VILNIAUS UNIVERSITETAS
EKONOMIKOS IR VERSLO ADMINISTRAVIMO FAKULTETAS
VADYBOS KATEDRA

Margarita STRAŽNICKIENĖ
Kokybės vadybos programa

MAGISTRO DARBAS

INFOMACIJOS SAUGOS VADYBOS SISTEMOS NAUDOJIMOYPATUMAI

PECULIARITIES OF USE INFORMATION SECURITY MANAGEMENT SYSTEMS

Leidžiama ginti _____

(parašas)

Katedros vedėja prof. **D. Diskienė**

Magistrantas _____

(parašas)

Darbo vadovas_____

(parašas)

Asist. **D. Ruželė**

Darbo įteikimo data:

Registracijos Nr.

Vilnius, 2018

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Temos aktualumas. Šiuolaikiniame pasaulyje, atsiradus naujoms ir patogioms techninėms priemonėms, atsirado ir informacijos saugos problema. Gaminant kokybišką produkciją ir teikiant išskirtines paslaugas, organizacijoms yra labai svarbu saugoti paslaptyje reikalingą informaciją nuo konkurentų, kad išlaikyti palankią poziciją rinkoje. Konkurencinėje kovoje plačiai taikomi skirtingi veiksmai, skirti gauti konfidencialius duomenis skirtingais būdais. Tokiu atveju, rinkos lyderiais tampa organizacijos, kurios naudojasi tarptautine praktika, kuria informacijos saugos valdymo sistemas. Tai paaiškinama reikšmingų duomenų apdorojimu korporatyvinėje informacinėje sistemoje, kiekio padidėjimu.

Mūsų laikais didelį kiekį duomenų galima patalpinti nedideliuose portatyviniuose įrenginiuose, o procesoriai gali apdirbti milžinišką duomenų kiekį. Bet kartu su naujomis informacinėmis technologijomis atsirado naujos problemos ir naujos nusikalstamumo rūšys, t.y. naujos informacijos saugos grėsmės (Pardo ir kt., 2016; Grigorjeva, Meškov, 2006) Tai kompiuteriniai virusai, hakeriai, pramoninis šnipinėjimas, duomenų vagystė, teroras, šantažas ir t.t. Šių grėsmių šaltiniais gali būti informaciniai tinklai ir sistemos, darbuotojai, vartotojai, finansinės organizacijos ir valstybinės įstaigos. Silpna apsauga taip pat yra nuolatinis informacijos grėsmės šaltinis. Šiandien kaip niekada verslo konkurencingumas bet kurioje verslo srityje priklauso nuo informacinio turto. Siekiant užtikrinti efektyvią informacijos saugą, reikalaujami sisteminiai sprendimai, grindžiami šiuolaikiniu rizikos valdymu ir integruoti į bendrą organizacijos valdymo sistemą. Informacijos saugos valdymas – tai užduotis, kurią organizacijos vadovai turi spręsti kiekvieną dieną, nepriklausomai nuo veiklos specifikos, apimties ir kitų faktorių (Dmitriev, 2014; Dorofeev, Markov, 2014)

Darbo naujumas. Standartas ISO 27001:2013 sukurtas prieš penkis metus, taigi jo naudojimo ypatumai nėra plačiai analizuojami. Labai mažai literatūros, nagrinėjančios būtent 2013 metais sukurto standarto naudojimo ypatumus, dažniausiai analizuojama visa ISO 27001 standartų visuma, tačiau pavyko rasti duomenų, kurie išsamiai aprašo 2005 ir 2013 metų išleistų standartų skirtumus. Iš šios literatūros verta paminėti Cosutic, D., 2017; Dmitriev, 2014; RAI Technology University ir t.t. Mokslinėje literatūroje plačiai nagrinėjami taikomos informacijos saugos priemonės (Šahalov, Dorofeev, 2013; Tibetkin, 2017; Rajkova, 2013).

