, jie neturi teisės susipažinti su tokia informacija. Visos laikmenos turi būti saugiai laikomos užrakintos, kai jų nenaudoja įgaliotasis asmuo. Kiekviena laikmena (atspausdinta medžiaga, kompaktiniai diskai ir pan.), kuri nebėra naudojama, turi būti visiškai ištrinta ir fiziškai sunaikinta.

PHARE Dvynių projekto "Duomenų apsauga – pirmieji žingsniai" autoriai teigia, jog duomenų tvarkytojai ir duomenų valdytojo darbuotojai turi būti informuoti, kad be duomenų valdytojo leidimo negalima diegti jokios programinės įrangos. Be to, jie turi būti informuoti apie šiuos dalykus[14]:

- nešiojami kompiuteriai turi būti visada prižiūrimi, o juose saugomi asmens duomenys turi būti užkoduoti;
- jokiam kitam asmeniui (net viršininkui) nėra atskleidžiami kompiuterio slaptažodis ar vartotojo tapatybė ir turi būti periodiškai keičiami;
- bet koks duomenų perdavimas (techniniu ar organizaciniu būdu) turi būti atliekamas taip, kad jų nepriimtų kitas asmuo nei numatytas gavėjas;
- jokia informacija nėra atskleidžiama telefonu kitam asmeniui, prieš tai nepatikrinus jo tapatybės (pvz., perskambinant) ir jo teisėtumo.

Tarp organizacinių padalinių ir operatyvinių darbuotojų aiškiai paskirstomos funkcijos dėl duomenų naudojimo. Duomenų naudojimas turi būti susietas su įgaliotų organizacinių padalinių ir operatyvinių darbuotojų teisėtais nurodymais. Kiekvienam operatyviniams darbuotojui pateikiami

[13] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios 2003, Nr. 15- 597.

[14] Phare programme twinning project no. LT02/IB-JH-02/-03 strengthening administrative and technical capacity of personal data protection. Phare Dvynių projektas// www.ada.lt/images/cms/File/**Pirmieji**%20duomenu%20**apsaugos**%20zingsniai.pdf; prisijungimo laikas: 2006-05-10.

nurodymai dėl jo pareigų pagal vidaus duomenų apsaugos taisykles bei duomenų saugumo taisykles. Turi būti reglamentuota teisė patekti į duomenų valdytojo ar tvarkytojo patalpas. Be to, turi būti reglamentuota teisė susipažinti su dokumentais ir programomis, taip pat su laikmenomis, kad su jais negalėtų susipažinti atitinkamo įgaliojimo neturintys asmenys. Turi būti nustatyta teisė naudotis duomenų tvarkymo įranga, be leidimo draudžiant naudotis bet kokiu įtaisu; apsaugos priemonės turi būti taikomos bet kokiai technikai ir programoms.

Apibendrintai galima teigti, jog organizacija įdiegus į savo veiklą duomenų apsaugos auditą gali tikėtis naudos. Pirmiausia ji vadovausis įstatymais, vykdys savo įdiegtas apsaugos sistemas, darbuotojai ir vadovai bus dėmesingesni duomenų apsaugai, o visą tai suteiks vartotojams pasitenkinimą, dėl sumažėjusios klaidų tikimybės ir neapsaugotų duomenų neteisėto panaudojimo.

N. Zhao ir D.C. Yen teigia, jog auditas organizacijai gali suteikti didžiulę naudą. Besivystant informacinėms technologijoms atlikti audito procesą tapo ir paprasčiau ir sudėtingiau vienu metu. Pasinaudojus informacinėmis technologijomis nereikalingos rašytinės ataskaitos, nes duomenys gali būti surenkami ir kitu alternatyviu būdu. Dabar daugelis rodiklių gali būti gaunami, paskaičiuojami ir pateikti elektroninėje ataskaitoje[15]. Tačiau, iš kitos pusės, informacinės technologijos atveria galimybes ir nesąžiningų organizacijų ir pavienių asmenų piktnaudžiavimams ir galimybės pasinaudoti vertingais duomenimis savanaudiškais tikslais.

Viešojo sektoriaus organizacijos vis daugiau naudojasi informacinių technologijų teikiamais privalumais ir savo funkcijoms atlikti renka, apdoroja ir analizuoja duomenis informacinių technologijų pagalba. Pasak E. Loukis Daugiausia informacinės technologijos naudojamos[16]:

- administracinėms funkcijoms, tokioms kaip algalapių, biudžeto, inventoriaus ir kitoms administracinėms funkcijoms automatizuoti;
- paslaugų teikimui ir kitoms operacinėmis funkcijomis, tokioms kaip mokesčių surinkimas, vairuotojo pažymėjimo išdavimo ir palaikymo, subsidijavimo funkcijoms palengvinti ir pagreitinti;
- vidiniam koordinavimui ir kontrolei atlikti;
- viešosios politikos analizei, kūrimui, įdiegimui bei prižiūrėjimui;
- valdymui ir sprendimų priėmimui;

[15] N. Zhao, D.C. Yen. Auditing in the e-commerce era // Information management & Computer Security. 2004, Nr. 12 (5). P. 389.
[16] E.Loukis, D. Spinellis. Information systems security in the Greek public sector // Information management & Computer Security. 2001, Nr. 9 (1). P. 21.

- tarporganizaciniams koordinavimui ir bendradarbiavimui tarp įvairių viešųjų organizacijų.

Informacinių sistemų prieinamumas dažnai yra labai svarbus valdymo aspektas. T.y., dauguma informacinių sistemų, tokių kaip medicininės apsaugos teikimas, mokesčių rinkimas, konfidencialios ar kitos svarbios informacijos laikymas turi garantuoti aukštą konfidencialumo lygį. Duomenų apsaugai ypač pavojingos yra šiuo metu esančios galimybės apsikeisti duomenimis tarp viešojo sektoriaus įstaigų. Todėl duomenų pasikeitimo sistemoms turėtų būti skiriamas ypatingas dėmesys ir apsauga. Maža to, viešojo sektoriaus saugomi duomenys yra labai svarbūs, todėl jų integralumui turėtų būti keliami ypatingi reikalavimai. Galiausiai, moderni, tolyn žvelgianti viešojo sektoriaus informacinė sistema, kuri teikia elektronines viešojo sektoriaus paslaugas dažniausiai yra prieinama per Internetą ne tik ribotam valstybės tarnautojų skaičiui, bet taip pat daugeliui piliečių, įmonių ir organizacijų, o tai sudaro didesnę tikimybę ir duomenų saugumo pažeidimui.

Šiuo metu informacinių sistemų veikiančių kompiuterių tinkluose saugumas yra plačiai diskutuojama tema. Į saugumo sistemas nuolat kas nors įsilaužia, todėl galima teigti, jog kompiuterių, sujungtų į tinklą saugumas pagal savo prigimtį gali būti labai menkas, vis dėl to, diegiant saugumo sistemas, šiuolaikiškoje, nuolat kintančioje technologinėje aplinkoje susiduriama su iššūkiu, tačiau kiekvienas duomenų tvarkytojas (tiek privačiame, tiek viešajame sektoriuose) turi tai įvertinti ir diegti bent jau pakankamą saugumą užtikrinančias sistemas.

Įsibrovėliai į kompiuterinius tinklus gali turėti įvairių tikslų, ir tai gali būti[17]:

- Užsienio žvalgyba;
- Organizuotas nusikalstamumas;
- Teroristinės organizacijos;
- Privatūs tyrinėtojai;
- Informacijos brokeriai, kurie suradę vertingos informacijos parduota ją nelegaliai;
- Hakeriai, norintys pasisavinti finansinius duomenis.

E. Sandeson ir kt. teigia, jog kai kurie kompiuterių vartotojai supranta, kad įsilaužiant į organizacijų tinklus įmanoma gauti labai naudingos informacijos. Ši informacija gali būti panaudojama dvejopai – parduodant pasisavintą informaciją, arba pakeičiant ją savo naudai. Kiekviena organizacija turėtų turėti saugumo politiką, kuri ypatingą dėmesį skirtų elektroniniam saugumui. Ypatingi asmens duomenys (ang. Sensitive data) yra ypač jautrūs atakoms ar įsibrovimas

[17] A. Jankūnas, A. Klibas. Informacijos technologijos. Vilnius, Verslo žinios, 2005. P. 83.

elektroninėje erdvėje. Amerikoje naudojamas posakis „Uncija prevencijos yra verta svarui vaistų“ labai tinka kompiuterių tinklų saugumui[18].

Šiuo metu viešojo sektoriaus organizacijos dažnai tampa potencialiomis grėsmėmis žmogaus privatumui. Jos turi nemažai įrankių padedančių gauti asmeninę informaciją iš populiacijos ir daugelis valstybės tarnautojų visiškai laisvai prieina prie šių duomenų.

Jau minėta, kad kompiuterių technologijos privalumai kartu su telekomunikacijos pasiekimais leidžia asmeniniams duomenims keliauti po pasaulį nepaisant sienų ir labai dideliu greičiu. To pasekoje duomenys, susiję pavyzdžiui su vienos Europos Sąjungos šalies piliečiais kartais naudojami kitoje ES šalyje. Kadangi asmens duomenys yra renkamai ir naudojami vis dažniau, saugaus duomenų perdavimo reikalavimai tapo būtini toliau keičiantis informacija.

Apibendrinant įvairių autorių mintis galima teigti, jog duomenys ir informacija tiek viešajame, tiek privačiame sektoriuose yra labais svarbūs:

- Organizacijoje laikomų duomenų reikalingumas turi būti apibrėžtas anksčiau, negu tie duomenys buvo/bus surinkti, o surinkta informacija turi būti griežtai apibrėžta ir naudojama tik nustatytiems tikslams. Duomenų valdytojai turėtų drausmingai prižiūrėti ir tvarkyti surinktus duomenis ir atskleisti tik įstatymų numatytais atvejais;
- Duomenys turi būti gaunami sąžiningai ir teisėtai;
- Duomenys negali būti atskleisti ar panaudojami ne pagal tikslą, kuriuo jie buvo surinkti, išskyrus susijusiais atvejais;
- Asmeniniai duomenys ir kita gaunama informacija turi būti pilna, tiksli, aktuali ir naujausia, kad patenkintų jai keliamus tikslus;
- Asmeniniai duomenys neturėtų būti laikomi ilgau, negu jie yra reikalingi;
- Visi asmeniniai duomenys turėtų būti pasiekiami tiems žmonėms, kurie šiuos duomenis pateikė, t.y. duomenų subjektams. Turi būti prieinama tik kiekvieno asmens asmeninė informacija su galimybe ją atnaujinti ar ištrinti.
- Asmeniniai duomenys ir kita organizacijos informacija turi būti apsaugota nuo nesankcionuoto naudojimo. Be to turi būti sukurta sistema, leidžianti nebenaudojamus duomenis sunaikinti arba atnaujinti;
- Maža to, visi asmeniniai duomenys turi būti apsaugomi nuo atsitiktinių praradimų ar jų sugadinimo tyčia;

[18] E. Sanderson, K. A. Forcht. Information security in business environments // Information management & Computer Security. 1996, Nr. 4 (1). P. 32.

- Labai svarbu, kad organizacijoje būtų atsakingas už asmeninių duomenų naudojimą asmuo. Jis turėtų prižiūrėti kaip laikomasi saugumo principų, standartų.

Gali kilti klausimas kokią naudą gauna organizacija laikydamasi šių principų, įvertinant visus organizacijos duomenis ir palyginus juos su asmeniniais duomenimis. Atsakymas labai paprastas, tai trys pagrindiniai kriterijai, kuriais galima įvertinti organizacijos veiklą – efektyvumas, ekonomiškumas ir veiksmingumas. Nereikalingų ar nereikšmingų duomenų rinkimas, valdymas ir laikymas yra pasikartojantis išteklių ir fondų eikvojimas[19].

Geriausias būdas patikrinti savo veiklą pagal duomenų apsaugos teisinius reikalavimus yra atlikti duomenų apsaugos auditą, kuris parodytų esamą situaciją, tačiau norint jį atlikti efektyviai būtina susipažinti su duomenų apsaugą reglamentuojančiais įstatymais ir kitais dokumentais. Duomenų apsaugos auditas įvertina tą atitikimą reikalavimams ir atskleidžia duomenų apsaugos sistemos trūkumus.

1.2. Duomenų apsaugos teisinis reglamentavimas

Europos teisinę bazę ir Lietuvos duomenų apsaugos sistemą sudaro šie teisės aktai:

- 1981 m. Europos Tarybos konvencija (ETS no. 108), kurios tikslas – apginti asmens privatumą ir laisvę keistis informacija už nacionalinės sienos ribų. Beveik visos 46 Europos Tarybos valstybės narės pasirašė šią konvenciją ir įsipareigojo laikytis joje nustatytų principų.
- Tarptautinę teisę saistantis dokumentas EB duomenų apsaugos direktyva 95/46/EB.
- 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) suderina valstybių narių nuostatas, reikalingas užtikrinti tinkamą pagrindinių teisių ir laisvių lygį, ypač teisę į privatumą, tvarkant asmens duomenis elektroninių ryšių sektoriuje ir užtikrinant laisvą tokių duomenų, elektroninių ryšių įrangos ir paslaugų judėjimą Bendrijoje.
- 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir taip pat numato abonentų, kurie yra juridiniai asmenys, teisėtų interesų apsaugą.

[19] G. Collier. Information privacy: Just how private are the private details of individuals in a company's database? // Information Management & Computer Security. 1995 , Nr. 3 (1). P. 41.

Sekančiuose poskyriuose autorė atskleis pagrindinius šių teisės aktų reikalavimus duomenų apsaugai bei principus.

1.2.1. Teisinis reglamentavimas įvairiose pasaulio šalyse

Kai kalbama apie duomenų apsaugą (*ang. data protection*) teisės aspektu, ji suprantama kaip užtikrinimas, kad su kiekvienu asmeniu susiję duomenys turi būti apdorojami laikantis teisės principų, kurie buvo pirmą kartą suformuluoti Didžiojoje Britanijoje Duomenų Apsaugos Akte 1984 metais, o 1998-aisiais patvirtinta naujoji akto redakcija, kurioje buvo toliau išplėtoti duomenų apsaugos principai. Šių aktų paskirtis - užtikrinti asmens teises.

Duomenų apsaugos aktas reikalauja, kad kiekviena organizacija, renkanti duomenis apie asmenis, būtų užregistruota. Žinoma, tai nesusiję su asmenimis, kurie kompiuteriuose turi sukūrę asmenines adresų knygeles, jei tai jie daro savo asmeninėms reikmėms, o ne kieno nors (kito asmens ar įstaigos) pavedimu[20]. Duomenų Apsaugos Akte nurodoma, kad ją saugantis asmuo turi įrodyti, jog ėmėsi tinkamų priemonių, neleidžiančių pašaliniams asmenims susipažinti su šia informacija. Surinkti nebereikalingi duomenys turi būti sunaikinti.

Duomenų Apsaugos Akto priėmimas Didžiojoje Britanijoje 1984 metais buvo labai reikšmingas faktorius, nes be jo Didžioji Britanija galėjo prarasti verslą užsienyje, nes užjūrio įmonės negalėtų siųsti asmeninių duomenų į Britaniją. Iki Akto priėmimo Didžioji Britanija buvo sugriežtinusi savo teisinę bazę, kuri draudė tarptautinį duomenų dalinimąsi, jeigu gaunančioji šalis neturėjo tokių pačių asmeninių duomenų tvarkymo reikalavimų[21]. Visame pasaulyje egzistuoja trys duomenų apsaugos įdiegimo atvejai. Pirmuoju atveju, kuris taikomas didžiojoje daugumoje šalių asmeniniai duomenys nėra svarbūs, ir atitinkamai tose šalyse neegzistuoja jokia asmeninių duomenų apsaugos teisinė bazė. Šalyse, kuriuose duomenų apsauga yra svarbi egzistuoja du modeliai – „sektorinis“ ir „omnibusas“. Sektorinis modelis (kuriame teisinė bazė priklauso nuo kiekvieno skirtingo atvejo ir yra pritaikyta pvz. kredito institucijoms, kompiuterių biurams) yra plačiai naudojamas JAV ir Kanadoje, o omnibusas (duomenų saugumas yra vertinamas pagal vieną statutą) daugiausiai vartojamas Vakarų Europoje. Šių modelių skirtingumai atspindi skirtingą valstybių

[20] A. Jankūnas, A. Klibas. Informacijos technologijos // http://www.vz.lt/konferencijos/konsultacijos/it/IT-60-1.php#wp999157 ; prisijungimo laikas: 2006-06-02.

[21] G. Collier. Information privacy: Just how private are the private details of individuals in a company's database? // Information Management & Computer Security. 1995 , Nr. 3 (1). P. 42.

dėmesį duomenų saugumui bei atitinkamų vyriausybių pasiekiamam balansui tarp privataus saugumo ir laisvo informacijos judėjimo.

Dauguma Europos šalių duomenų saugumą apibūdina kaip žmogaus teises ir ieško būdų kaip puoselėti asmens duomenų saugumą pripažinta kaip žmogaus teise. Pavyzdžiui Vokietijoje teismai šią koncepciją išvystė dar toliau ir naudoja terminą informacijos apsisprendimo teisė[22].

Tuo tarpu Jungtinės Valstijos turėjo didžiulę naudą dominuodamos technologijų ir informacinių išteklių srityse, todėl JAV informacijos laisvė yra ekonominis padarinys. Natūralu, jog valstijos yra susirūpinusios bet kokiu potencialiu suvaržymu, kuris uždraus laisvą informacijos judėjimą ir taip galės pakenkti ekonomikai. Be to, kiekvienos valstijos ieškojimai kaip reguliuoti duomenų apsaugą ir laisvą informacijos judėjimą pačioje valstijos teritorijoje yra taip pat svarbus priartėjimas prie tarpvalstybinio duomenų judėjimo. Šalys, kurios nori užtikrinti savo piliečių duomenų saugumą yra susirūpinusios dėl asmeninių duomenų laisvo judėjimo ir tvarkymo už šalies teritorijos leidimo padarinių. Kai tik duomenys perkerta valstybės sieną jų kontrolė labai stipriai sumažėja. Tada labai sunku užtikrinti duomenų saugumą. Todėl taip manančios valstybės bando uždrausti laisvą duomenų judėjimą, jeigu duomenis priimančioje šalyje duomenys nėra apsaugoti tokiais pačiais teisės aktais ir reikalavimais. Tai ne tik kai kurių Jungtinių valstijų nuostata, bet ir Europos Tarybos, kuri stengiasi apsaugoti asmeninius duomenis nuo tarptautinio duomenų judėjimo be jokių ribų ir draudimų[23]. Asmeninių duomenų saugojimas yra viena iš priežasčių draudžianti tarptautinį laisvą duomenų judėjimą. Pagrindinis draudimo privalumas yra tas, kad vyriausybės saugo žmogaus teises, tačiau jie neketina statyti barjerus prekybai. Iš kitos pusės tam tikruose sluoksniuose tokiu būdu duomenų saugumui suteikiamas prastas vardas, nes informacijos rinkoje užsienio konkurentai nebegali konkuruoti.

Kaip jau minėta, kompiuterių naudojimas asmeninių duomenų tvarkymui Didžiojoje Britanijoje yra valdomas Duomenų Apsaugos Akto reikalavimais. Šis aktas[24] yra Europos Tarybos konvencijos Dėl Individo Apsaugos padarinys susijęs su asmeninių duomenų judėjimu.

Pagrindiniai Akto tikslai yra[25]:

- Nustatyti duomenų tvarkytojo registraciją ir praktinius įsipareigojimus;
- Leisti asmenims, kurių asmeninė informacija yra saugoma skaitmeninėse laikmenose sužinoti kokie duomenys apie juos kur ir kokiu tikslu saugomi ir naudojami.

[22] A. White. Control of Transborder Data Flow: Reactions to the European Data Protection Directive // International journal of law and information technology Nr. 5 (2). P. 232.
[23] Ten pat. P. 234.
[24] Data protection act 1984 // http://www.hmso.gov.uk/acts/acts1984/1984035.htm; prisijungimo laikas: 2006-05-02.
[25] Data protection act // http://www.opsi.gov.uk/acts/acts1998/80029--a.htm#3; prisijungimo laikas: 2006-06-02.

1998 metais priimtas Duomenų Apsaugos Aktas skelbia aštuonis pagrindinius principus, kurie yra taikomi asmeninių duomenų valdytojams, neatsižvelgiant į tai ar jie laikomi kompiuteriuose ar popieriniuose dokumentuose. Šie principai yra taikomi bet kurios formos asmeninių duomenų valdytojams. Šie aštuoni principai yra tokie[26]:

1. Asmens duomenys turi būti tvarkomi sąžiningai ir teisėtai. Jie negali būti perduoti jokioms kitoms šalims, jeigu neatitinka tam tikrų Akto nustatyto sąlygų;
2. Asmeniniai duomenys turi būti surenkami tik teisėtam nustatytam tikslui ir negali būti naudojami jokiems kitiems tikslams, nesuderintiems su pagrindiniu tikslu, kuriuo šie duomenys buvo surinkti;
3. Asmeniniai duomenys turi būti adekvatūs, tiesiogiai susiję ir ne besaikiai atsižvelgiant į jų surinkimo tikslą ar tikslus;
4. Asmeniniai duomenys turi būti tikslus ir naujausi;
5. Asmeniniai duomenys negali būti laikomi ilgiau negu reikia nustatytam tikslui ar tikslams pasiekti;
6. Asmeniniai duomenys gali būti apdoroti tik remiantis duomenų subjekto teisėmis nustatytomis Duomenų Apsaugos Aktu;
7. Atitinkami techniniai ar organizaciniai apribojimai (pvz. saugumo apribojimai) turi būti nustatyti nesankcionuotam ir neteisėtam asmeninių duomenų perdavimui ir naudojimui. Be to, jie turi būti apsaugoti nuo atsitiktinio praradimo ar sugadinimo.
8. Asmeniniai duomenys neturėtų būti perduoti už Europos Ekonominės zonos ribų, išskyrus tuos atvejus, kai šalis arba teritorija užtikrina atitinkamą saugumo lygį duomenų subjekto laisvėms ir teisėms perduodant asmeninius duomenis.

Kasdieninį šių veiksmų administravimą ir Akto vykdymo priežiūrą Didžiojoje Britanijoje atlieka Duomenų Apsaugos Registro Tarnyba[27].

Europos duomenų apsaugos priežiūros pareigūno įstaiga įsteigta 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentu (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir tokių duomenų laisvo judėjimo (toliau – Reglamentas Nr. 45/2001). Europos duomenų apsaugos priežiūros pareigūnas atsako už tai, kad būtų užtikrinta, jog Bendrijos institucijos ir įstaigos, tvarkydamos asmens duomenis, gerbtų fizinių asmenų pagrindines teises ir laisves, svarbiausia – jų teisę į privataus gyvenimo neliečiamumą.

[26] Data protection policy // www.wales.nhs.uk/sites3/documents/49/15DPA.pdf; prisijungimo laikas: 2006-05-10.
[27] Directgov internetinė svetainė // http://www.open.gov.uk/dpr/dprhome.htm; prisijungimo laikas: 2006-06-10.

Europos duomenų apsaugos priežiūros pareigūnas atsako už šio Reglamento Nr. 45/2001 ir visų kitų Bendrijos aktų, reglamentuojančių fizinių asmenų pagrindinių teisių ir laisvių apsaugą Bendrijos institucijai ar įstaigai tvarkant asmens duomenis, nuostatų vykdymo priežiūrą ir užtikrina jų taikymą bei Bendrijos institucijų, įstaigų ir duomenų subjektų konsultavimą visais su asmens duomenų tvarkymu susijusiais klausimais [28].

1995 metų rudenį Europos parlamentas ir Taryba priėmė asmens duomenų apsaugos direktyvą, norėdami užtikrinti saugų ir laisvą duomenų judėjimą [29]. Visos Europos Sąjungos šalys narės turėjo įdiegti į savo teisinę bazę direktyvos reikalavimus iki 1998 metų spalio 24 dienos. Ši direktyva yra tik maža dalis Europos Sąjungos teisinės bazės, kuri yra privaloma visoms šalims narėms. Kai tik direktyva yra priimama Europos lygiu, ji tampa privaloma ir visoms šalims narėms. Šalys turi užtikrinti, kad ji efektyviai įdiegta į jų teisinę sistemą. Direktyva galioja galutiniams rezultatams. Pritaikymo formos ir metodai priklauso nuo kiekvienos šalies atskirai. Iš esmės direktyva galioja tik per nacionalinį įgyvendinimo mastą. Vis dėl to, net jeigu Europos Sąjungos šalis narė neįgyvendinus direktyvos nacionalinėje teisėje, direktyva gali daryti tiesioginę įtaką teisinei bazei. Tai reiškia, kad asmenys gali pasinaudoti direktyva teismuose net ir tada, kai nacionalinėje teisėje ji dar neįdiegta. Be to, asmenys, kurie mano, kad nukentėjo dėl to, kad direktyva nacionalinėje teisėje įdiegta neteisingai, gali kreiptis į tarptautinius teismus [30].

EB direktyva (95/46EB) siekiama skatinti bei užtikrinti tolesnį bendrosios rinkos kūrimą[31]. Ji reikalauja, kad visos valstybės narės priimtų nacionalinius įstatymus, kurie atitiktų minimalius asmens duomenų apsaugos standartus. Direktyvos normoms tapus pilnai implementuotomis valstybių narių teisinėse sistemose, asmens duomenys bus siunčiami ir tvarkomi visoje EB tokiomis pat sąlygomis kaip ir vienoje valstybėje narėje. Taigi direktyva garantuoja laisvą informacijos judėjimą EB ribose. Pagal direktyvos nuostatas valstybėms narėms nebebus suteikta galimybė uždrausti asmeninės informacijos judėjimą į kitas valstybes nares. Direktyva skirta įgyvendinti dvejopo pobūdžio tikslams – iš vienos pusės apsaugoti fizinių asmenų pagrindines teises ir laisves, o ypač jų privatumo teisę tvarkant asmens duomenis, o iš kitos pusės – nevaržyti ir nedrausti laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su asmens duomenų

[28] Europos duomenų apsaugos prižiūrėtojas // www.ada.lt/index.php?lng=lt&action=page&id=172 ; prisijungimo laikas: 2006-05-10.
[29] Privacy law // http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas: 2006-05-10.
[30] Data protection in the European union // http://europa.eu.int/comm/justice_home/ fsj/privacy/index_en.htm - 27k; prisijungimo laikas: 2006-05-10.
[31] 95/46 EB Direktyvos preambulė // http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas: 2006-05-10.

apsauga[32].

Direktyvos teisiniai rėmai taipogi yra orientuoti į šių viena kitai prieštaraujančių vertybių – laisvo asmens duomenų judėjimo ir asmens privatumo teisės – suderinimą. Direktyvos 3 – ojoje įžanginėje citatoje akcentuojama, kad sukurti ir veikti vidaus rinkai, kurioje pagal Romos Sutarties 7a straipsnį užtikrinamas laisvas prekių, žmonių, paslaugų ir kapitalo judėjimas, būtina ne tik galimybė asmens duomenims laisvai judėti iš vienos valstybės narės į kitą, bet taip pat ir asmens pagrindinių teisių apsauga. Direktyva siekia užtikrinti esminių žmogaus teisių, kaip visuotinai pripažįstamų socialinių vertybių, apsaugą: „asmens duomenų tvarkymą reglamentuojančių nacionalinių įstatymų tikslas - apsaugoti pagrindines teises ir laisves, ypač privatumo teisę, ir tai pripažįstama Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnyje, taip pat Bendrijos teisės aktų bendruosiuose principuose“[33].

Direktyvos priėmimas išreiškia EB institucijų susirūpinimą tuo, jog asmens duomenų rinkimas, kaupimas, tvarkymas ir pan. tampa kasdieniniu reiškiniu daugelyje ekonominių ir socialinių sferų. Tuo pačiu informacinių technologijų vystymasis ypatingai pagreitina asmens duomenų rinkimą ir apsikeitimą jais[34].

Radikaliai išaugęs mokslinio ir techninio bendradarbiavimo ir koordinavimo poreikis, susijęs su naujų telekomunikacinių tinklų įdiegimu neišvengiamai susijęs su milžiniškais asmens duomenų srautais[35]. Skirtingi nacionaliniai asmens duomenų apsaugos režimai gali tapti viena pagrindinių kliūčių sklandžiam asmens duomenų judėjimui, todėl Direktyva siekiama visose valstybėse narėse įtvirtinti visuotinai privalomą asmens duomenų apsaugos minimumą tokiu būdu garantuojant efektyvų EB vidaus rinkos funkcionavimą, pagrįstą netrukdomu asmens duomenų judėjimu[36]. Suvienodinus valstybių narių įstatymus asmens duomenų apsaugos srityje visoje EB vidaus rinkoje bus pasiektas ekvivalentiškas asmens duomenų apsaugos lygis ir valstybės narės nebegalės riboti asmens duomenų judėjimo pagrindais, susijusias su žmogaus teisių, žmogaus teisės į privatumą, apsauga.

---

[32] Direktyvos 1 straipsnis // http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas : 2006-05-10.
[33] Direktyvos 10 įžanginė citata// http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas: 2006-05-10.
[34] Direktyvos 4 įžanginė citata// http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas: 2006-05-10.
[35] Direktyvos 6 įžanginė citata// http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas: 2006-05-10.
[36] Direktyvos 7 įžanginė citata// http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas: 2006-05-10.

Dauguma Europos šalių kontroliuoja asmeninių duomenų judėjimą tarpvalstybiniu lygiu taikydamos nacionalinės teisės reikalavimus užsienyje (pvz. Olandija) arba reikalaudamos būti informuotos prieš pradedant naudoti duomenis ir suderinti naudojimo tikslus. Austrija, Norvegija, Portugalija ir Švedija reikalauja kitos šalies duomenų apsaugos organo garantijų dėl saugumo prieš eksportuojant duomenis, tuo tarpu Prancūzija prašo tik išankstinio perspėjimo dėl duomenų naudojimo kitoje šalyje. Lietuvoje pagal ADTAĮ 28 straipsnio 1 dalį „asmens duomenys teikiami duomenų gavėjams užsienio valstybėse, gavus Valstybinės duomenų apsaugos inspekcijos leidimą, išskyrus šio straipsnio 4 dalyje nustatytus atvejus[37]“. Toliau įstatyme teigiama, jog valstybinė duomenų apsaugos inspekcija išduoda leidimą teikti asmens duomenis į užsienio valstybes, jei šiose valstybėse yra tinkamas asmens duomenų teisinės apsaugos lygis. Asmens duomenų teisinės apsaugos lygis vertinamas atsižvelgiant į visas aplinkybes, susijusias su duomenų teikimu, ypač į užsienio šalyje, į kurią teikiami asmens duomenys, galiojančius įstatymus bei kitus teisės aktus, užtikrinančius asmens duomenų teisinę apsaugą, į teikiamų duomenų pobūdį, duomenų tvarkymo būdus, tikslus, trukmę, saugumo priemones, kurių bus laikomasi toje valstybėje[38].

Taigi, visose Europos Sąjungos šalyse narėse galioja dalis bendrų teisinių aktų susijusių su duomenų apsauga, ir jie yra viršesni už nacionalinės teisės aktus, tačiau galima teigti, jog pavyzdžiui, Lietuvoje, Duomenų Apsaugos Akto atitikmuo yra ADTAĮ. Lietuvai įstojus į Europos Sąjunga įsigaliojo ir ES direktyvos ir kiti sąjungoje taikomi teisiniai dokumentai, kurie kaip minėta anksčiau yra viršesni už nacionalinės teisės aktus. ADTAĮ ir kitų Lietuvoje taikomų teisinių aktų susijusių su duomenų apsaugą apžvalga pateikta sekančiame skyrelyje.

1.2.2. Teisinis reglamentavimas Lietuvoje

Lietuvoje duomenų apsaugą reglamentuoja tokie pagrindiniai įstatymai:

- Asmens duomenų teisinės apsaugos įstatymas (aktuali redakcija nuo 2004-04-13)[39];
- Įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr.108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis ratifikavimo (aktuali redakcija nuo 2001-04-13)[40];

[37] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios 2003, Nr. 15- 597.
[38] Ten pat.
[39] Ten pat.
[40] Lietuvos Respublikos įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis ratifikavimo // Valstybės žinios 2001, Nr.32-1055.

- Įstatymas „Dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomo protokolo dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų ratifikavimo“ (aktuali redakcija nuo 2004 03 07)[41];
- Elektroninių ryšių įstatymas (aktuali redakcija nuo 2004-05-01)[42];
- Įstatymas dėl Konvencijos dėl informacijos technologijos naudojimo muitinės tikslais, parengtos vadovaujantis Europos Sąjungos sutarties K.3 straipsniu, jos protokolų ir Susitarimo dėl laikino Konvencijos taikymo ratifikavimo (aktuali redakcija nuo 2004-05-01)[43];
- Įstatymas dėl Konvencijos, parengtos vadovaujantis Europos Sąjungos sutarties K.3 straipsniu, dėl Europos policijos biuro įsteigimo (Europolo konvencijos) ir jos protokolų ratifikavimo (aktuali redakcija nuo 2004-05-01)[44];
- Administracinių teisės pažeidimų kodeksas (aktuali redakcija nuo 2005-06-16) (straipsniai 214(14), 214(15) , 214(16), 214(17) , 214(23), 259 (1))[45];
- Direktyva 95/46/EB, pagal kurią valstybės narės saugo fizinių asmenų pagrindines teises ir laisves, o ypač jų privatumo teisę tvarkant asmens duomenis, nevaržo ir nedraudžia laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su apsauga[46].

Pagrindinis teisinis dokumentas Lietuvoje reguliuojantis duomenų apsaugą yra Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas. Šis įstatymas pilietį įvardina duomenų subjektu, o tvarkančius asmens duomenis - duomenų valdytojais ir duomenų tvarkytojais[47] .

Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas reguliuoja santykius, atsirandančius renkant, kaupiant, apdorojant, saugant, naudojant ir teikiant duomenis apie fizinius asmenis informacinėms sistemoms arba kitokiam su tuo susijusiam arba galimam susieti duomenų tvarkymui (toliau – informacinėms sistemoms).

Įstatymo tikslas – nustatyti duomenų subjektų teises ir šių teisių apsaugos tvarką, teisių į duomenis bei duomenų apsaugos garantijas tvarkant asmens duomenis informacinėse sistemose.

---

[41] Lietuvos Respublikos įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomo protokolo dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų ratifikavimo // Valstybės žinios, 2004, Nr.36-1177.

[42] Lietuvos Respublikos elektroninių ryšių įstatymas // Valstybės žinios, 2004, Nr.69-2382.

[43] Teisinė bazė // http://www.ada.lt/index.php?lng=lt&action=page&id=69; prisijungimo laikas 2006-06-05.

[44] Lietuvos Respublikos įstatymas dėl Konvencijos, parengtos vadovaujantis Europos Sąjungos sutarties K.3 straipsniu, dėl Europos policijos biuro įsteigimo (Europolo konvencijos) ir jos protokolų ratifikavimo// Valstybės žinios, 2004, Nr.69-2384.

[45] Lietuvos Respublikos administracinių teisės pažeidimų kodeksas // Valstybės žinios 2005, Nr. 149-5421.

[46] Privacy law // http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas 2006-05-10.

[47] žr. 1.1. skyrelį.

Šis įstatymas saugo asmens duomenis, tarp jų ir ypatingus asmens duomenis, kurių tvarkymas ar teikimas gali padaryti žalos pačiam duomenų subjektui ar su juo susijusiems asmenims.

Duomenų subjektai turi teisę susipažinti su savo duomenimis ir juos patikslinti. Jie taip pat turi teisę gauti informaciją, iš kokių šaltinių gauti duomenys, kokiu tikslu ir kada jie buvo panaudoti, yra naudojami arba gali būti panaudoti.

Pagal ADTAĮ, visos organizacijos, kaupiančios informaciją apie privačius asmenis kompiuterine forma (telekomunikacijų operatoriai, komunalinių paslaugų įmonės) turi registruotis kaip asmens duomenų valdytojai ir užtikrinti saugomų duomenų apsaugą. Asmens duomenų teisinės apsaugos įstatymo vykdymą prižiūri Valstybinė duomenų apsaugos inspekcija. Jos svetainėje[48] galima rasti pilną informaciją įmonėms - asmens duomenų saugotojoms: registravimo procedūrą, reikalaujamas pateikti ataskaitas, keliamus saugumo reikalavimus. Be asmens duomenų apsaugos įstatymo, informacinių technologijų saugumo klausimai aptariami ir kituose įstatymuose, tarp jų ir Elektroninio parašo bei Valstybės paslapčių. Kadangi elektroninio parašo infrastruktūra Lietuvoje dar neišplėtota, nevykdoma šiuo parašu pagrįsta veikla, kol kas anksti kalbėti apie šio įstatymo taikymo niuansus[49].

Tvarkydamos asmens duomenis valstybės institucijos taip pat privalo garantuoti duomenų saugumą. Tai apima organizacines ir technines priemones, siekiant užkirsti kelią bet kokiam atsitiktiniam ar neteisėtam duomenų sunaikinimui, pakeitimui, atskleidimui ar kitokiam neteisėtam jų tvarkymui.

Valstybinė duomenų apsaugos inspekcija atsakinga už Asmens duomenų teisinės apsaugos įstatymo, išskyrus 8 straipsnį, vykdymo priežiūrą ir kontrolę bei už Elektroninių ryšių įstatymo devintojo skirsnio „Asmens duomenų tvarkymas ir privatumo apsauga“ straipsnių nuostatų (išskyrus minėto Įstatymo 63 straipsnio 5 dalies, 65 straipsnio 4 dalies ir 70 straipsnio 7 dalies nuostatas), įgyvendinimą. Lietuvos Respublikos Vyriausybė 2004 m. gruodžio 6 d. nutarimo Nr. 1593 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą“ 4 punktu įgaliojo Inspekciją vykdyti elektroninių ryšių paslaugų naudotojų privataus gyvenimo neliečiamumo užtikrinimo kontrolę Lietuvos Respublikos Vyriausybės nustatyta tvarka. Lietuvos Respublikos Vyriausybė 2005 m. liepos 20 d. nutarimu Nr. 807 patvirtino Ryšio slaptumo patikrinimų atlikimo taisykles, kurios nustato Inspekcijos atliekamų patikrinimų, ar laikomasi Elektroninių ryšių įstatymo

[48] Asmens duomenų apsaugos inspekcijos internetinė svetainė // www.ada.lt; prisijungimo laikas 2006-04-28.
[49] A. Jankūnas, A. Klibas. Informacijos technologijos. Vilnius, Verslo žinios, 2005.

63 straipsnio 1 dalies reikalavimų užtikrinti ryšio slaptumą, ir šių patikrinimų rezultatų įforminimo procedūras[50].

Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komitetas 2005 m. balandžio 18 d. priėmė sprendimą Nr. 9 „Dėl valstybės informacinių sistemų apsaugos stiprinimo“, kuriame konstatavo, kad nėra užtikrintas saugus valstybės informacinėse sistemose esančios informacijos vartojimas bei nėra garantuota asmens teisė į privačių duomenų apsaugą, bei pasiūlė Valstybinei duomenų apsaugos inspekcijai stiprinti prevencinę veiklą, o tikrinant asmens duomenų tvarkymo teisėtumą daugiau dėmesio skirti organizacinių, techninių duomenų apsaugos priemonių patikrinimams. Tai buvo vienas iš politinių veiksnių nagrinėjant aplinkos išteklius ir sudarinėjant 2006 – 2008 metų Valstybinės duomenų apsaugos inspekcijos strateginį planą. Darbo autorė sutinka su Valstybinės duomenų apsaugos inspekcijos strateginio planavimo grupės Strateginiame 2006-2008 metų plane išreikštomis galimybėmis dėl teisinės bazės tobulinimo įvedant duomenų apaugos įgaliotinio pareigybę[51] bei duomenų subjekto supratimo duomenų apsaugos srityje didinimo.

Apibendrinant galima teigti, jog Nacionalinio saugumo ir gynybos komiteto sprendimas aiškiai parodo, jog Lietuvoje reikalingas duomenų apsaugos auditas, kuris padėtų stiprinti asmens duomenų apsaugą Lietuvoje.

1.3. Duomenų apsaugos audito formos, metodai ir etapai

Kaip jau minėta anksčiau, duomenų apsaugos auditas turi įvertinti ar organizacija laikosi teisinės bazės reikalavimų ir kaip vykdoma duomenų apsauga organizacijoje. Didžiosios Britanijos sudarytame duomenų apsaugos audito vadove teigiama, jog šiandien vartojama daug įvairių audito rūšių. Tuo tarpu duomenų apsaugos auditas yra tik trijų rūšių[52]. Visos jos pateiktos 1 lentelėje.

1 lentelė. **Didžiosios Britanijos Duomenų apsaugos audito rūšys[53]**

Apibūdinimas	**Audito rūšis**	**Organizuojama**
Pirmo asmens	Vidinis	Pačios organizacijos
Antro asmens	Tiekėjų	Pačios organizacijos ir tiekėjo sutarties sąlygomis
Trečio asmens	Išorinis	Nepriklausomų konsultantų

[50] Valstybinės duomenų apsaugos inspekcijos 2006-2008 –ųjų metų strateginis veiklos planas // www.ada.lt/images/cms/File/Teises%20aktai/2.pdf; prisijungimo laikas 2006-05-10.
[51] Ten pat.
[52] Data protection audit manual // http://www.ico.gov.uk/documentUploads/the_complete_audit_guide.pdf; prisijungimo laikas: 2006-05-10.
[53] Ten pat.

Kaip matyti iš 1 lentelėje pateiktų duomenų apsaugos auditas gali būti vidinis, dar vadinamas pirmo asmens auditu, tiekėjų, arba antro asmens auditas ir išorinis arba trečio asmens auditas. Priklausomai nuo audito rūšies skirtingi ir jį organizuojantys asmenys. Vidinį auditą atlieka pačios organizacijos, o išorinį – nepriklausomi konsultantai. Galima teigti, jog tiek vidiniai tiek išoriniai auditoriai turi būti nepriklausomi ir kompetentingi, norėdami kuo efektyviau atlikti auditą.

Nepriklausomai nuo audito rūšies, atliekant duomenų apsaugos auditą auditorius turi tris pagrindinius tikslus:

1. Patikrinti ar yra formali duomenų apsaugos sistema:
    - Sistema turi būti dokumentuota;
    - Sistema turi būti atnaujinama
2. Patikrinti ar visi darbuotojai yra įtraukti į duomenų apsaugą, t.y.:
    - Yra informuoti apie duomenų apsaugos sistemos buvimą;
    - Supranta duomenų apsaugos sistemą;
    - Naudoja duomenų apsaugos sistemą;
3. Patikrinti ar duomenų apsaugos sistema veikia ir yra efektyvi, t.y.:
    - Metodologija yra paremta kitų sektorių įrodytais metodais
    - Taikoma tiek profesionalių auditorių, tiek ne specialistų;
    - Gali būti naudojama išorinių ir vidinių auditorių bei Duomenų Apsaugos inspektorių;

Apibendrintai galima teigti, jog duomenų apsaugos auditas turėtų atsakyti į 2 pagrindinius klausimus:

- Kokius duomenis organizacija valdo ir operuoja?
- Ar duomenų perdavimas ir jų valdymas atitinka duomenų apsaugos teisinių aktų reikalavimus?

Atliekant duomenų apsaugos auditą labai svarbu apklausti visus darbuotojus, kurie tiesiogiai susiję su duomenų rinkimu, saugojimu ir sklaida. Pagal Sh. Gaskill atliekant duomenų apsaugos auditą būtina apklausti visus tiesiogiai su duomenų apsauga susijusius darbuotojus. Klausimynas turėtų apimti tokias sritis[54]:

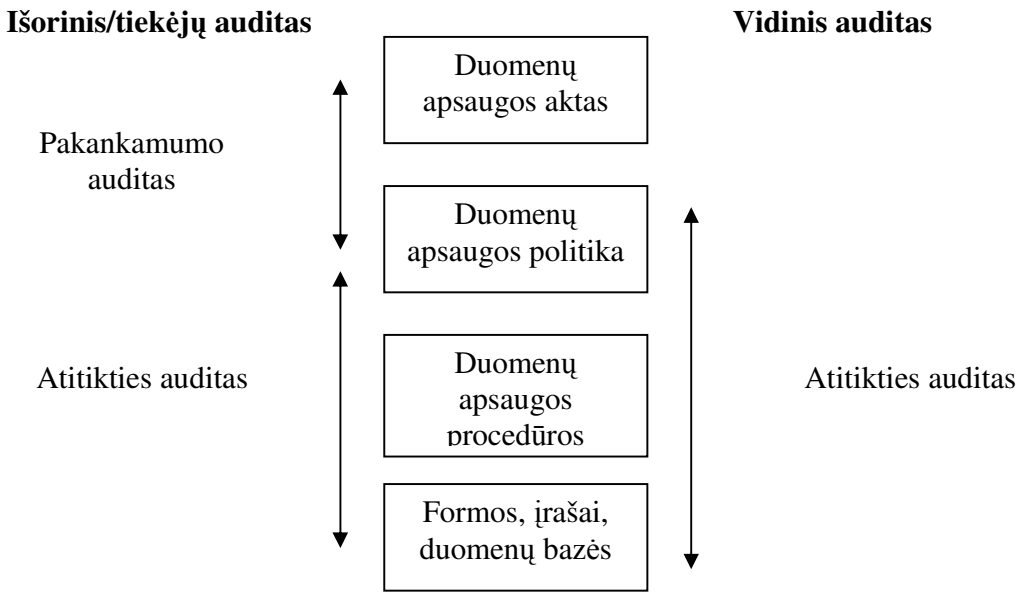
- Duomenų rinkimas;
- Saugojimas;

[54] Interneto technologijos // http://www.ukuug.org/events/winter99; prisijungimo laikas 2006-05-25.

- Priėjimas prie duomenų;
- Duomenų apdorojimas;
- Duomenų atskleidimas;
- Duomenų sauga;
- Duomenų archyvavimas;
- Duomenų eksportas.

Be klausimyno, kiekvienas auditorius turėtų surinkti informaciją apie vidinius ir išorinius asmenis, su kuriais organizacija dalijasi duomenimis.

Pagal Didžiojoje Britanijoje parengtą duomenų apsaugos audito vadovą audito metodologija susideda iš Pakankamumo ir Atitikties (*ang. compliance*) audito (žr. 1 pav.).



1 pav. Audito metodologija [55]

Galima teigti, jog vidinis iš išorinis auditai ieško skirtingų duomenų apsaugos įrodymų. Iš 2 lentelės matyti, kad tarp pakankamumo ir atitikties audito yra skirtumai, t.y. pakankamumo audito įrodymai yra susiję su teisine baze, o atitikties auditui svarbu ar duomenų apsauga iš viso egzistuoja, yra naudojama ir ar ji naudojama efektyviai.

[55] Data protection audit manual // http://www.ico.gov.uk/documentUploads/the_complete_audit_guide.pdf; prisijungimo laikas: 2006-05-10.

2 lentelė. **Audito įrodymai**

Audito tikslas	**Įrodymo rinkimas**	**Pakankamumo auditas**	**Atitikties auditas**
Apsaugos sistema egzistuoja ir yra pakankama	Dokumentacija, teisinė bazė, procedūros	Taip	Taip
Apsaugos sistema yra naudojama	Subjektų įrašai, nusiskundimai	Ne	Taip
Sistema naudojama efektyviai	Sistemos atnaujinimas, tobulinimas	Ne	Taip

Prieš imantis tikrojo duomenų apsaugos audito kiekvienas auditorius turėtų susipažinti su kliento organizacijos veikla. Auditoriui labai svarbu suprasti pačią kliento vykdomą veiklą, kasdienines operacijas, apimančias asmens duomenis tam, kad vykdant auditą jis atsižvelgtų tik į svarbius veiklos aspektus. Šis pažinimo procesas dažniausiai apima vieną arba dvi darbo dienas.

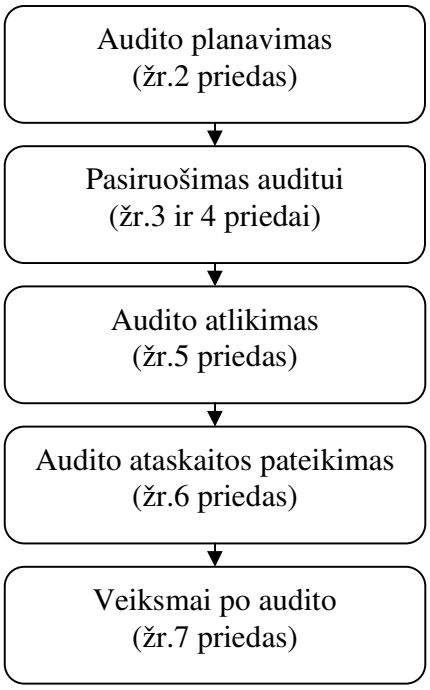
Pilnas duomenų apsaugos auditas apima keletą etapų. Pagal G. Collier pirmasis etapas yra *patikrinti* pagrindinius už duomenų apsaugą atakingus asmenis[56]. *Tyrimo* etape atliekamas interviu arba duodamas klausimynas, kurį asmuo užpildo pats. Po to seka *duomenų tvarkymo analizė*. Šiame etape yra svarbu įvertinti duomenų apsaugos riziką ir įvairias duomenų tvarkymo operacijas. Atliekant duomenų apsaugos auditą labai svarbu patikrinti ne tik skaitmeninėse laikmenose laikomus duomenis bet ir galimybę įsilaužti į kompiuterinius tinklus, o taip pat internetinės svetainės, jei tokią organizacija turi, saugumą.

Bendravimas su darbuotojais/tarnautojais apims du būdus:

- Darbuotojų apklausa per funkcinį bei procedūrinį auditus, naudojant Audito kontrolinį sąrašą;
- Darbuotojų įsisąmonino interviu (akis į akį arba Fokus grupėse).

Pagal Duomenų apsaugos audito vadovą duomenų apsaugos auditas susideda iš 2 paveiksle pavaizduotų etapų.

[56] G. Collier. Information privacy: Just how private are the private details of individuals in a company's database? // Information Management & Computer Security. 1995 , Nr. 3 (1). P. 43.



2 pav. Duomenų apsaugos audito etapai[57]

Toliau pateikiamas trumpas kiekvieno etapo apibūdinimas ir būdingi etapui elementai.

Audito planavimas – labai svarbus duomenų apsaugos audito etapas. Yra teigiama, kad kuo daugiau pastangų auditorius įdės į audito planavimą, tuo efektyviau jis atliks suplanuotą auditą. Šiam išankstiniam etapui rekomenduojama skirti 25 % viso audito laiko[58]. 2 priede pavaizduotas audito planavimo etapas schematiškai. Apibendrintai galima teigti, jog audito planavimo etapą sudaro[59]:

- Rizikos įvertinimas;
- Audito tvarkaraščio sudarymas;
- Atranka;
- Išankstinių audito klausimų sudarymas;
- Išankstinis susitikimas/apsilankymas organizacijoje;
- Audito valdymo kontrolinio sąrašo sudarymas.

[57] Data protection audit manual // http://www.ico.gov.uk/documentUploads/the_complete_audit_guide.pdf; prisijungimo laikas: 2006-05-10.
[58] Ten pat.
[59] Data protection auditing // www.isaca-london.org/presentations/ ISACA%20Data%20Protection%20Auditing.ppt; prisijungimo laikas: 2006-05-25.

Jau anksčiau minėta, kad kuo daugiau dėmesio skiriama audito planavimui, tuo sėkmingesnis bus auditas. Tą patį galima pasakyti ir apie pasiruošimo auditui etapą. Audito pasiruošimo etapas, tai etapas po auditoriaus ir kliento susitikimo, iki pačio audito atlikimo[60]. Smulki audito pasiruošimo etapo schema pateikta 3 ir 4 prieduose. Pagrindiniai darbai šiame etape yra:

- Pakankamumo auditas;
- Audito tvarkaraščio patvirtinimas;
- Pavyzdžių atrinkimo kriterijų nustatymas;
- Audito plano sudarymas.

Sekantis ir tikrai ne mažiau svarbus audito etapas – tai pačio audito atlikimas. Audito atlikimas priklauso nuo auditoriaus patirties, organizacijos aplinkos ir kitų faktorių. 5 priede pavaizduoti audito atlikimo darbai „žingsnis po žingsnio“. Šie etape auditoriui labai svarbu surinkti audito įrodymus ir pasiruošti ataskaitos pateikimui. Pagal Duomenų apsaugos vadovą pagrindiniai audito atlikimo etapai yra:

- Susitikimas su klientu;
- Audito aplinkos ištyrimas;
- Audito vykdymas (funkcinis auditas, procesų auditas, darbuotojų interviu, teigiamų ir neigiamų rezultatų užrašymas).

Priešpaskutinis duomenų apsaugos audito etapas yra audito ataskaitos pateikimas. Šis etapas atskleistas 6 priede. Duomenų apsaugos audito vadove galima rasti kokios turi būti audito ataskaitos dalys (kaip išdėstytos ir t.t.), taip pat rekomendacijos kaip paskleisti ataskaitą suinteresuotoms šalims.

Paskutinis, bet ne mažiau svarbus, etapas yra veiksmai po audito (ang. follow – up). Pagrindinė jo paskirtis – įvertinti kaip įgyvendinamos audito rekomendacijos. Auditorius turi domėtis savo atliktu auditu, palaikyti ryšį su klientu. Čia galima pasinaudoti J. Mackevičiaus rekomendacijomis finansiniam auditui, kuris tinka ir duomenų apsaugos auditui, t.y. auditorius turėtų bendrauti su kliento vadovybe ir išsiaiškinti, ar:

- Trūkumai bei nesklandumai, nurodyti auditoriaus ataskaitoje, yra pašalinti;

[60] Data protection audit manual // http://www.ico.gov.uk/documentUploads/the_complete_audit_guide.pdf; prisijungimo laikas: 2006-05-10.

- Reaguojama į auditoriaus pateiktus pasiūlymus įmonės valdymo ir finansinės apskaitos, kontrolės sistemoms ar konkrečioms veiklos sritims gerinti[61].

Apibendrintai galima teigti, jog atlikto audito kontrolės etapą reikėtų vertinti kaip audito kokybės gerinimo etapą, nes jo metu naginėjama audito atlikimo kokybė, išaiškinami sėkmingai atlikti dalykai arba padarytos klaidos, įvertinamas konkrečių auditorių vaidmuo.

Atskleidus audito etapus galima nesunkiai įsivaizduoti visą audito procesą: iš pradžių sukuriamas planas. Vėliau auditorius pasiruošia auditui. Pagal audito planą ir tikslus renkama reikalinga auditui medžiaga, ji tikrinama. Patikrinus medžiagą auditorius rašo ataskaitą ir teikia savo išvadą dėl audituojamo subjekto duomenų apsaugos. Po ataskaitos pateikimo auditoriui rekomenduojama vykdyti atlikto audito kontrolę – t.y. patikrinti ar audituojamoji įmonė laikosi rekomendacijų, taiso savo klaidas ir t.t.

Atlikti duomenų apsaugos auditą galima ir pasinaudojus dar vienu literatūroje aprašytų būdu, t.y. procedūriniu auditu. Tai formalus įvertinimas, kurį pagal tam tikrą metodologiją atlieka tai išmanantys specialistai. Metodologija - tarsi formalus rinkinys principų, į kuriuos reikia atsižvelgti atliekant auditą. Labai svarbus procedūrinio audito aspektas - patikrinimas, ar veiksmingai veikia įdiegtos saugumo priemonės.

Iš tokių saugumo metodologijų standartu *de facto* tapo ISO standartas 17799, kuris savo ruožtu atsirado iš britų standarto BS 7799. Standartas rekomenduoja[62]:

- Turėti Saugumo politikos dokumentą;
- Nustatyti atsakingus asmenis;
- Informuoti ir mokyti naudotojus;
- Reaguoti į saugumo incidentus;
- Kontroliuoti virusus;
- Turėti veiklos tęstinumo planą;
- Kontroliuoti informacijos srautus;
- Apsaugoti duomenis nuo praradimo;
- Užtikrinti įstatymų vykdymą;
- Turėti priemones, padedančias įrodyti atitikimą saugumo politikai.

Procedūriniai auditai atliekami formaliai, užpildant visus reikiamus dokumentus, numatytus metodologijoje. Procedūrinis auditas sąlygiškai yra ilgas ir brangus procesas, galintis kainuoti net

[61] Mackevičius, Jonas. Audito teorija ir praktika: monografija. Vilnius: Lietuvos mokslų akademija, 1999. P. 179.
[62] A. Jankūnas, A. Klibas. Informacijos technologijos. Vilnius, Verslo žinios, 2005.

šimtus tūkstančių litų. Paprastai juos atlieka tik didelės organizacijos. Pastaruoju metu šių auditų poreikis auga pasauliniu mastu.

Apibendrintai galima teigti, jog pats duomenų apsaugos auditas, visai nepriklausomai nuo organizacijos vykdomos veiklos turi:

- Nustatyti, kad kliento tvarkomi duomenys yra duomenų apsaugos objektas;
- Nustatyti duomenų surinkimo metodus (pavyzdžiui duomenys gali būti surenkami įvairių renginių, mugių metu, naudojant telefonų skriptus, interneto puslapiuose, paraiškos formomis ir t.t.) ir patikrinti ar jie surenkami sąžiningai ir teisingai;
- Nustatyti teisėtumo taisykles tvarkant duomenis;
- Nustatyti ypatingų asmeninių duomenų laikymo ir tvarkymo pateisinančias priežastis;
- Patikrinti ar asmeniniai duomenys vartojami pagal jų surinkimo tikslą ir ar jie yra sunaikinami pasiekus šį tikslą;
- Išsiaiškinti kokius asmeninius duomenis organizacija atskleidė kitoms šalims;
- Išsiaiškinti kokius duomenis organizacija paskelbė už valstybės ribų ir kodėl;
- Patikrinti ar yra atpažinimo ir patikrinimo asmens prisijungimo procedūros bei išanalizuoti ar duomenys efektyviai saugomi;

Iš kitų valstybių praktikos paaiškėjo, kad yra tam tikros sritys, kuriose asmens duomenų apsauga yra daug svarbesnė nei kitose. Tokios sritys yra tiesioginis marketingas, telekomunikacijų paslaugos ir pan.[63]. Todėl atliekant duomenų apsaugos auditą labai svarbu suprasti srities reikšmingumą ir įvertinti galimą audito riziką.

Duomenų apsaugos audito pasirinkimą gali lemti daugelis veiksnių tokių kaip kaštai, laiko sąnaudos, auditoriaus išsilavinimas, audito tikslas ir t.t. Kad ir kokią duomenų apsaugos audito rūšį pasirinktų auditorius (pakankamumo ir atitikties ar procedūrinį) šis auditas turėtų padėti organizacijai efektyviai valdyti asmens duomenys ir apginti asmens privatumo laisvę. Šiuo metu asmens duomenų apsaugos srityje susiduriant su tokiomis grėsmėmis kaip spartaus naujų informacinių technologijų vystymusi, kuris sąlygoja asmens duomenų apsaugos ypatumus, aukštos kvalifikacijos duomenų apsaugos specialistų trūkumu Lietuvoje bei ypač sparčiai didėjančiu duomenų teikimo kompiuterių tinklais mastu (ypač valstybės registrų ir informacinių sistemų) asmens duomenų apsaugos audito aktualumas tik didėja. Tai parodo ir atliktas asmens duomenų apsaugos tyrimas biudžetinėse duomenų valdytojų įstaigose Lietuvoje.

[63] G. Collier. Information privacy: Just how private are the private details of individuals in a company's database? // Information Management & Computer Security. 1995 , Nr. 3 (1). P. 43.

2. ASMENS DUOMENŲ APSAUGOS IR AUDITO YPATUMAI LIETUVOJE, BIUDŽETINĖSE DUOMENŲ VALDYTOJŲ ORGANIZACIJOSE

Valstybinės institucijos vykdydamos savo pareigas turi surinkti daug informacijos apie piliečius, ją saugoti, perduoti kitiems asmenims, tam tikru būdu naudoti ir panaudotus duomenis sunaikinti, kai jie yra nebereikalingi. Tačiau informacija apie asmenį skiriasi nuo bet kokių kitų duomenų. Šie duomenys yra susiję su žmogumi, galbūt atspindi kai kurias jo ar jos savybes, patirtį ar požiūrį į gyvenimą. Duomenų apsaugos inspekcijos parengtame lankstinuke teigiama, kad demokratinėje teisinėje visuomenėje asmens teisės yra svarbiausios. Viena iš šių teisių yra teisė į privatumą ir duomenų apsaugą, kurią saugo Lietuvos Konstitucija, ES pagrindinių teisių chartija, kiti tarptautiniai dokumentai. Ji taip pat apima teisę savarankiškai priimti sprendimus dėl asmens duomenų naudojimo. Dėl minėtų priežasčių, norėdamos tvarkyti asmens duomenis, valstybės institucijos turi turėti tam teisinį pagrindą. Daugeliu atvejų šį pagrindą joms suteikia koks nors konkretus įstatymas arba bendro pobūdžio duomenų apsaugą reglamentuojantis įstatymas: Asmens duomenų teisinės apsaugos įstatymas (ADTAĮ)[64].

Keletą bendrųjų teisėto duomenų tvarkymo teisinių pagrindų numato ADTAĮ 5 straipsnis; kiti įstatymo straipsniai numato specialias nuostatas. Be to, privaloma vadovautis teisėto duomenų tvarkymo principais. ADTAĮ 3 straipsnis be kita ko numato, kad asmens duomenys gali būti renkami tik konkrečiam ir teisėtam tikslui ir ne daugiau nei jų reikia, tai yra, galima rinkti tik konkrečiai užduočiai reikalingus duomenis. Todėl darbe buvo aktualu išsiaiškinti kaip duomenų valdytojai (t.y. juridiniai asmenys, kurie vieni arba drauge su kitais nustato asmens duomenų tvarkymo tikslus ir priemones) elgiasi su asmens duomenimis. Darbe buvo pasirinkta išnagrinėti biudžetines duomenų valdytojų registruotas įstaigas. Tyrimo metodika ir gauti rezultatai pateikiami sekančiuose poskyriuose.

2.1. Biudžetinių duomenų valdytojų organizacijų tyrimo metodikos pagrindimas

Teorinėje dalyje išsiaiškinus duomenų apsaugos audito reikšmę ir teisinį reglamentavimą, nustačius duomenų apsaugos audito formas, metodus ir etapus toliau pasirinkta ištirti biudžetinių

[64] Lankstinukai duomenų apsaugos klausimais // http://www.ada.lt/index.php?lng=lt&action=page&id=256; prisijungimo laikas: 2006-05-15.

(išskyrus švietimo įstaigų) duomenų valdytojų įstaigas registruotas Valstybinės duomenų inspekcijos valdomame duomenų valdytojų registre. Išanalizavus visus pirminių duomenų rinkimo metodus (apklausą, stebėjimą ir eksperimentą) pasirinkta anketinė apklausa raštu. Stebėjimui ir eksperimentui nebuvo tinkamų sąlygų. Be to, anketavimo metodas pasirinktas dėl laiko ir kaštų sąnaudų teikiamų privalumų bei plačios „geografijos“. Tyrimo metu taikyta individuali anketinė apklausa, t.y. anketa buvo išsiųsta elektroniniu paštu bendrais duomenų valdytojų internetinėse svetainėse pateiktais adresais su tyrimo pristatomuoju ir paaiškinamuoju laišku. Pagrindiniai individualaus anketavimo privalumai pagal I. Luobikienę yra tokie[65]:

- Respondentas gali skirti tam kiek norima laiko;
- Respondento neveikia aplinka ir pats apklausėjas.

Tai buvo pagrindinės priežastys pasirenkant individualią anketinę apklausą elektroniniu paštu.

Tyrimas vyko tris savaites, tai nebuvo brangus metodas, nes apklausa vyko elektroniniu paštu, todėl neteko patirti popieriaus kaštų sąnaudų ir pašto siuntimo išlaidų. Tačiau darbo autorė susidūrė su kita problema – negrįžusiomis anketomis.

Šio tyrimo pasirinktoji populiacija, t.y. visi objektai, kurie turi darbo autorę dominantį požymį yra - duomenų valdytojai, užsiregistravę asmens duomenų valdytojų registre[66].

Iš viso nuo 1991m. sausio 1 d. iki 2006m. lapkričio1d. asmens duomenų valdytojų registre įregistruoti 2622 asmens duomenų valdytojai (žr. 3 lentelę).

3 lentelė. **Duomenų valdytojai Lietuvoje**

Duomenų valdytojų registravimo statistika	
Įregistruoti	2622
Laikinai įregistruoti	0
Išregistruoti	935
Patikslinti registravimo duomenys	508

Iš lentelės matyti, kad per tą patį laikotarpį išregistruoti 935 duomenų valdytojai, t.y. beveik 36 proc. visų per minėtą laikotarpį įregistruotų valdytojų. Asmens duomenų valdytojų valstybės registre yra išskirtos 27 duomenų tvarkymo tikslų grupės, t.y.:

- 85 advokatų paslaugos teikiantys valdytojai;

[65] Luobikienė I. Socialinių tyrimų metodika: mokomoji knyga. – Kaunas: Technologija, 2002. P.84.
[66] Internetinės svetainės adresas - http://db.ada.lt/.

- 132 antstoliai;
- 9 aukštojo mokslo įstaigos;
- 15 bankų;
- 1232 bendrojo lavinimo įstaigų;
- 57 draudimo organizacijos;
- 144 komunalinių paslaugų bendrovės;
- 17 lizingo organizacijų;
- 20 finansinio tarpininkavimo įmonių;
- 108 ikimokyklinio ugdymo organizacijų;
- 13 Jungtinių skolininkų duomenų rinkmenų tvarkymo įmonių;
- 40 kelionių agentūrų;
- 291 kitos įstaigos;
- 61 kita švietimo veiklą organizuojanti įmonė;
- 4 pašto paslaugas teikiančios įmonės;
- 44 personalo atranką vykdančios įmonės;
- 79 prekybos įmonės;
- 42 profesinio ir aukštesniojo mokymo institucijos;
- 47 savivaldybės;
- 3 statistikos įstaigos;
- 81 telekomunikacijų bendrovė;
- 125 tiesioginės rinkodaros bendrovės;
- 13 valstybės ir žinybinius registrus tvarkančios įstaigos;
- 66 viešbučių veiklą vykdančios įmonės;
- 6 žemės ūkio bendrovės.

Bendram duomenų apsaugos lygiui įvertinti ir tyrimui atlikti buvo pasirinktos organizacijos pagal juridinio asmens rūšį, t.y. biudžetinės įstaigos (išskyrus švietimo įstaigas). Asmens duomenų valdytojų registre iš viso įregistruotos 197 tokios įmonės (2006 lapkričio 1 dienos duomenimis).

Žinant šiuos duomenis galima paskaičiuoti imties dydį. Pirmiausiai paskaičiuojame biudžetinių įstaigų procentą visoje populiacijoje. Žinome, jog visoje populiacijoje yra 2622 registruoti asmens duomenų tvarkytojai, iš jų 197 – tyrėją dominančios įmonė. Jos sudaro 3,7 proc. visos populiacijos (197 *1 00 / 2262 =3,7).

Žinodami šį skaičių galime paskaičiuoti imties vidutinį standartinį nuokrypį (S). Jis randamas iš formulės:

$$S = \sqrt{\% * (100 - \%)} \quad \text{t.y. } S = \sqrt{3,7 * (100 - 3,7)} = \sqrt{3,7 * 96,3}$$

Toliau pasirinktas 3, 5 proc. tikslumas (Δ) ir 95 proc. patikimumas (z). Tokiu būdu Δ = 3,5, o z = 1.96 [67]. Reikimas imties tūris apskaičiuojamas pagal formulę:

$$n = \frac{z^2 * S^2}{\Delta^2}, \text{ t.y. } n = \frac{1.96^2 * 3,7 * 96,3}{3,5^2} = \frac{1368,8}{12,25} \approx 112$$

Siekiant tyrimo reprezentatyvumo imties elementai buvo atrinkti atsitiktiniu būdu. Populiacijos elementų skaičius buvo baigtinis, todėl paprasčiausiai buvo pasirinkti *tikimybinę sistemingąją* imtį. Visi elementai jau asmens duomenų valdytojų registre buvo surikiuoti į eilę, darbo autorė tik nustatė jų atrankos žingsnį, t.y."2". Mažas žingsnis buvo pasirinktas dėl to, kad tiriamojoje visumoje nedaug imties elementų, o pagal paskaičiavimus reikėjo pasiekti 112 imties tūrį. Šis metodas padėjo iš visų tiriamųjų išrinkti 99 respondentus. Savo nuožiūra autorė pasirinko dar 13 įstaigų, kad pasiekti 112 elementų imties tūrį Iš viso buvo išsiųstos 112 anketų iš jų perskaitytos ir pasiekusios adresatą – 98 per minėtąjį 14 dienų laikotarpį sugrįžo 17 (17,4%). Tam įtakos galėjo turėti:

- apklausos laikas (artėjant metų pabaigai paprastai įstaigos turi daug daugiau darbų);
- anketos sudėtingumas;
- respondentų nesuinteresuotumas;

Žinoma, anketų grįžtamumui poveikį galėjo daryti ir kiti veiksniai, pavyzdžiui per trumpas (14 dienų) anketos užpildymo ir grąžinimo laikas. Norėdama išvengti kitų veiksmų galėjusių sutrukdyti anketos grįžtamumui darbo autorė respondentams priminė (per minėtąjį 14 dienų laikotarpį po anketų išsiuntimo) apie išsiųstas anketas ir ragino jas atsakyti. Be to, pasinaudojusi šiuolaikinių technologijų teikiamais privalumais išsiųsdama anketas užsakė ataskaitas, kurios parodytų, kada respondentas gavo laišką ir jį perskaitė. Iš visų 112 išsiųstų anketų 6 grįžo atgal nepasiekusios adresatų ir dar 8 anketos per minėtąjį laikotarpį nebuvo perskaitytos. Kaip jau minėta, iš visų 106 anketų pasiekusių adresatą 98 buvo perskaitytos.

Iš turimų duomenų galime paskaičiuoti atsakymų lygį – apskaičiuojama pasak S. Puškorio padalijus atsakiusiųjų respondentų skaičių iš visų atrinktų respondentų skaičiaus[68]. Šiuo atveju iš

[67] S. Puškorius. Veiklos auditas. Vilnius: Lietuvos teisės universitetas, 2004. P. 317.
[68] Ten pat. P. 137.

viso atrinktų respondentų buvo 112, tačiau atsakymų lygį skaičiuosime pasirinkdami tik tas anketas kurios pasiekė adresatus ir buvo perskaitytos, t.y. 98.

Atsakymų lygis = 98 / 17 = 5,7

Galima teigti, kad kuo gautas atsakymų lygio koeficientas artesnis vienetui, tuo mažiau pažeista reprezentatyvumo sąlyga. Tačiau, pasak S. Puškoriaus nesutariama dėl to, koks turi būti šis koeficientas, kad būtų galima tvirtinti, jog reprezentatyvumo sąlyga pažeista neženkliai[69].

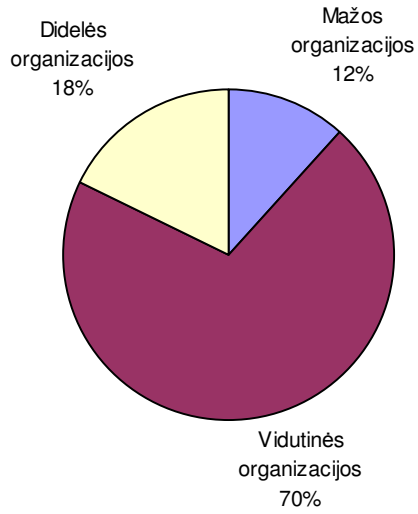
Visgi, pasaulinėje praktikoje nustatyta, jog anketinės apklausos paštu turi pakankamai žemą grįžusių anketų skaičiaus lygį, kad ir kokių priemonių imtųsi tyrėjas, tačiau tyrėjas turi stengtis, kad anketa būtų kuo paprastesnė ir suprantamesnė respondentui. Respondentams pateiktoje anketoje buvo užduoti uždari ir atviri klausimai. Šio tyrimo metu respondentams buvo pateikti 36 klausimai. Dauguma jų, t.y. 30 buvo uždari, o likę 6 - atviri. Į atvirus klausimus respondentai turėjo atsakyti raštu, o ne pažymėti tinkamiausią variantą. Uždari klausimai buvo pateikti dėl to, kad į juos atsakyti tiriamajam reikia mažiau laiko, o tyrėjui juos paprasčiau apibendrinti ir apskaičiuoti kiekybiškai. Kad išvengti vieno pagrindinio uždarų klausimų trūkumo, t.y. tendencingumo ir nepriversti respondentų rinktis tik iš pateiktų variantų daugelyje uždarų klausimų buvo pateiktas variantas „kita“, į kurio laukelį respondentas galėjo įrašyti tinkamą atsakymą (jei jo nerado pateiktuose atsakymų variantuose) ar paaiškinti savo pasirinkimą. Darbo autorei buvo svarbu išsiaiškinti *respondentų nuomonę* apie asmens duomenų apsaugą, todėl pasirinkti uždari klausimai. Atvirais klausimais stengtasi išsiaiškinti neaiškius arba nežinomus ir aktualius tyrėjui duomenis.

Anketos pagalba stengtasi ištirti kuo daugiau asmens duomenų apsaugos auditą veikiančių sričių, t.y. duomenų rinkimo, saugojimo, priėjimo prie duomenų, duomenų apdorojimo, duomenų atskleidimo, duomenų saugos ir archyvavimo procedūras. Bene daugiausiai dėmesio buvo skiriama duomenų saugai, nes tai viena pažeidžiamiausių asmens duomenų apsaugos sričių. Visi gauti duomenys ir komentarai bus apžvelgti sekančiuose skyreliuose.

2.2. Asmens duomenų apsaugos ypatumai biudžetinėse duomenų valdytojų įstaigose

Kaip jau minėta anksčiau tyrimui pasirinktos duomenų valdytojų organizacijos būtent pagal juridinį asmenį – biudžetinės (išskyrus švietimo) įstaigos. Iš visų respondentų atsakytų anketų matyti, kad daugiausia anketas grąžino vidutinio dydžio organizacijos (žr. 3 pav.).

[69] Ten pat.



3 pav. Organizacijų dydis

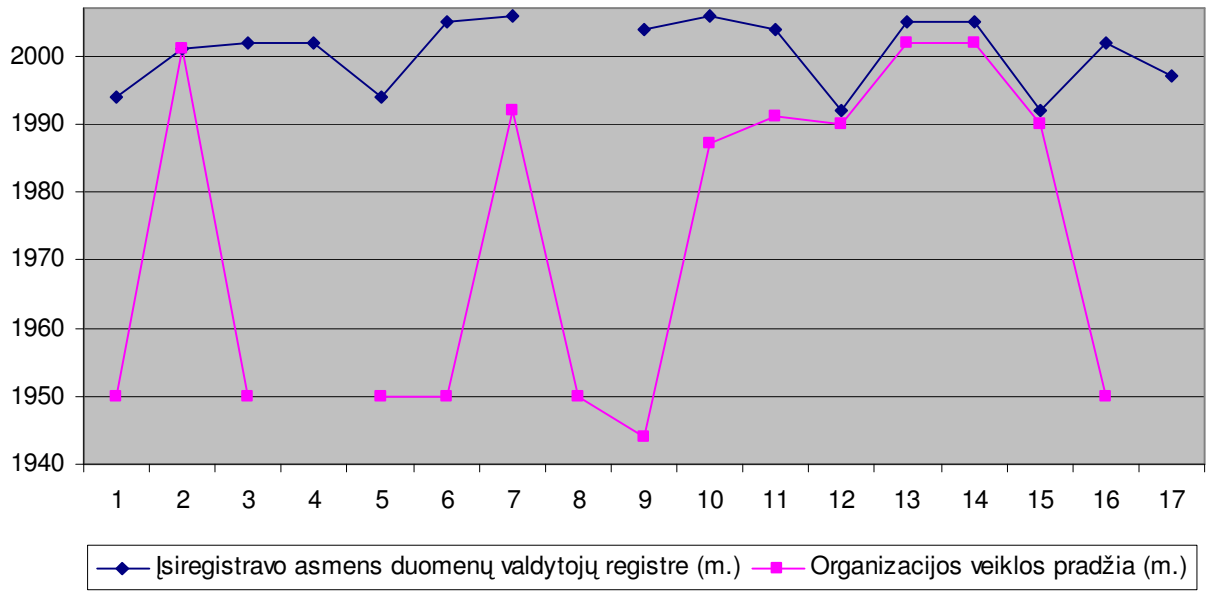
Kaip matyti iš 3 paveikslo, net 70 proc. užpildžiusių anketas įstaigų buvo vidutinio dydžio. Respondentai buvo paprašyti įvertinti savo įstaigas pagal žmonių, dirbančių jose skaičių. Vidutinio dydžio organizacija yra ta, kurioje dirba nuo 51 iki 250 darbuotojų. 18 proc. organizacijų atsiuntusių užpildytas anketas priklauso didelėms organizacijoms, kuriose dirba daugiau kaip 250 žmonių, šiek tiek mažesnė dalis, t.y. 12 proc. respondentų pateko į mažos organizacijos kategoriją, t.y. jose dirba nuo 11 iki 50 darbuotojų. Anketoje buvo išskirtos ir pačios mažiausios t.y. mikro organizacijos, kuriose dirba iki 10 žmonių, bet tokių organizacijų nebuvo. Dėl mažo anketų grįžtamumo sunku būtų palyginti ar egzistuoja skirtumai tarp mažų ir didelių organizacijų skiriamo dėmesio asmens duomenų apsaugai ir jo auditui. Tačiau, pagal gautus duomenis galima teigti, jog tik vidutinės ir didelės duomenų valdytojų organizacijos savo veikloje yra atlikusios duomenų apsaugos auditą.

Asmens duomenų apsaugos būklę ir dinamiką valstybiniame sektoriuje atspindi Asmens duomenų valdytojų valstybės registras. Asmens duomenų valdytojų valstybės registras ir jo informacinė paieškos sistema veikia Asmens duomenų apsaugos inspekcijos interneto svetainėje www.ada.lt ir yra prieinama visiems vartotojams – tiek duomenų subjektams, norintiems sužinoti apie duomenų tvarkymo vietas, tiek duomenų valdytojams, norintiems pranešti apie asmens duomenų tvarkymą ar patikslinti pateiktus registravimo duomenis, tiek kiekvienam norinčiam susipažinti su registru. Vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo nuostatomis, asmens duomenys gali būti tvarkomi automatiniu būdu tik kai duomenų valdytojas Lietuvos Respublikos Vyriausybės nustatyta tvarka praneša Inspekcijai, išskyrus atvejus, kai asmens duomenys tvarkomi vidaus administravimo ar sveikatos apsaugos tikslais, ar Lietuvos

Respublikos valstybės ir tarnybos paslapčių įstatymo[70] nustatyta tvarka, ir kitus įstatyme nustatytus išskirtinius atvejus.

Interneto vartotojas (duomenų subjektas) Asmens duomenų valdytojų valstybės registro duomenų bazėje gali surasti informaciją apie visus asmens duomenų valdytojus, Valstybinei duomenų apsaugos inspekcijai pranešusius apie asmens duomenų tvarkymą automatiniu būdu ir įregistruotus minėtame Registre. Viešai prieinami yra šie Registro duomenys: duomenų valdytojo pavadinimas; buveinė; identifikavimo kodas; įregistravimo data; asmens duomenų tvarkymo tikslas (-ai); duomenų subjektų grupė (-ės) ir su ja (-omis) susijusių asmens duomenų sąrašas (išskiriant ypatingų asmens duomenų sąrašą); asmens duomenų šaltiniai; asmens duomenų gavėjai; informacija apie duomenų teikimą į užsienį; duomenų saugojimo terminas; duomenų valdytojo atstovų duomenys; duomenų tvarkytojų ir jų atstovų duomenys.

Įstaigos grąžinusios užpildytas anketas duomenų valdytojų registre yra įsiregistravusios taip pat skirtingu metu (žr. 4 pav.).



4 pav. Respondentų veiklos pradžios ir registracijos duomenų valdytojų registre metai

Kaip matyti iš 4 paveikslo respondentų tarpe yra įstaigos savo veiklą pradėjusios vykdyti nuo 1944 metų, tuo tarpu anksčiausiai įsiregistravusi įmonė asmens duomenų valdytojų registre tai padarė 1992 metais. Iš paveikslo galima pastebėti, kad kuo vėliau įsteigta organizacija, tuo anksčiau

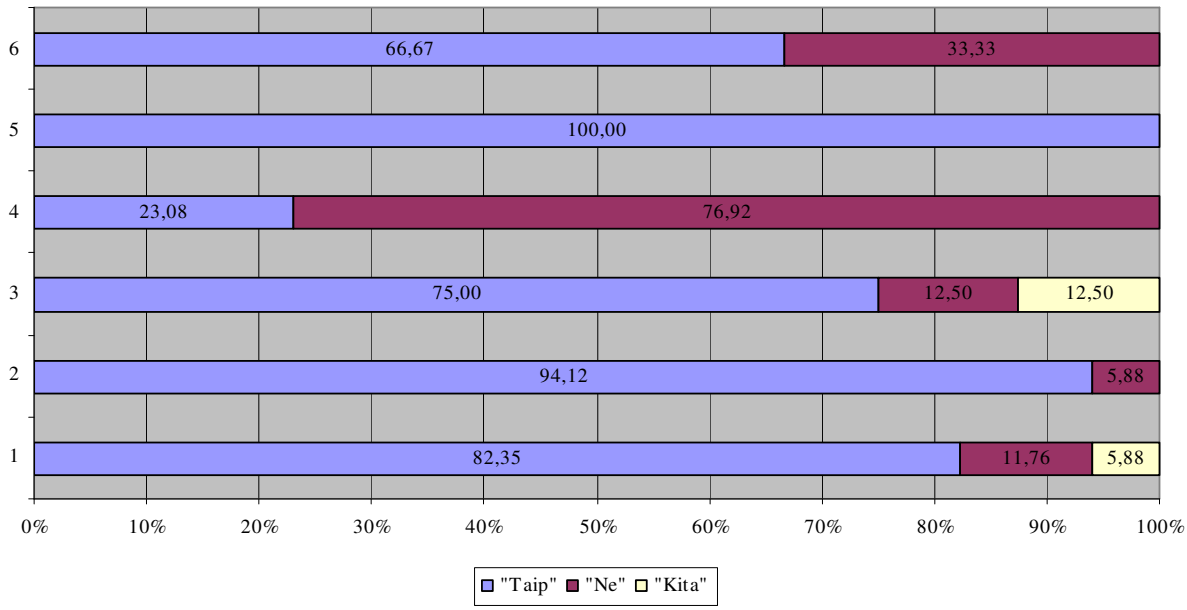
[70] Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas // Valstybės žinios, 1999, Nr. 105-3019.

ji užsiregistravo kaip duomenų valdytoja, tačiau anksčiau veikla vykdžiusios organizacijos to negalėjo padaryti bet kokiu atveju, nes registras neegzistavo iš viso. Visgi, iš 4 paveikslo matyti, kad įstaigos vykdžiusios veikla dar prieš nepriklausomybės atgavimą į duomenų valdytojų registrą įsiregistravo skirtingu metu. Analizuojant registre pateiktą statistiką matyti, kad registracijos suaktyvėjo 1996 metais (metai, kai buvo priimtas Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas). Tai galėjo būti pagrindine priežastimi įsiregistruoti asmens duomenų valdytojų registre (minėto įstatymo 27 str. 1 d. reikalavimas).

Dar du anketos klausimai buvo tiesiogiai susiję su Valstybine duomenų apsaugos inspekcija. Vienas iš jų skambėjo taip „ar apie asmens duomenų tvarkymą organizacijoje informuota Valstybinė duomenų apsaugos inspekcija". Tai kartu buvo ir taip vadinamas „klausimas – filtras", nes visi respondentai tyrimui buvo atrinkti būtent iš Valstybinio duomenų valdytojų registro, taigi, jei Valstybinė duomenų apsaugos inspekcija nebūtų informuota, tai respondentai ir negalėtų pakliūti į tiriamą visumą. Nenuostabu, kad į šį klausimą teigiamai atsakė net 94,12 proc. respondentų. Ir tik vienas iš atsakiusiųjų to negalėjo pasakyti, nes nežinojo. Klausimas „filtras" suteikė respondentų atsakymams daugiau patikimumo. Į klausimą „ar organizacijos duomenų apsaugos priemonių aprašas pateiktas Valstybinei duomenų apsaugos inspekcijai" teigiamai atsakė mažiau respondentų, nei į pieš tai nagrinėtą klausimą. Vis gi, didžioji dauguma respondentų, t.y. 82,35 proc. teigė, kad toks aprašas yra pateiktas.

Duomenų valdytojams pateiktoje anketoje klausimai apėmė įvairiais asmens duomenų apsaugos sritis. Viena iš jų buvo administracinio – techninio duomenų saugumo klausimai (5 pav.). Paveiksle pateiktas šešių administracinio – techninio duomenų saugumo klausimų atsakymų pasiskirstymo grafikas. Klausimai sužymėti and Y ordinatės:

1. Ar yra organizacijoje raštu išdėstytos pagrindinės organizacijos informacijos apsaugos nuostatos, patvirtintos aukščiausios vadovybės?
2. Ar organizacijoje atliekamas kompiuterinių programų patikrinimas?
3. Ar yra organizacijoje saugumo politikos nuostatos, kurios aiškiai apibrėžia, kokia informacija yra saugoma, o kokia ne?
4. Ar organizacijoje saugomi asmens duomenys kaip nors šifruojami?
5. Ar yra įdiegta apsauga nuo kenksmingos programinės įrangos?
6. Ar yra nustatyti techniniai ir organizaciniai apribojimai asmeninių duomenų perdavimui ir panaudojimui organizacijoje?

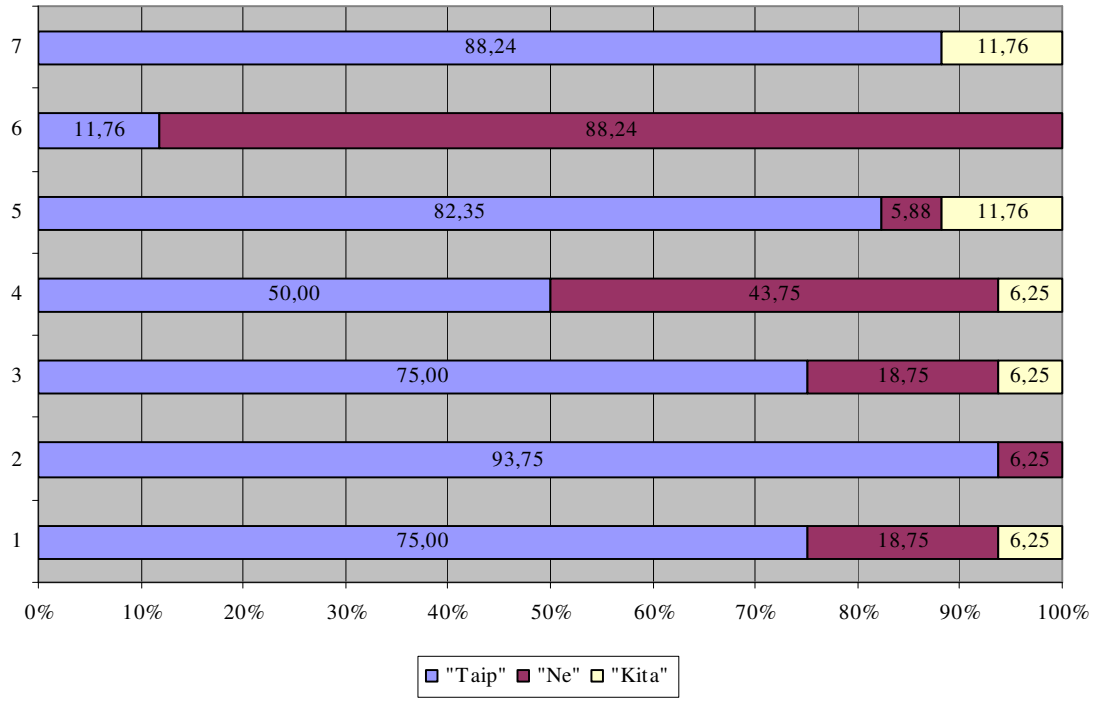


5 pav. Duomenų administracinis – techninis saugumas

Kaip matyti iš 5 paveikslo geriausia duomenų administracinio – techninio saugumo sritis yra susijusi su apsauga nuo kenksmingos programinės įrangos (klausimas Nr. 5). Visi respondentai į šį klausimą atsakė teigiamai, taigi galima teigti, jog kenksminga programinė įranga kelia mažiausią grėsmę asmens duomenų apsaugai. Kitas klausimas susijęs su programine įranga (Nr. 2) taip pat vertinamas palankiai. Net 94,12 proc. respondentų teigė, jog organizacijoje atliekamas kompiuterinių programų patikrinimas.

Paveiksle matyti, kad respondentų atsakymai apie organizacijos informacijos apsaugos nuostatas ir saugumo politikos nuostatas, kurios apibrėžia kokia informacija yra saugoma, o kokia ne, yra žemesni nei atsakymai, susiję su programine įranga. Teigiamai į klausimą Nr. 1 atsakė 82, 35 proc. tiriamųjų, o į klausimą Nr. 3 – 75 proc. Galima teigti, jog ir šioje srityje yra užtikrinamas pakankamas saugumo lygis. Žemiausiai pateiktame paveiksle yra vertinami 6 ir 4 klausimai. Beveik 77 proc. respondentų teigia, jog organizacijoje saugomi asmens duomenys nėra kaip nors šifruojami. Tai gali sąlygoti neteisėtą duomenų panaudojimą. Be to, 33,33 proc. respondentų teigia, jog organizacijoje nėra nustatytų techninių ir organizacinių apribojimų asmeninių duomenų perdavimui ir apdorojimui. Visa tai susiję ir su žmogiškuoju veiksniu, kuris yra taip pat labai svarbus asmens duomenų apsaugoje. Svarbų vaidmenį atlieka ir kitas saugumo principas – konfidencialumas. Pagal respondentų atsakymus galima teigti, jog yra nemaža tikimybė, jog su organizacijoje saugoma asmens informacija galės susipažinti ir nesusiję asmenys. Taip informacija tyčia ar netyčia gali būti

atskleista pašaliniams asmenims, kartu pažeidžiant konfidencialumo principą. Be konfidencialumo, kitas svarbus asmens duomenų apsaugos principas – vientisumas. Kaip jau buvo minėta darbo teorinėje dalyje, vientisumo principas užtikrina, kad informacinės sistemos ir jose saugoma informacija nebus pakeista nesankcionuotu būdu, kitaip sugadinta arba visiškai prarasta. Tai gali būti padaryta tiek tyčia, norint pakenkti arba siekiant naudos, tiek netyčia - dėl nežinojimo ar žmogiškos klaidos. Būtent žmogiškoji klaida ir saugumo veiksniai susiję su darbuotojų įsitraukimu į asmens duomenų apsaugą įstaigose, atskleisti žemiau pateiktame paveiksle.



6 pav. Įstaigos darbuotojų poveikis asmens duomenų apsaugai

6 paveiksle pavaizduoti atsakymų stulpeliai į tokius klausimus:

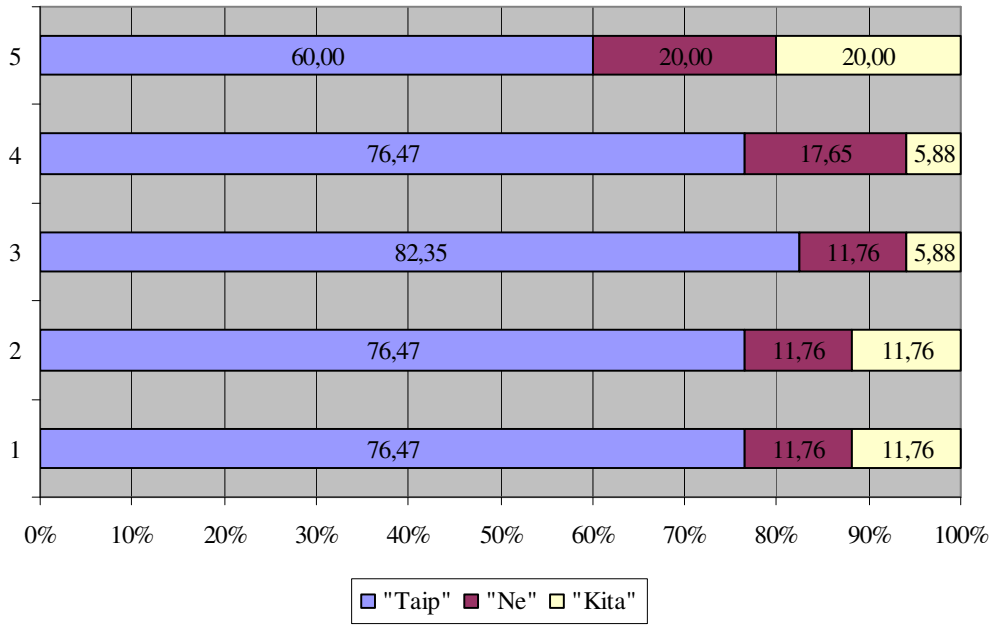
1. Ar yra organizacijoje paskirtas asmuo atsakingas už IS saugumo politikos įgyvendinimą?
2. Ar Jūsų organizacijoje yra žmogus (-nės), atsakingas (-i) už duomenų apsaugą?
3. Ar organizacijos darbuotojai yra įtraukti į duomenų apsaugą?
4. Ar organizacijoje paruošti aiškūs (techniniai ir organizaciniai) nurodymai dėl to, kuris asmuo gali susipažinti su kokiais duomenimis?
5. Ar organizacijoje yra nustatytos vartotojų teisės kompiuterinėse sistemose?
6. Ar asmeniniais, organizacijoje saugomais duomenimis, gali naudotis visi organizacijos darbuotojai?

7. Ar visi organizacijos darbuotojai darbe naudojantys asmeninius duomenis yra apmokyti teisingai naudotis šiais duomenimis?

Iš 6 paveikslo matyti, kad į pirmą klausimą teigiamai atsakė 75 proc. respondentų. Galima teigti, jog daugumoje tirtų organizacijų yra žmogus atsakingas už informacinių sistemų saugumo politikos įgyvendinimą. Jis organizacijoje turi prižiūrėti kaip laikomasi saugumo principų ir standartų. Iš antro klausimo atsakymų matyti, kad už duomenų apsaugą atsakingų žmonių organizacijose yra net daugiau nei paskirtų atsakyti ir prižiūrėti informacinių sistemų saugumą. Nepaisant to, kad dauguma įstaigų teigė turinti už duomenų apsaugą atsakingą asmenį, kitų darbuotojų atžvilgių asmens duomenų apsauga atrodo šiek tiek prieštaringai. Dauguma respondentų (88,24 proc.) atsakė, kad organizacijos darbuotojai, darbe naudojantys asmeninius duomenys yra apmokyti teisingai naudotis šiais duomenimis. Be to, dauguma (82,35 proc.) teigė, jog organizacijoje yra nustatytos vartotojų teisės kompiuterinėse sistemose. Tirtose organizacijose net 75 proc. tiriamųjų sutiko, jog organizacijos darbuotojai yra įtraukti į asmens duomenų apsaugą. Vis dėl to, į ketvirtą klausimą „ar organizacijoje paruošti aiškūs techniniai ir organizaciniai nurodymai dėl to, kuris asmuo gali susipažinti su kokiais duomenimis“ teigiamai atsakė tik pusė respondentų. Kyla klausimas, kaip įtraukti į duomenų apsaugą darbuotojai su nustatytomis vartotojų teisėmis kompiuterinėse sistemose bei apmokyti teisingai darbe naudoti asmeninius duomenis gali žinoti su kokiais duomenimis jiems galima susipažinti, o su kokiais ne, jeigu nėra aiškių techninių ir organizacinių nurodymų? Darbo autorės nuomone čia gali kilti pareigų atskyrimo problema bei kolizija dėl galimo vartotojų teisių neteisingo suteikimo. Galbūt net apmokomi ne tie darbuotojai, kurie savo darbe turėtų teisingai naudoti asmens duomenis. Galima būtų daryti prielaidą, kad įstaigose neteisingai valdomi asmens duomenys, nes neaišku, kurie darbuotojai su kokiais duomenimis gali susipažinti, tačiau šią prielaidą galima atmesti ar bent jau sumažinti jos tikimybę, nes į šeštą klausimą „ar asmeniniais, organizacijoje saugomais duomenimis gali naudotis visi organizacijos darbuotojai“ didžioji dauguma respondentų (88,24 proc.) atsakė neigiamai. Tai reiškia, kad tik likusių 11, 76 proc. tiriamų įstaigų nevaldo šio proceso ir visos organizacijos darbuotojai gali naudotis visais organizacijoje saugomais duomenimis. Tokiose organizacijose atsiranda daug didesnė rizika neteisėtam duomenų panaudojimui, atskleidimui ir platinimui už organizacijos ribų. Apibendrinant galima teigti, jog didžiausia problema susijusi su duomenų apsauga ir žmogiškaisiais ištekliais yra trūkumas rašytinių nurodymų, kurie darbuotojai gali dribti su kokias asmens duomenimis. Esant šiems nurodymams žmogui, atsakingam už duomenų apsauga, būtų paprasčiau patikrinti ir kontroliuoti asmens duomenų apsaugos procesą įstaigoje, be to, sumažėtų tikimybė dėl neteisėto tyčinio ar netyčinio duomenų panaudojimo.

Be duomenų organizacinio ir techninio saugumo užtikrinimo, o taip pat žmogiškųjų išteklių racionalaus valdymo ir panaudojimo duomenų apsaugos srityje labai svarbus ir teisinis aspektas. Anketoje duomenų valdytojams nebuvo tiesioginių klausimų ar jie laikosi asmens duomenų apsaugos ir kitų LR galiojančių teisės aktų, tačiau buvo svarbu išsiaiškinti kaip organizacijos viduje valdomas asmens duomenų apsaugos procesas tiek pagal LR, tiek pagal ES reikalavimus ir geros praktikos pavyzdžius. Pavyzdžiui, į trisdešimt ketvirtą anketoje pateiktą klausimą „ar duomenų subjektas turi galimybę susipažinti su savo asmenine informacija bei ją atnaujinti ir ištrinti“ 71, 43 proc. atsakė teigiamai, 14,29 proc. atsakė neigiamai, lygiai tiek pat pasirinko kitą atsakymą. Pagal Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 19 ir 20 straipsnius duomenų subjektas turi klausime minėtas teises. Galima teigti, jog neigiamai į minėtąjį klausimą atsakę įstaigos nesilaiko ar bent jau nepilnai laikosi įstatymo nustatytų normų. Tuo tarpu į trisdešimt trečią klausimą „per kiek laiko organizacija atsako į asmeninių duomenų užklausimą duomenų subjektui“ atsakymai svyravo nuo 3 iki 30 dienų. Pagal asmens duomenų teisinės apsaugos įstatymo 19 str. 2 d. duomenų valdytojai privalo duomenų subjektui atsakyti ne vėliau kaip per 30 dienų, todėl galima tvirtinti, kad šią įstatymo normą duomenų valdytojai įsisavinę puikiai. Tačiau neaišku, ar jie iš tiesų taip elgiasi. Norint tai patikrinti reiktų atlikti atskirą tyrimą duomenų subjektui pateikus paklausimą dėl asmens duomenų tvarkymo. 7 paveiksle pateikti kiti svarbūs duomenų valdytojams pateiktų klausimų atsakymai. Kaip jau buvo minėta anksčiau, kiekvienas auditorius atlikdamas duomenų apsaugos auditą, turėtų patikrinti ar organizacijoje yra formali (t.y. dokumentuota ir nuolat atnaujinama) duomenų apsaugos sistema, patikrinti ar organizacijos darbuotojai įtraukti į duomenų apsaugą ir įsitikinti ar duomenų apsaugos sistema veikia organizacijoje ir yra efektyvi. Pasiekti šiuos audito tikslus gali padėti organizacijoje esančios procedūros, nuostatai, taisyklės, tvarkos ir kt. dokumentai. Tvarkydamos asmens duomenis valstybės institucijos taip pat privalo garantuoti duomenų saugumą. Tai apima organizacines ir technines priemones, siekiant užkirsti kelią bet kokiam atsitiktiniam ar neteisėtam duomenų sunaikinimui, pakeitimui, atskleidimui ar kitokiam neteisėtam jų tvarkymui. Tarp kitų organizacinių priemonių yra ir aiškios nuostatos dėl atsakomybės, rašytinės duomenų tvarkymo instrukcijos ir kompiuterių bei kitų įrenginių techninės apsaugos priemonės nuo neteisėtos duomenų prieigos ir kitų rizikų.

Šiame tyrime buvo svarbu išsiaiškinti ar organizacijose egzistuoja minėtieji su duomenų sauga susiję dokumentai, kurie galėtų padėti auditoriui atlikti duomenų apsaugos auditą organizacijoje. Atsakymai į šiuos klausimus pateikti 7 paveiksle.



7 pav. Įstaigoje naudojami formalūs dokumentai susiję su duomenų apsauga

7 paveiksle pateiktų atsakymų klausimai užduoti duomenų valdytojams anketoje:

1. Ar organizacijos informacinių sistemų veiklos procedūros dokumentuotos?
2. Ar parengti IS duomenų saugos nuostatai organizacijoje?
3. Ar organizacijoje yra formali ir nuolat atnaujinama duomenų apsaugos sistema?
4. Ar organizacijoje patvirtintos asmens duomenų tvarkymo taisyklės?
5. Ar parengta saugaus darbo su duomenimis tvarka?

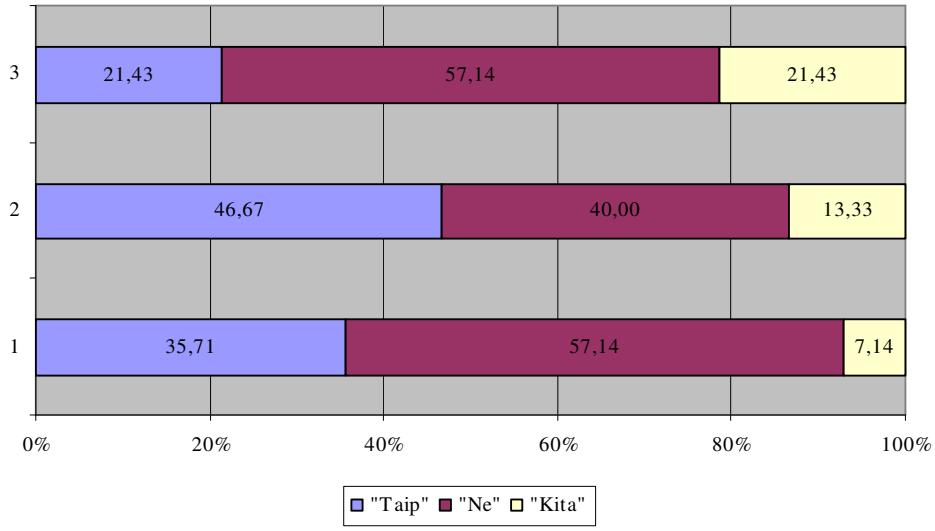
Iš paveikslo matyti, kad daugumos įstaigų informacinių sistemų procedūros dokumentuotos, parengti duomenų saugos nuostatai, duomenų apsaugos sistema nuolat atnaujinama, asmens duomenų tvarkymo taisyklės patvirtintos. Tačiau saugaus darbo su duomenimis tvarka yra parengta tik 60 proc. tirtųjų įstaigų. Vadinasi, dar 40 proc. įstaigų šių tvarkų neturi, todėl darbuotojai gali nežinoti koks turi būti saugus darbas su asmens duomenimis. Nesant minėtų reikalavimų ir tvarkų darbuotojai ir už asmens duomenų apsaugą atsakingas žmogus organizacijoje negali prisiimti atsakomybės už nesaugų darbą su duomenimis.

Asmens duomenų apsaugai ir saugumui įtaką daro ne tik vidiniai organizacijos nuostatai, dokumentai ir tvarkos bei darbuotojai bet ir išorė. Duomenų valdytojams pateiktoje anketoje buvo pateikti 3 klausimai susiję su trečiosiomis šalimis ir išoriniais veiksniais, t.y.:

1. Ar organizacijos elektroninis susirašinėjimas su antrosiomis šalimis ir organizacijos viduje yra apsaugotas?

2. Ar yra nustatyta organizacijos turimos informacijos apsikeitimo politika ir procedūros su kitomis organizacijomis ir trečiosiomis šalimis?
3. Ar organizacija valdo trečiųjų šalių paslaugų teikimo procesą?

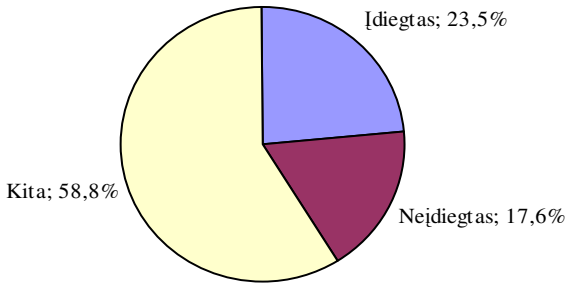
Įstaigų atsakymai į šiuos klausimus pavaizduoti 8 paveiksle.



8 pav. Duomenų apsauga ir kitos šalys

Iš 8 paveiksle pateiktų atsakymų matyti, kad tai bene pati silpniausia duomenų apsaugos organizacijose sritis. Į visus tris pateiktus klausimus pirmauja neigiami atsakymai. Šie procesai yra susiję beveik su visomis duomenų apsaugos sritimis, t.y. – duomenų rinkimu, saugojimu, apdorojimu, atskleidimu, sauga ir ypač eksportu. Iš aukščiau esančio paveikslo matyti, kad silpnai apsaugotas elektroninis susirašinėjimas. Viena įstaiga minėjo, jog jie naudoja filtrus ir kitas apsaugos priemones elektroniniame susirašinėjime. Tačiau visos kitos nepaminėjo nei vieno elektroninio susirašinėjimo apsaugos būdo. Daugumoje įstaigų nėra parengtų turimos informacijos apsikeitimo procedūrų. Mažiausiai teigiamų atsakymų (21,43 proc.) sulaukė trečiasis šios srities klausimas „ar organizacija valdo trečiųjų šalių paslaugų teikimo procesą“. Žinoma, valdyti trečiųjų šalių paslaugų teikimo procesą yra pakankamai sudėtinga, tačiau dalinantis duomenimis su trečiosiomis šalimis yra būtina turėti bent procedūras, kurios padėtų valdyti šiuos procesus, nustatytų kiekvienos šalies atsakomybę. Galima teigti, jog Lietuvos valstybinių registrų sistema, o kartu ir kiekvienos duomenų valdytojo saugomi asmens duomenys – tai didžiulis informacijos apie asmenis ar kitus objektus kiekis. Šie duomenys yra vienas iš pagrindinių informacijos šaltinių valstybės institucijoms, todėl jų sklaida turi vykti sklandžiai su kuo mažesnę neteisėto naudojimo ir pasisavinimo rizika.

Dar viena, bet ne mažiau svarbi asmens duomenų apsaugos sričių yra duomenų archyvavimas ir laikymas. 93,33 proc. respondentų teigė, jog organizacijoje daromos saugomos informacijos atsarginės kopijos. Tai padeda išvengti galimo visiško duomenų praradimo. Respondentai teigė, jog kopijos daromos pagal patvirtintas tvarkas ir nuolat. Be to, pasikeitus bet kokiai informacijai kopijos atnaujinamos. Tačiau į kitą klausimą „ar organizacijoje saugomų asmeninių duomenų laikymo ir saugojimo metodai aiškiai aprašyti“ teigiamai atsakė 66,67 proc. tirtų duomenų valdytojų. Tai vienas pagrindinių D. Baker išskirtų ir duomenų apsaugos akte aprašytų duomenų apsaugos principų, todėl buvo aktualu sužinoti atsakymus ir į minėtąjį klausimą. Vėlgi, galime teigti, jog nemažoje dalyje respondentų organizacijų trūksta aiškiai nustatytų ir aprašytų tvarkų kaip laikomi ir saugomi asmens duomenys. Daugelį minėtų trūkumų valdyti ar pašalinti galėtų padėti standartų susijusių su IS ir duomenų apsauga įdiegimas organizacijose. Vienas iš tokių standartų yra ISO/IEC 17799:2005 standartas, kurio neoficialus vertimas pateiktas 1 darbo priede.



9 pav. ISO/IEC 17799:2005 standarto būsena

Kaip matyti iš 9 paveikslo tik 23,5 proc. respondentų organizacijose yra įdiegtas minėtas standartas. Šis standartas galėtų tapti net saugumo metodologija (apie tai buvo rašyta 1.2.2. skyrelyje). Standartas reikalauja turėti saugumo politikos dokumentą, nustatyti atsakingus asmenis, kontroliuoti virusus, užtikrinti įstatymų vykdymą ir t.t. Galima teigti, jog jis apima visas asmens duomenų apsaugą turinčias užtikrinti sritis, todėl duomenų valdytojams rekomenduojama įsidiegti minėtą standartą į savo veiklą.

Paskutiniai, bet vieni iš svarbiausių klausimų reikalingi darbe iškeltai hipotezei patvirtinti ar paneigti anketoje buvo susiję su duomenų apsaugos auditu. Respondentams buvo užduoti klausimai „ar organizacijoje buvo atliekamas duomenų apsaugos auditas“ ir jeigu taip, kas ji atliko? Tik 23,53 proc. (t.y. 4) tiriamieji atsakė, kad pas juos buvo atliktas duomenų apsaugos auditas. Dvejose organizacijose jį atliko išorės auditoriai, vienoje – vidaus, o paskutinės organizacijos atsakyme buvo pažymėtas „kita“ atsakymas, bet nepaaiškinta, kas atliko minėtą auditą. Galima teigti, jog iš gautų duomenų negalima iškeltos hipotezės nei patvirtinti nei paneigti, nes gauta per mažai duomenų, kad galima būtų išvesti tendencijas ir nustatyti koreliaciją tarp jų. 10 priede pateiktoje visų tiriamųjų suvestinėje lentelėje yra iškirti 2, 3, 10 ir 11 respondentai, būtent jie teigė, kad jų įstaigoje buvo atliktas duomenų apsaugos auditas, tačiau žvelgiant į tyrimo rezultatus ir atskirus klausimus matyti, kad dviejų respondentų atsakymai (2 ir 11) yra tikrai teigiami ir rodantys gerus organizacijos pasiekimus asmens duomenų apsaugos srityje, tuo tarpu kitų dviejų t.y. 3 ir 10 respondentų atsakymai yra vieni iš prasčiausių lyginant su visais tyrimo duomenimis. Vadinasi, norit patvirtinti ar atmesti hipotezę būtinai reikalingas didesnis tyrimas. Kita vertus tai taip pat gali rodyti respondentų nesuinteresuotumą duomenų apsauga. Iš viso buvo išsiųsta 112 anketų, jei būtų sugrįžę bent 80 proc. iš jų galima būtų tiksliai patvirtinti arba atmesti hipotezę. Dėl negrįžusių anketų tyrimas nebus reprentatyvus, todėl hipotezės patvirtinimui ar atmetimui reiktų atlikti dar vieną tyrimą. Pavyzdžiui eksperimentą. Iš tiriamosios visumos atrinkus eksperimentinius kintamuosius juose atlikti duomenų apsaugos auditą. Po metų reiktų patikrinti hipotezę ar “duomenų valdytojai, neatliekantys duomenų apsaugos audito duomenis valdo neefektyviai ir nesilaikydami duomenų apsaugai keliamų teisinių reikalavimų“ tikrinant eksperimentinius kintamuosius (įstaigas, kuriose buvo atliktas duomenų apsaugos auditas) ir kontrolinius kintamuosius (įstaigas, kuriose nebuvo atliktas duomenų apsaugos auditas).

Apibendrinant galima teigti, jog tyrimas atskleidė, kad duomenų apsaugos auditas yra aktuali problema tirtose Lietuvos įstaigose. Daugelyje jų trūksta oficialių, dokumentuotų procedūrų, tvarkų ir nuostatų, kurios padėtų asmens duomenis valdyti saugiai ir efektyviai. Be to, labai silpnai valdomi trečių šalių ir išorės veiksniai, darantys svarbią įtaką asmens duomenų apsaugoje. Stipriosios pusės asmens duomenų apsaugoje yra programinė įranga, kurioje yra įdiegta apsauga nuo kenksmingų programų ir ji nuolat tikrinama, tačiau tai tik vienas saugos veiksnys. Tyrimas atskleidė, jog duomenų valdytojai naudoja nepakankamas duomenų saugumo priemones. Programinė įranga neapsaugo duomenų nuo neįgaliotų vartotojų, trūksta informacinių sistemų dokumentavimo, nenaudojamos duomenų teikimo sutartys ir darbuotojų pasižadėjimai saugoti asmens duomenų paslaptį visa tai gali pažeisti asmens teises ir laisves.

IŠVADOS IR REKOMENDACIJOS

Išnagrinėjus asmens duomenų apsaugos audito ypatumus ir atlikus biudžetinių duomenų valdytojų tyrimą, būtų galima daryti keletą *išvadų*:

1. Lietuvoje dar nėra tiksliai apibrėžtos asmens duomenų apsaugos audito sampratos, tačiau duomenų apsaugos auditas tampa vis reikšmingesniu ir reikalingu, norint užtikrinti asmens duomenų apsaugą sparčiai besiplėtojant šiuolaikinėms technologijoms ir daugėjant duomenų bazių ir registrų (kuriuose saugomi asmeniniai duomenys) skaičiui;
2. Šiuo metu Lietuvoje yra įsigalioję asmens duomenų apsaugos teisinės bazės pagrindai, tačiau norint užtikrinti šios bazės veiksmingumą jį turi būti nuolat tobulinama atsižvelgiant į besikeičiančios rinkos sąlygas;
3. Asmens duomenų apsaugos audito metodai ir procesas nedaug skiriasi nuo kitų audito rūšių, skiriasi tik reikalavimai, pagal kuriuos atliekamas auditas.
4. Pasaulinėje praktikoje duomenų apsaugos audito tipo/metodo pasirinkimą lemia laiko sąnaudos, auditoriaus išsilavinimas, audito tikslai ir t.t. Kad ir kurį duomenų apsaugos audito tipą (pakankamumo ir atitikties ar procedūrinį) pasirinktų auditorius svarbiausias jo tikslas turėtų būti – padėti organizacijai efektyviai valdyti asmens duomenis ir patikrinti jų saugumą ir atitikimą teisinių aktų reikalavimams;
5. Informacinėje visuomenėje asmens duomenų apsaugos auditas labai svarbus ginant asmeninės žmogaus teises ir laisves ir apsaugant jas nuo neteisėto panaudojimo;
6. Tvarkydamos asmens duomenis valstybės institucijos privalo garantuoti duomenų saugumą. Duomenų apsaugai ypač pavojingos yra šiuo metu esančios galimybės apsikeisti duomenimis tarp viešojo sektoriaus įstaigų. Todėl duomenų pasikeitimo sistemoms turėtų būti skiriamas ypatingas dėmesys ir apsauga.
7. Atliktas tyrimas atskleidė, jog kenksminga programinė įranga kelia mažiausią grėsmę asmens duomenų apsaugai. Be to, tyrimas parodė, kad organizacijų darbuotojai yra apmokyti teisingai naudotis asmens duomenimis, kompiuterinėse sistemose yra suteiktos vartotojų teisės, tačiau daugelis problemų kyla dėl nepakankamų ar neparengtų aiškių techninių reikalavimų, nurodymų, taisyklių, nuostatų, tvarkų dėl asmens duomenų apsaugos įstaigų viduje;

8. Tyrimas parodė, jog pati silpniausia asmens duomenų apsaugos sritis yra susijusi su organizacijos vykdoma veikla kartu su kitomis šalimis (pav. elektroninis susirašinėjimas, paslaugų teikimas);
9. Tirtieji duomenų valdytojai dažniausiai naudoja nepakankamas duomenų saugumo priemones. Programinė įranga ne visada ir ne visose įstaigose apsaugo duomenis nuo neįgaliotų vartotojų, trūksta informacinių sistemų dokumentavimo;

Rekomendacijos:

- Duomenų valdytojams - paskirti už duomenų apsaugą atsakingą asmenį organizacijoje; atlikti duomenų apsaugos auditą, kuris įvertintų veiklos atitikimą reikalavimams ir atskleistų duomenų apsaugos sistemos trūkumus, kuriuos pašalinus asmens duomenys būtų valdomi daug saugiau; parengti visas reikalingas tvarkas, nuostatas, procedūras ir t.t. reikalingas saugiam asmens duomenų valdymui; pagal galimybes įsidiegti ISO/IEC 17799:2005 standartą;
- Valstybinei duomenų apsaugos inspekcijai – išnaudoti tarptautinio bendradarbiavimo galimybes ir daugiau dėmesio skirti organizacinių ir techninių duomenų apsaugos priemonių patikrinimams; didinti Lietuvos visuomenės informuotumą duomenų apsaugos srityje; stiprinti ir ugdyti ne tik priežiūros bei teisėsaugos institucijų, bet ir duomenų valdytojų administracinius gebėjimus duomenų apsaugos srityje.
- Duomenų subjektams – domėtis savo teisėmis ir pareigomis.

LITERATŪROS SĄRAŠAS

Norminiai aktai:

1. Lietuvos Respublikos administracinių teisės pažeidimų kodeksas // Valstybės žinios 2005, Nr. 149-5421.
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios 2003, Nr. 15- 597.
3. Lietuvos Respublikos įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis ratifikavimo // Valstybės žinios 2001, Nr.32-1055.
4. Lietuvos Respublikos įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomo protokolo dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų ratifikavimo // Valstybės žinios, 2004, Nr.36-1177.
5. Lietuvos Respublikos įstatymas dėl Konvencijos, parengtos vadovaujantis Europos Sąjungos sutarties K.3 straipsniu, dėl Europos policijos biuro įsteigimo (Europolo konvencijos) ir jos protokolų ratifikavimo // Valstybės žinios, 2004, Nr.69-2384.
6. Lietuvos Respublikos elektroninių ryšių įstatymas // Valstybės žinios, 2004, Nr.69-2382.
7. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas // Valstybės žinios, 1999, Nr. 105-3019.

Specialioji literatūra:

8. A. Jankūnas, A. Klibas. Informacijos technologijos. Vilnius, Verslo žinios, 2005. P. 60.
9. Barker D. Duomenų apsaugos auditas. Tarptautinės konferencijos E-verslas ir duomenų apsauga medžiaga. Vilnius: Expozona, 2005. P. 146.
10. Collier G. Information privacy: Just how private are the private details of individuals in a company's database? // Information Management & Computer Security. 1995 , Nr. 3 (1). P. 41-45.
11. E. Sanderson, K. A. Forcht. Information security in business environments // Information management & Computer Security. 1996, Nr. 4 (1). P. 32-37.
12. E.Loukis, D. Spinellis. Information systems security in the Greek public sector // Information management & Computer Security. 2001, Nr. 9 (1). P. 21-31.
13. I. Gray ir S. Manson. The audit process principles, practice and Cases. London: Chapman and Hall, 2001. P. 243 – 303.

14. Luobikienė I. Socialinių tyrimų metodika: mokomoji knyga. Kaunas: Technologija, 2002. P. 84.
15. Mackevičius J. Audito teorija ir praktika: monografija. Vilnius: Lietuvos mokslų akademija, 1999. P. 179.
16. Millichamp A. H. Auditing. London: Ashford Color Press, 1996. P. 483.
17. N. Zhao, D.C. Yen. Auditing in the e-commerce era // Information management & Computer Security. 2004, Nr. 12 (5). P. 389-400.
18. Puškorius S. Veiklos auditas. Vilnius: Lietuvos teisės universitetas, 2004. P. 317.
19. White A. Control of Transborder Data Flow: Reactions to the European Data Protection Directive // International journal of law and information technology. 2005, Nr. 5 (2). P. 230-247.

Dokumentai iš interneto svetainių:

20. Asmens duomenų apsaugos inspekcijos internetinė svetainė // www.ada.lt; prisijungimo laikas: 2006-04-28.
21. Data protection act // http://www.opsi.gov.uk/acts/acts1998/80029--a.htm#3; prisijungimo laikas: 2006-06-02.
22. Data protection act 1984 // http://www.hmso.gov.uk/acts/acts1984/1984035.htm; prisijungimo laikas: 2006-05-02.
23. Data protection audit manual // http://www.ico.gov.uk/documentUploads/the_complete_audit_guide.pdf; prisijungimo laikas: 2006-05-10.
24. Data protection in the European union // http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm; prisijungimo laikas: 2006-05-10.
25. Data protection policy // www.wales.nhs.uk/sites3/documents/49/15DPA.pdf; prisijungimo laikas: 2006-05-10.
26. Directgov internetinė svetainė // http://www.open.gov.uk/dpr/dprhome.htm; prisijungimo laikas: 2006-06-10.
27. Data protection auditing // www.isacalondon.org/presentations/ISACA%20Data%20Protection%20Auditing.ppt; prisijungimo laikas: 2006-05-25.
28. EB 45/2201 direktyva // http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas: 2006-05-10.

29. Europos duomenų apsaugos prižiūrėtojas // www.ada.lt/index.php?lng=lt&action=page&id=172; prisijungimo laikas: 2006-05-10.
30. Interneto technologijos // http://www.ukuug.org/events/winter99; prisijungimo laikas: 2006-05-25.
31. Lankstinukai duomenų apsaugos klausimais // http://www.ada.lt/index.php?lng=lt&action=page&id=256; prisijungimo laikas: 2006-05-15.
32. Liskovas O. Duomenų apsauga elektroninėje komercijoje//http://www.esecurity.lt/article/1145.html; prisijungimo laikas: 2006-03-26.
33. Montreux deklaracija // www.ada.lt/images/cms/File/ Montre_deklaracija_doc.0922%20(1).doc; prisijungimo laikas: 2006-05-10.
34. Phare programme twinning project no. LT02/IB-JH-02/-03 strengthening administrative and technical capacity of personal data protection. Phare Dvynių projektas // www.ada.lt/images/cms/File/Pirmieji%20duomenu%20apsaugos%20zingsniai.pdf; prisijungimo laikas: 2006-05-10.
35. Privacy law // http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; prisijungimo laikas: 2006-05-10.
36. Teisinė bazė // http://www.ada.lt/index.php?lng=lt&action=page&id=69; prisijungimo laikas: 2006-06-05.
37. Valstybinės duomenų apsaugos inspekcijos 2006-2008–ųjų metų strateginis veiklos planas // www.ada.lt/images/cms/File/Teises%20aktai/2.pdf; prisijungimo laikas: 2006-05-10.

SANTRAUKA

Magistro baigiamasis darbas „Asmens duomenų apsaugos auditas biudžetinėse duomenų valdytojų organizacijose" atskleidžia duomenų apsaugos audito sampratą ir reikšmę, apžvelgia asmens duomenų apsaugos teisinę bazę įvairiose pasaulio šalyse ir Lietuvoje. Be to, darbe yra atskleisti asmens duomenų apsaugos tikslai ir privalumai, audito formos, metodai ir etapai. Darbo tiriamojoje dalyje aprašyti asmens duomenų apsaugos ypatumai Lietuvoje, biudžetinėse duomenų valdytojų organizacijose, išskirtos pagrindinės problemos šioje srityje. Palyginus teorinėje darbo dalyje aprašytą asmens duomenų apsaugos auditą su atlikto tyrimo duomenimis darbo pabaigoje, pateiktos pagrindinės išvados ir rekomendacijos.

SUMMARY

This master thesis on basis of „Personal data protection audit in the budgetary data controllers organizations". The master thesis studies the process of data protection audit, briefly depicts leagal status of the data protection in the world and Lithunia. It also describes the audit objectives and benefits. The describtion and analysis of the main data protection audit methods, forms and principles are also included in the Master thesis. Finnally, the Master thesis names the main problems in the system of data protection audit in budgetary data controllers organizations. It also compares the theory and practice of the field, sugest the possible ways to solve the existing problems.

1 PRIEDAS

ISO/IEC 17799:2005

Standarte naudojamų apsaugos priemonių sąrašas su trumpu paaiškinimu. (*tai nėra oficialus vertimas*)
ISO/IEC 17799:2005

1. Saugumo politika
    1. Informacijos apsaugos politika
        i. (1) Informacijos apsaugos politikos dokumentas (patvirtintas organizacijos vadovybės politikos dokumentas, su kuriuo supažindinami visi darbuotojai)
        ii. (2) Informacijos apsaugos politikos peržiūra (dokumentas peržiūrimas periodiškai arba atsiradus didesniems pokyčiams organizacijoje ar aplinkoje)
2. Informacijos apsaugos organizavimas
    1. Vidinis organizavimas
        i. (3) Vadovybės įsipareigojimai informacijos apsaugai (vadovybė užtikrina saugumą organizacijoje, demonstruodama palaikymą, bei numatydama atsakomybes)
        ii. (4) Informacijos apsaugos koordinavimas (informacijos apsaugos veiksmai turi būti koordinuojami, dalyvaujant atstovams iš skirtingų organizacijos skyrių)
        iii. (5) Informacijos apsaugos atsakomybių priskyrimas (visos atsakomybės, užtikrinant informacijos apsaugą, turi būti aiškiai apibrėžtos)
        iv. (6) Informacijos apdorojimo priemonių autorizavimo procesas (valdomas informacijos apdorojimo priemonių autorizavimo procesas turi būti nustatytas ir įgyvendintas)
        v. (7) Konfidencialumo reikalavimai (turėtų būti nustatyti ir reguliariai peržiūrimi konfidencialumo reikalavimai, atspindintys organizacijos poreikius)
        vi. (8) Kontaktai su informacijos apsaugos priežiūros institucijomis (turi būti palaikomi ryšiai su atitinkamomis priežiūros institucijomis)
        vii. (9) Kontaktai su specialistais (turi būti palaikomi ryšiai su informacijos apsaugos specialistais)
        viii. (10) Nepriklausomas informacijos apsaugos auditas (organizacijos informacijos apsaugos būklė turį būti reguliariai peržiūrima nepriklausomų ekspertų)
    2. Saugumas, susijęs su trečiosiomis šalimis
        i. (11) Rizikų, susijusių su trečiosiomis šalimis, identifikavimas (prieš suteikiant prieigą trečiosioms šalims, turi būti įvertintos rizikos ir priimtos atitinkamos priemonės)
        ii. (12) Saugumo aspektai dirbant su klientais (turi būti įvertinti visi saugumo reikalavimai, prieš suteikiant klientams prieigą prie organizacijos informacijos ar vertybių)
        iii. (13) Saugumo reikalavimai sutartyse su trečiosiomis šalimis (sutartyse su trečiosiomis šalimis turi būti įtraukti visi reikalingi saugumo reikalavimai)
3. Vertybių valdymas
    1. Atsakomybė už vertybes
        i. (14) Vertybių inventorizacija (visos organizacijos vertybės turi būti inventorizuotos)
        ii. (15) Vertybių savininkai (visos organizacijos vertybės turi turėti savininką)
        iii. (16) Tinkamas vertybių naudojimas (turi būti nustatytos, dokumentuotos ir įgyvendintos tinkamo vertybių naudojimo taisyklės)
    2. Informacijos klasifikavimas
        i. (17) Klasifikavimo gairės (informacija turi būti klasifikuojama jos vertės, teisinių reikalavimų, svarbumo bei kritiškumo organizacijai aspektais)
        ii. (18) Informacijos žymėjimas ir naudojimas (atsižvelgiant į organizacijos priimtą informacijos klasifikavimo schemą, turi būti parengtos ir įgyvendintos informacijos žymėjimo ir naudojimo procedūros)
4. Personalo saugumo aspektai
    1. Iki įdarbinant
        i. (19) Vaidmenys ir atsakomybės (atsižvelgiant į organizacijos saugumo politiką, turi būti nustatyti ir apibrėžti su informacijos apsauga susiję darbuotojų vaidmenys ir atsakomybės)
        ii. (20) Patikrinimas (turi būti atliekamas darbuotojų, rangovų, ar trečiųjų šalių pateiktų faktų, biografijos patikrinimas, atitinkantis teisinių aktų ir etikos reikalavimus)
        iii. (21) Terminai ir sąvokos darbo sutartyse (darbuotojai, rangovai ar trečiosios šalys turi pasirašyti sutartis, kuriose numatyta jų atsakomybė, susijusi su informacijos apsauga)
    2. Įdarbinus
        i. (22) Vadovybinė atsakomybė (organizacijos vadovybė turi užtikrinti, kad darbuotojai, rangovai ar trečios šalys laikytųsi saugumo reikalavimų, atsižvelgiant į organizacijos politiką ir atitinkamas procedūras)
        ii. (23) Informacijos apsaugos švietimas ir mokymas (visi organizacijos darbuotojai turi būti mokomi ir šviečiami informacijos apsaugos klausimais, atsižvelgiant į jų atliekamas funkcijas)
        iii. (24) Disciplinarinis procesas (turėtu būti numatytas formalus disciplinarinis procesas darbuotojams, pažeidusiems saugumo reikalavimus)
    3. Sutarties nutraukimas/pakeitimas
        i. (25) Atsakomybės, nutraukiant darbo sutartį (turi būti aiškiai apibrėžtos ir priskirtos atsakomybės, nutraukiant darbo sutartį)
        ii. (26) Vertybių gražinimas (visi darbuotojai, rangovai ar trečios šalys privalo gražinti organizacijai informacines vertybes iki nutraukiant sutartį)
        iii. (27) Prieigos teisių panaikinimas (darbuotojams, rangovams ar trečiosioms šalims suteiktos prieigos teisės turi būti panaikintos iki nutraukiant sutartį)
5. Fizinis ir aplinkos saugumas
    1. Saugios zonos
        i. (28) Fizinė perimetro apsauga (turi būti užtikrinama zonų, kuriose randasi informacija ar jos apdorojimo priemonės, perimetro

fizinė apsauga)
   ii. (29) Fizinė praėjimo kontrolė (saugiose zonose turi būti numatyta atitinkama praėjimo kontrolė , siekiant užtikrinti praėjimą tiktai autorizuotam personalui)
   iii. (30) Biurų, kabinetų ir informacijos apdorojimo priemonių apsauga (turi būti numatytos *fizinės* patalpų ir įrangos apsaugos priemonės)
   iv. (40) Fizinė apsauga nuo išorinių ir aplinkos grėsmių (turi būti numatyta fizinė apsauga nuo išorinių ir aplinkos grėsmių, tokių kaip gaisrai, užliejimas vandeniu ir kt.)
   v. (50) Darbas saugiose zonose (turi būti numatyta darbo tvarka saugiose zonose)
   vi. (60) Viešos prieigos, pristatymo ir iškrovimo zonos (viešos prieigos, pakrovimo ir iškrovimo zonos, t.y. zonos, į kurias patenka neautorizuoti asmenys, turi būti kontroliuojamos ir, jei tai įmanoma, izoliuotos nuo informacijos apdorojimo įrengimų)
2. Informacijos apdorojimo įrangos apsauga
   i. (61) Saugus įrangos išdėstymas (planuojant įrangos išdėstymą, pastatymo vietas turi būti numatyta jos apsauga nuo aplinkos grėsmių ir nuo neautorizuotos prieigos)
   ii. (62) Palaikymas (turi būti numatytos apsaugos priemonės, apsaugančios nuo elektros tiekimo sutrikimų, kondicionavimo sutrikimų, kitų informacijos apdorojimo priemonių veiklą palaikančių funkcijų sutrikimų)
   iii. (63) Elektros ir duomenų perdavimo linijų apsauga (elektros ir duomenų perdavimo linijos, kabeliai turį būti apsaugoti nuo pažeidimų)
   iv. (64) Įrangos priežiūra (įranga turi būti atitinkamai prižiūrima, užtikrinant jos prieinamumą ir vientisumą)
   v. (65) Įrangos už organizacijos ribų apsauga (turi būti įvertintos rizikos ir užtikrinta įrangos, esančios už organizacijos ribų, apsauga)
   vi. (66) Saugus įrangos utilizavimas ir pakartotinis panaudojimas (visa įranga, turinti galimybę saugoti informaciją, turi būti patikrinama prieš utilizuojant ar pakartotinai panaudojant)
   vii. (67) Nuosavybės apsauga (negalimas neautorizuotas įrangos ar informacijos patekimas už organizacijos ribų)
6. Ryšiai ir operacijų valdymas
   1. Veiklos procedūros ir atsakomybės
      i. (68) Dokumentuotos veiklos procedūros (veiklos procedūros turi būti dokumentuotos, prižiūrimos ir prieinamos vartotojams, kuriems jos reikalingos)
      ii. (69) Pokyčių valdymas (turi būti valdomi informacijos apdorojimo priemonių ir sistemų pokyčiai)
      iii. (70) Pareigų atskyrimas (pareigos ir atsakomybių ribos organizacijoje turi būti atskirtos)
      iv. (71) Kūrimo, testavimo ir veiklos aplinkų atskyrimas (turi būti numatytas šių aplinkų atskyrimas, siekiant apsaugoti nuo neautorizuotos prieigos prie sistemos ar jos pakeitimo)
   2. Trečiųjų šalių paslaugų teikimo valdymas
      i. (72) Paslaugų teikimas (turi būti užtikrinta, kad trečiosios šalys, teikiančios paslaugas, laikytųsi sutartyje apibrėžtų paslaugų lygio ir saugumo priemonių)
      ii. (73) Trečiųjų šalių teikiamų paslaugų stebėjimas ir peržiūra (turi būti atliekamas teikiamų paslaugų stebėjimas ir kontrolė)
      iii. (74) Trečiųjų šalių teikiamų paslaugų keitimų valdymas (turi būti atliekamas teikiamų paslaugų pokyčių stebėjimas ir kontrolė)
   3. Sistemų planavimas ir priėmimas
      i. (75) Pajėgumų valdymas (turi būti stebimas resursų panaudojimas, ir atliekamas pajėgumų planavimas, siekiant užtikrinti reikalaujamą sistemos našumą)
      ii. (76) Sistemų priėmimas (turi būti numatyti naujų sistemų, atnaujinamų sistemų priėmimo naudojimui kriterijai)
   4. Apsauga nuo kenksmingos programinės įrangos ir mobilaus kodo
      i. (77) Apsauga nuo kenksmingos programinės įrangos (turi būti įgyvendintos stebėjimo, prevencijos ir atstatymo priemonės apsaugai nuo kenksmingos programinės įrangos, taip pat turi būti numatytas vartotojų švietimas)
      ii. (78) Apsauga nuo mobilaus kodo, angl. - mobile code (turi būti užtikrinama, kad mobilaus kodo naudojimas būtų autorizuotas ir atitiktų saugumo politiką. Mobilaus kodo pavyzdžiai - JavaScript, VBScript, Java appletai, ActiveX priemonės)
   5. Atsarginės kopijos
      i. (79) Informacijos atsarginės kopijos (turi būti reguliariai daromos informacijos kopijos, ir išbandomas atstatymas atsižvelgiant į patvirtintą atsarginių kopijų darymo politiką)
   6. Tinklo saugumo valdymas
      i. (80) Tinklo valdymas (organizacijos tinklas turi būti valdomas tam, kad būtų užtikrinta apsauga nuo grėsmių, užtikrintas sistemų ir informacijos tinkle saugumas)
      ii. (81) Tinklo paslaugų (servisų) apsauga (turi būti nustatyti saugumo reikalavimai, paslaugų lygiai ir valdymo reikalavimai visoms tinklo paslaugoms)
   7. Laikmenų naudojimas
      i. (82) Pernešamų informacijos laikmenų valdymas (turi būti parengtos pernešamų laikmenų valdymo procedūros)
      ii. (83) Laikmenų utilizavimas (informacijos laikmenos turi būti saugiai utilizuojamos, laikantis formalių procedūrų)
      iii. (84) Informacijos naudojimo procedūros (turi būti parengtos informacijos naudojimo ir saugojimo procedūros)
      iv. (85) Sisteminės dokumentacijos apsauga (sisteminė dokumentacija turi būti apsaugota nuo neautorizuotos prieigos)
   8. Informacijos apsikeitimas
      i. (86) Informacijos apsikeitimo politika ir procedūros (siekiant užtikrinti informacijos apsikeitimo apsaugą, turi būti parengtos formalios politikos procedūros ir priemonės)
      ii. (87) Informacijos apsikeitimo sutartys (informacijos apsikeitimas tarp organizacijos ir kitų šalių turi būti reglamentuotas sutartyse)
      iii. (88) Fizinė laikmenų apsauga (transportuojant informacijos laikmenas už organizacijos ribų, turi būti užtikrinta laikmenų apsauga nuo neautorizuotos prieigos ar praradimo)
      iv. (89) Elektroninis susirašinėjimas (informacija, perduodama elektroninio susirašinėjimo metu, turi būti tinkamai apsaugota)
      v. (90) Biznio/biuro informacinės sistemos (turi būti numatytos politikos ir procedūros, siekiant apsaugoti biznio/biuro informacinėse sistemose esančią informaciją)
   9. Elektroninės komercijos paslaugos
      i. (91) Elektroninė komercija (elektroninės komercijos informacija, perduodama viešaisiais tinklais, turi būti apsaugota nuo jai kylančių grėsmių)

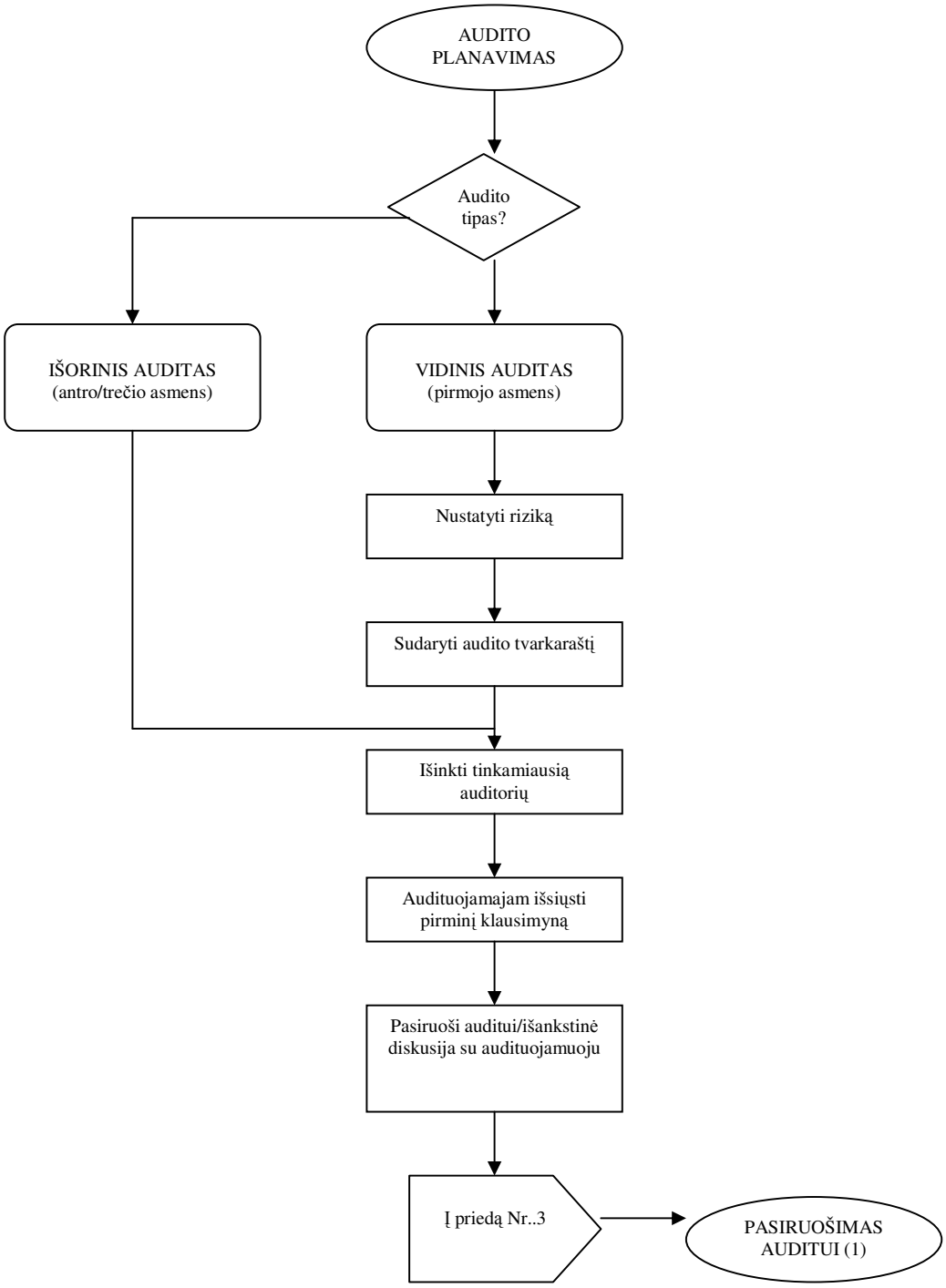
ii. (92) Elektroniniai mokėjimai (elektroninių mokėjimų informacija turi būti apsaugota nuo jai kylančių grėsmių)
iii. (93) Viešai prieinama informacija (turi būti užtikrinta viešai prieinamos informacijos vientisumo apsauga)

10. Stebėjimas
    i. (94) Žurnaliniai įrašai (turi būti pildomi ir nustatytą laiko tarpą saugomi žurnaliniai įrašai apie vartotojų veiksmus ir saugumo įvykius)
    ii. (95) Sistemų naudojimas (turi būti parengtos procedūros, leidžiančios registruoti informacijos apdorojimo priemonių panaudojimą)
    iii. (96) Žurnalinių įrašų apsauga (žurnaliniai įrašai turi būti apsaugoti nuo neautorizuotos prieigos ir pakeitimo)
    iv. (97) Administratorių ir operatorių veiksmų žurnaliniai įrašai (sistemų administratorių ir operatorių veiksmai turi būti registruojami)
    v. (98) Gedimų registravimas (gedimai turi būti registruojami, analizuojami ir priimamos atitinkamos priemonės)
    vi. (99) Laiko sinchronizavimas (laikas visose organizacijos informacijos apdorojimo priemonėse turi būti sinchronizuotas)

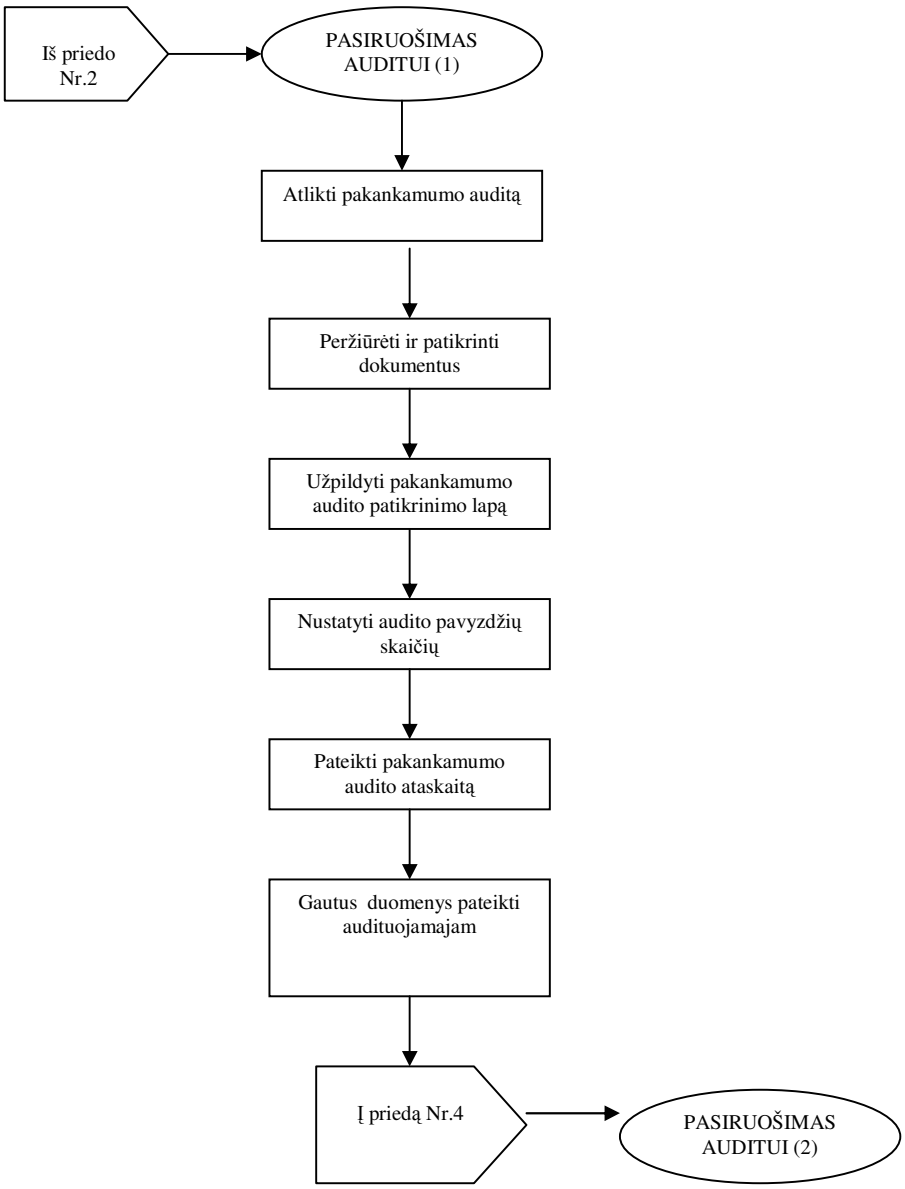
7. Prieigos valdymas
    1. Veiklos reikalavimai prieigos valdymui
        i. (100) Prieigos valdymo politika
    2. Vartotojo prieigos valdymas
        i. (101) Vartotojo registravimas
        ii. (102) Teisių valdymas
        iii. (103) Vartotojo slaptažodžio valdymas
        iv. (104) Vartotojo teisių peržiūra
    3. Vartotojo atsakomybės
        i. (105) Slaptažodžio naudojimas
        ii. (106) Įranga palikta be priežiūros
        iii. (107) Švaraus stalo ir švaraus ekrano politika
    4. Tinklo prieigos valdymas
        i. (108) Tinklo paslaugų (servisų) naudojimo politika
        ii. (109) Vartotojo autentifikavimas išoriniams prisijungimams
        iii. (110) Įrangos tinkle identifikavimas
        iv. (111) Nuotolinių priežiūros ir administravimo prieigų apsauga
        v. (112) Tinklų atskyrimas
        vi. (113) Tinklų sujungimo valdymas
        vii. (114) Tinklų maršrutizavimo valdymas
    5. Prieigos prie operacinės sistemos valdymas
        i. (115) Saugi įsiregistravimo procedūra
        ii. (116) Vartotojo identifikavimas ir autentifikavimas
        iii. (117) Slaptažodžių valdymo sistema
        iv. (118) Sisteminių programinių priemonių naudojimas
        v. (119) Sesijos time-out'as
        vi. (120) Sujungimo laiko apribojimas
    6. Prieigos prie aplikacijų ir informacijos valdymas
        i. (121) Prieigos prie informacijos ribojimas
        ii. (122)Svarbių sistemų izoliavimas
    7. Mobilūs įtaisai ir nuotolinis darbas
        i. (123) Mobilūs įtaisai ir komunikacijos
        ii. (124) Nuotolinis darbas

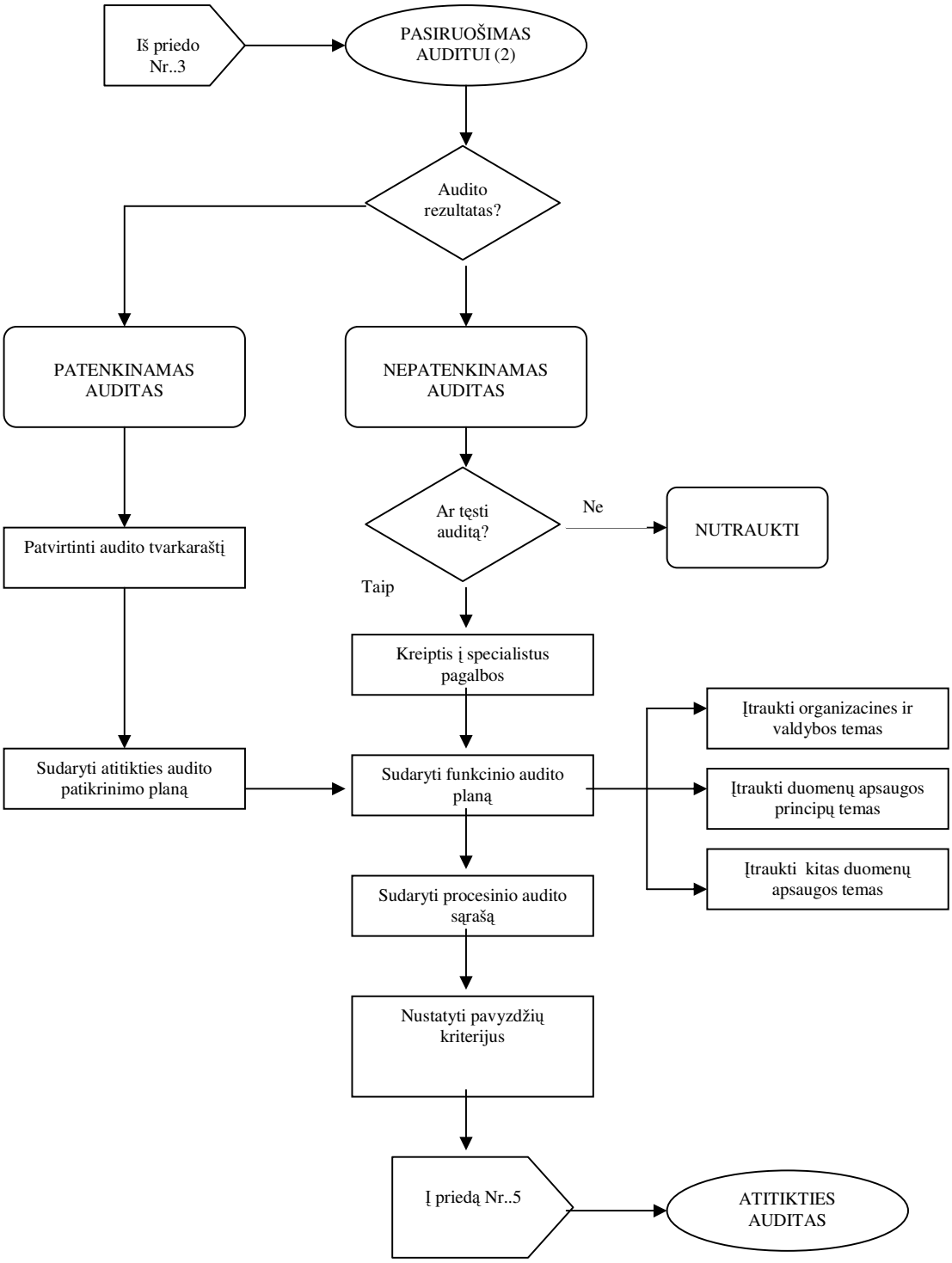
8. Informacinių sistemų įsigijimas, kūrimas ir priežiūra
    1. Saugumo reikalavimai informacinėms sistemoms
        i. (125) Saugumo reikalavimų analizė ir specifikavimas
    2. Tikslus programinės įrangos duomenų apdorojimas
        i. (126) Įvedamų duomenų tikrinimas
        ii. (127) Vidinio duomenų apdorojimo kontrolė
        iii. (128) Duomenų vientisumas
        iv. (129) Rezultato sutikrinimas
    3. Kriptografinės priemonės
        i. (130) Kriptografinių priemonių naudojimo politika
        ii. (131) Raktų valdymas
    4. Sisteminių bylų apsauga
        i. Operacinės programinės įrangos kontrolė
        ii. Sistemos testavimo duomenų apsauga
        iii. Prieigos prie programinio kodo valdymas
    5. Apsauga kūrimo ir palaikymo procese
        i. Pokyčių valdymo procedūra
        ii. Techninė sistemų peržiūra pakeitus operacinę sistemą
        iii. Programinės įrangos paketų keitimo ribojimai
        iv. Informacijos nutekėjimas
        v. Trečioms šalims perduotos programinės įrangos (outsourced) kūrimas
    6. Techninių pažeidžiamumų valdymas
        i. Techninių pažeidžiamumų valdymas

2 PRIEDAS

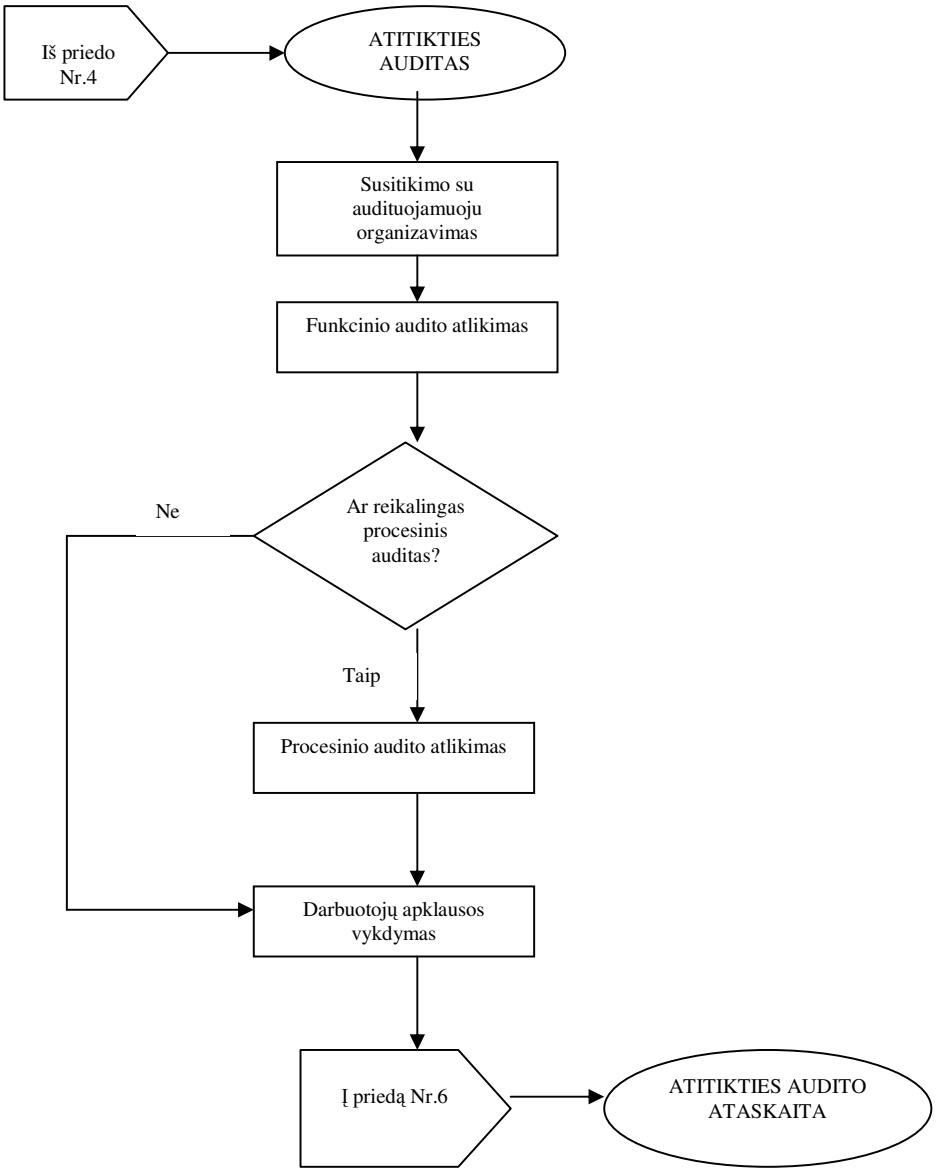

AUDITO PLANAVIMAS
Audito tipas?
IŠORINIS AUDITAS (antro/trečio asmens)
VIDINIS AUDITAS (pirmojo asmens)
Nustatyti riziką
Sudaryti audito tvarkaraštį
Išinkti tinkamiausią auditorių
Audituojamajam išsiųsti pirminį klausimyną
Pasiruoši auditui/išankstinė diskusija su audituojamuoju
Į priedą Nr..3
PASIRUOŠIMAS AUDITUI (1)

3 PRIEDAS

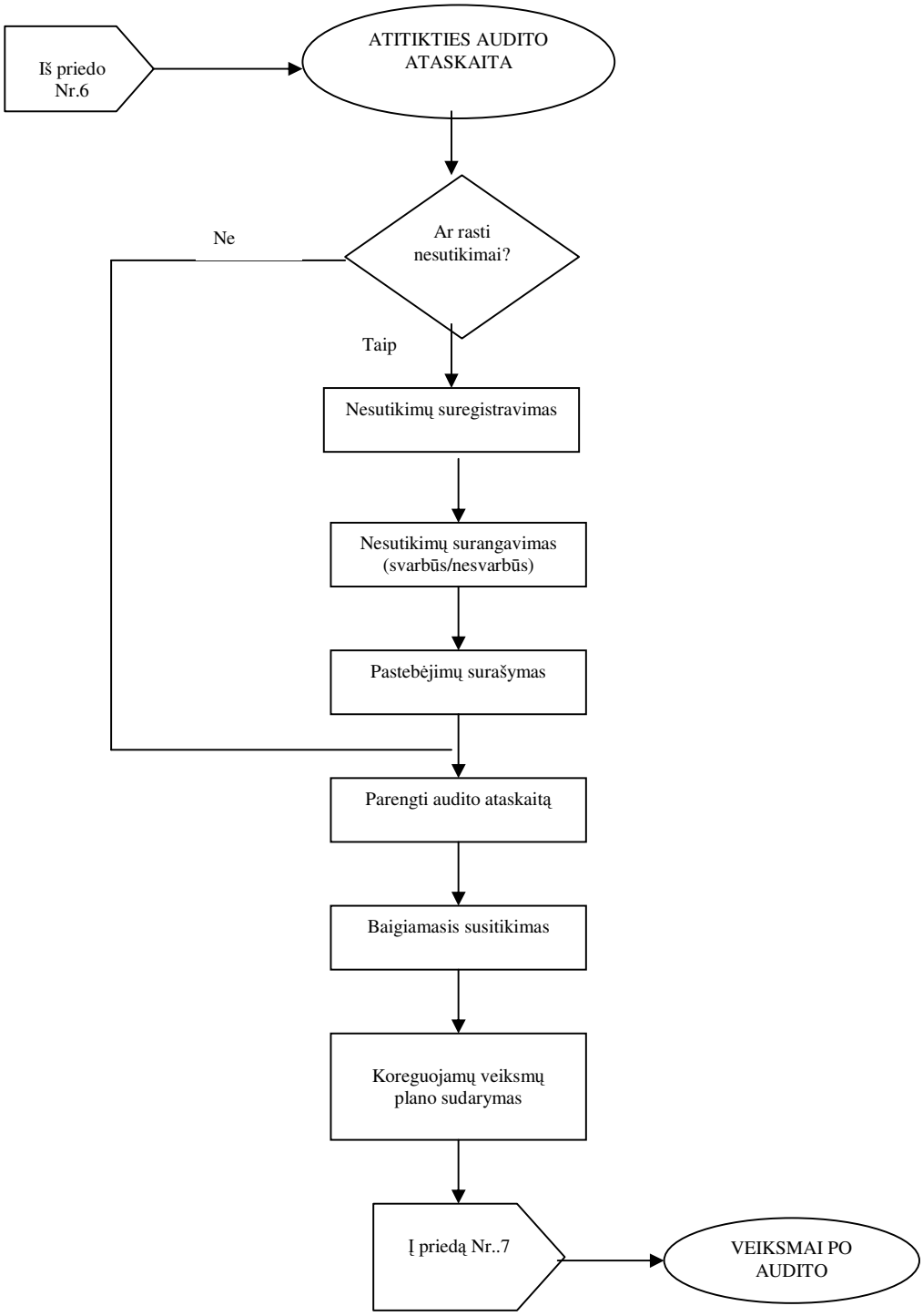

Iš priedo Nr.2
PASIRUOŠIMAS AUDITUI (1)
Atlikti pakankamumo auditą
Peržiūrėti ir patikrinti dokumentus
Užpildyti pakankamumo audito patikrinimo lapą
Nustatyti audito pavyzdžių skaičių
Pateikti pakankamumo audito ataskaitą
Gautus duomenys pateikti audituojamajam
Į priedą Nr.4
PASIRUOŠIMAS AUDITUI (2)


Iš priedo Nr..3
PASIRUOŠIMAS AUDITUI (2)
Audito rezultatas?
PATENKINAMAS AUDITAS
NEPATENKINAMAS AUDITAS
Ar tęsti auditą?
Ne
NUTRAUKTI
Taip
Patvirtinti audito tvarkaraštį
Kreiptis į specialistus pagalbos
Įtraukti organizacines ir valdybos temas
Sudaryti atitikties audito patikrinimo planą
Sudaryti funkcinio audito planą
Įtraukti duomenų apsaugos principų temas
Įtraukti kitas duomenų apsaugos temas
Sudaryti procesinio audito sąrašą
Nustatyti pavyzdžių kriterijus
Į priedą Nr..5
ATITIKTIES AUDITAS

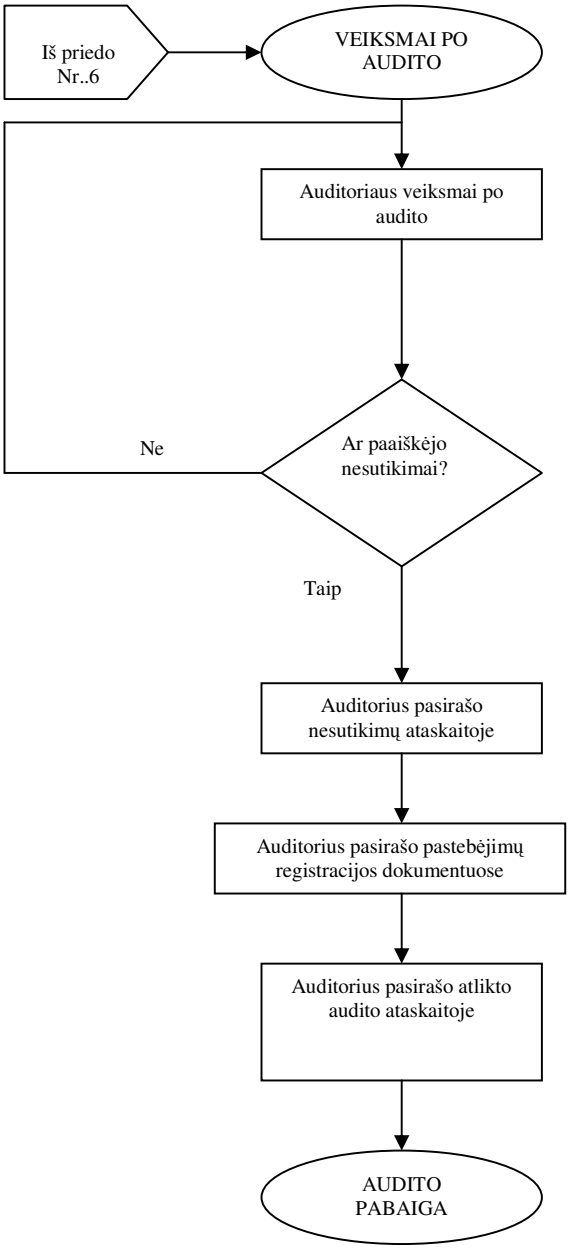
5 PRIEDAS


Iš priedo Nr.4
ATITIKTIES AUDITAS
Susitikimo su audituojamuoju organizavimas
Funkcinio audito atlikimas
Ar reikalingas procesinis auditas?
Ne
Taip
Procesinio audito atlikimas
Darbuotojų apklausos vykdymas
Į priedą Nr.6
ATITIKTIES AUDITO ATASKAITA

6 PRIEDAS


Iš priedo Nr.6
ATITIKTIES AUDITO ATASKAITA
Ar rasti nesutikimai?
Ne
Taip
Nesutikimų suregistravimas
Nesutikimų surangavimas (svarbūs/nesvarbūs)
Pastebėjimų surašymas
Parengti audito ataskaitą
Baigiamasis susitikimas
Koreguojamų veiksmų plano sudarymas
Į priedą Nr..7
VEIKSMAI PO AUDITO

7 PRIEDAS


Iš priedo Nr..6
VEIKSMAI PO AUDITO
Auditoriaus veiksmai po audito
Ar paaiškėjo nesutikimai?
Ne
Taip
Auditorius pasirašo nesutikimų ataskaitoje
Auditorius pasirašo pastebėjimų registracijos dokumentuose
Auditorius pasirašo atlikto audito ataskaitoje
AUDITO PABAIGA

8 PRIEDAS

Mykolo Romerio Universitetas
Viešojo administravimo fakultetas

Gerbiamas respondente,

Esu MRU viešojo administravimo magistratūros pakopos studentė ir atlieku tiriamąjį darbą „Duomenų apsaugos auditas“. Jūs buvote išrinkti iš Duomenų apaugos inspekcijoje registruotų asmens duomenų valdytojų. Prašau užpildyti šią anketą. Jūsų atsakymai padės išsiaiškinti darbo problemą ir tikslą. Atidžiai susipažinkite su kiekvienu klausimu ir atsakykite, pažymėdami (kryžiuku) labiausiai Jums tinkantį atsakymą (tiesiog paspauskite pelės kairiuoju mygtuku ant pilko langelio prie Jums labiausiai tinkančio atsakymo), jeigu nei vienas atsakymas netinka – prašome pažymėti variantą „kita“ ir paaiškinti, kodėl taip atsakėte. Jūsų atsakymai labai svarbūs kiekvienu keliamu klausimu, nuo to priklausys tyrimo rezultatų vertė. Anketa yra anoniminė. Tyrimo ataskaitoje bus naudojami tik apibendrinti duomenys. Dėkoju, už skirtą laiką ir kad sutinkate bendradarbiauti.

1. Jūsų organizacijos dydis:
☐ Mikro organizacija (iki 10 darbuotojų)
☐ Maža organizacija (nuo 11 iki 50 darbuotojų)
☐ Vidutinė organizacija (nuo 51 iki 250 darbuotojų)
☐ Didelė organizacija (virš 250 darbuotojų)

2. Asmens duomenų valdytojų registre įsiregistravote:
metais (įrašyti, *pvz. 1992*)

3. Organizacija savo veiklą vykdo nuo:
metų (įrašyti)

4. Ar yra organizacijoje raštu išdėstytos pagrindinės organizacijos informacijos apsaugos nuostatos, patvirtintos aukščiausios vadovybės?
Taip ☐ Ne ☐ Kita

5. Ar organizacijos informacinių sistemų (toliau anketoje – IS) veiklos procedūros dokumentuotos?
Taip ☐ Ne ☐ Kita

6. Ar parengti IS duomenų saugos nuostatai organizacijoje?
Taip ☐ Ne ☐ Kita

7. Ar yra organizacijoje paskirtas asmuo atsakingas už IS saugumo politikos įgyvendinimą?
Taip ☐ Ne ☐ Kita

8. Ar organizacijoje atliekamas kompiuterinių programų patikrinimas?
Taip ☐ Ne ☐ Kita

9. Ar yra organizacijoje saugumo politikos nuostatos, kurios aiškiai apibrėžia, kokia informacija yra saugoma, o kokia ne?

Taip ☐ Ne ☐ Kita

10. Ar organizacijoje yra formali ir nuolat atnaujinama duomenų apsaugos sistema?
Taip ☐ Ne ☐ Kita

11. Ar organizacijos duomenų apsaugos priemonių aprašas pateiktas Valstybinei duomenų apsaugos inspekcijai?
Taip ☐ Ne ☐ Kita

12. Ar apie asmens duomenų tvarkymą organizacijoje informuota Valstybinė duomenų apsaugos inspekcija?
Taip ☐ Ne ☐ Kita

13. Ar organizacijoje patvirtintos asmens duomenų tvarkymo taisyklės?
Taip ☐ Ne ☐ Kita

14. Ar organizacijoje yra įdiegtas ISO/IEC 17799:2005 standartas?
Taip ☐ Ne ☐ Kita

15. Ar Jūsų organizacijoje yra žmogus(-nės), atsakingas(-i) už duomenų apsaugą?
Taip ☐ Ne ☐ Kita

16. Ar organizacijos darbuotojai yra įtraukti į duomenų apsaugą?
Taip ☐ Ne ☐ Kita

17. Ar organizacijoje paruošti aiškūs (techniniai ir organizaciniai) nurodymai dėl to, kuris asmuo gali susipažinti su kokiais duomenimis?
Taip ☐ Ne ☐ Kita

18. Ar organizacijoje yra nustatytos vartotojų teisės kompiuterinėse sistemose?
Taip ☐ Ne ☐ Kita

19. Ar asmeniniais, organizacijoje saugomais duomenimis, gali naudotis visi organizacijos darbuotojai?
Taip ☐ Ne ☐ Kita

20. Ar visi organizacijos darbuotojai darbe naudojantys asmeninius duomenis yra apmokyti teisingai naudotis šiais duomenimis?
Taip ☐ Ne ☐ Kita

21. Ar organizacijoje saugomi asmens duomenys kaip nors šifruojami?
Taip ☐ Ne ☐ (į 22 klausimą neatsakinėkite) Kita

22. Kaip organizacijoje šifruojami saugomi asmens duomenys?
(įrašykite)

23. Ar parengta saugaus darbo su duomenimis tvarka?
Taip ☐ Ne ☐ Kita

24. Ar organizacijos elektroninis susirašinėjimas su antrosiomis šalimis ir organizacijos viduje yra apsaugotas?

Taip ☐ Ne ☐ (į 25 klausimą neatsakinėkite) Kita

25. Kokiomis priemonėmis apsaugotas elektroninis susirašinėjimas?

(įrašykite)

26. Ar yra nustatyta organizacijos turimos informacijos apsikeitimo politika ir procedūros su kitomis organizacijomis ir trečiosiomis šalimis?

Taip ☐ Ne ☐ Kita

27. Ar organizacijoje saugomų asmeninių duomenų laikymo ir saugojimo metodai yra aiškiai aprašyti?

Taip ☐ Ne ☐ Kita

28. Ar daromos organizacijoje saugomos informacijos atsarginės kopijos?

Taip ☐ Ne ☐ (į 29 klausimą neatsakinėkite) Kita

29. Kiek laiko saugomos atsarginės saugomos informacijos kopijos??

(įrašykite)

30. Ar yra įdiegta apsauga nuo kenksmingos programinės įrangos?

Taip ☐ Ne ☐ Kita

31. Ar organizacija valdo trečiųjų šalių paslaugų teikimo procesą?

Taip ☐ Ne ☐ Kita

32. Ar yra nustatyti techniniai ir organizaciniai apribojimai asmeninių duomenų perdavimui ir panaudojimui organizacijoje?

Taip ☐ Ne ☐ Kita

33. Per kiek laiko organizacija atsako į asmeninių duomenų užklausimą duomenų subjektams?

(įrašykite)

34. Ar duomenų subjektas turi galimybę susipažinti su savo asmenine informacija bei ją atnaujinti ar ištrinti?

Taip ☐ Ne ☐ Kita

35. Ar organizacijoje buvo atliekamas duomenų apsaugos auditas?

Taip ☐ Ne ☐ Kita

36. Jeigu atsakėte taip į 35 klausimą, kas jį atliko?

☐ vidaus auditorius
☐ išorės auditorius
☐ kita

Dėkoju už skirtą laiką.

9 PRIEDAS

lentelė. Respondentų veiklos pradžios ir registracijos duomenų valdytojų registre metai

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Įsiregistravo registre..	1994	2001	2002	2002	1994	2005	2006		2004	2006	2004	1992	2005	2005	1992	2002	1997
Vykdo veiklą nuo..	1950	2001	1950		1950	1950	1992	1950	1944	1987	1991	1990	2002	2002	1990	1950	

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	3	1994	1950	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	2	1	2		1	1		2	1	1	10m	1	2	2		1	2	
2	3	2001	2001	1	1	1	1	1	1	1	1	1	1	k	1	1	1	1	2	1			1	1		1	1	1		1	1	1		1	1	2
3	3	2002	1950	1	k		1	1	k		1	1	k	2	1	1	k	1	2	k	2		2	2			2	1	kol reikia	1	2	2	30	1	1	3
4	3	2002		1	1	1	1	1		1	1	1	1	k	1	1		1	2	1								1		1					2	
5	3	1994	1950	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	2	1	2		1	1		2	1	1	10m	1	2	2		1	2	
6	3	2005	1950	1	1	1	1	1	1	1	1	1	1	k	1	1	1	1	2	1	1		1	2		2		1		1		1		1	2	
7	3	2006	1992	1	1	1	1	1	1	1	1	1	2	k	1	k	1	2	1	1	1	SLL	1	2		1	1	1	10m	1	2	1	5	k	2	
8	4		1950	1	1	1	k	1	1	1	k	1	1	k	1	1	1	k	2	1	2		k	k		k	1	1		1	k	1	k	k	2	
9	3	2004	1944	2	2	2	2	2	1	1	1	1	2	k			1	1	2	1				1		1	1								k	
10	4	2006	1987	2	2	2	2	1		k	k	k	1	2	1	1	2	1	2	1	2		2			k	2	1	k	1	2	2	30	k	1	2
11	3	2004	1991	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	2		1	2		1	1	1		1	1	1		2	1	1
12	3	1992	1990	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2		1	2		1	1	1		1	2	1	10	1	2	
13	2	2005	2002	1	k	k	2	1	2	2	1	1	2	2	2	2	2	1	2	1	2		k	2		2	2	1	nuolat	1	k	2		1	2	
14	2	2005	2002	1	1	1		1	1	1	1	1	1	k	1	1	2	k	2	k			k			1	k			1	k	1		1	k	
15	4	1992	1990	k	1	k	1	1	k	2	2	1	1	k	1	1	2	1	2	1	1		2	1		2	1	1		1	2	1	3	2	2	
16	3	2002	1950	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2		1	2		2	1	2		1	2	1		1	2	
17	3	1997		1	1	1	1	1	2	1	1	1	1	k	1	1	2	1	1	1	2		1	2		1	2	1	įvairiai	1	1	1	30	1	2	

Paaiškinimai:

n (skaičius) – respondento numeris;

Viršutinėje eilutėje sužymėti anketos klausimų numeriai;

Atsakymų lentelės reikšmės (4 – 35 klausimams):

1 – “Taip”

2 – “Ne”

3 – “Kita”

1 klausimo atsakymų kodavimas: 2 – maža organizacija; 3 – vidutinė organizacija; 4 – didelė organizacija;

2 ir 3 klausimų atsakymų langeliuose surašyti konkretūs metai;

36 klausimo atsakymų kodavimas: 1 – vidaus auditorius; 2 – išorės auditorius; 3 – kita;