Baigiamasis darbas įneša naujoves į informacinės saugos analizę, kadangi darbe plačiai palyginamos skirtingos standartų versijos, paryškinami skirtumai standartų turinyje. Atliekant mokslinės literatūros analizę pažymimi konkretūs standarto naudojimo ypatumai, vardinamos konkrečios saugos užtikrinimo priemonės ir jų taikymo ypatumas bendrovėse su skirtinga veiklos specifika.

Tyrimo objektas: informacijos saugos sistemų naudojimas.

Tyrimo problema – mokslinėje literatūroje nėra griežtai apibrėžta kokios informacijos saugos priemonės gali užtikrinti informacijos saugą, to nenumato ir pats ISO standartas, todėl kuo gilesnė praktinė standarto taikymo analizė skirtinguose veiklos srityse gali palengvinti diegiančiųjų ir naudojančių ISO 27001 standarto veiklą.

Darbo tikslas: atlikus tyrimą, identifikuoti standarto ISO 27001:2013 naudojimo ypatumus.

Darbo uždaviniai:

1. Atlikus mokslinės literatūros analizę, suformuoti teorinį standarto ISO 27001 diegimo modelį;
2. Remiantis teoriniu ISO 27001 diegimo modeliu sudaryti tyrimo metodologiją, kurios pagrindas mokslinės literatūros analizės rezultatai;
3. Atlikus pusiau struktūrinio interviu tyrimą, nustatyti standarto diegimo praktinius aspektus;
4. Susisteminus interviu turinio rezultatus sukurti ISO 27001:2013 standarto diegimo Lietuvos bendrovėse praktinį modelį;

Tyrimo atlikimo galimybės ir tyrimo apribojimai

Lietuvoje palygintinai nedaug bendrovių naudoja ISO 27001:2013 standartą, todėl kiekybinis apklausos tyrimas buvo netinkamas tyrimo atlikimui, be to atliekant apklausą, anketą gali užpildyti nekompetentingi asmenys, kas gali iškreipti rezultatus. Todėl nuspręsta atlikti pusiau struktūrinį ekspertų interviu. Buvo apklausti bendrovių, kuriuose jau įdiegtas ISO 27001:2013 standartas, vadovai, kokybės vadovai, informacinių technologijų specialistai.Tyrimui buvo naudojami 4 ekspertų interviu duomenys, kurių pagalba buvo pasiektas baigiamojo darbo tikslas.Lietuvoje ISO 27001 nėra plačiai taikomas, todėl specialistų, galinčių suteikti tinkamą medžiagą apie minėto standarto naudojimą yra labai mažai.

Tyrimo metodai: Analizė, duomenų lyginamoji analizė, pusiau struktūrinis ekspertų interviu, duomenų sisteminimas.

Darbo struktūra. Baigiamąjį darbą sudaro trys pagrindinės dalys: pirmoje dalyje apžvelgiamos informacijos saugos valdymo sistemos ISO 27001:2013 naudojimo ypatumų mokslinės prielaidos. Antroje dalyje išsamiai aprašyta tyrimo metodologija. Trečioje dalyje aprašyti susisteminti pusiau struktūrinio interviu su ekspertais rezultatai.

Darbo apimtis 55 puslapiai, pateikiami 9 paveikslai ir 8 lentelės, panaudota 42 mokslinės literatūros šaltinių.

1. LITERATŪROS APIE INFORMACIJOS SAUGOS VALDYMO SISTEMOS ISO 27001:2013 NAUDOJIMO YPATUMUS APŽVALGA

1.1. Kokybės kaip valdymo proceso naudojimo evoliucija, informacinės valdymo sistemos atsiradimo gairės

Kokybės valdymas yra ISO standartų diegimo pagrindas. Kokybės valdymo teorijos modernizavosi ilgą laiką, kol nebuvo sukurta kokybės valdymo sistema ISO, kuri ir tapo standarto ISO 27001:2013 kūrimo ir diegimo pirminiu šaltiniu. Darbe analizuojama kokybės valdymo evoliucija, siekiant nustatyti, kaip vystėsi kokybės valdymo principai, kaip keitėsi valdymo prioritetai su laiku, kol įgijo šiuolaikinę prasmę.

A. Tibetkin (2017) teigia, kad kokybės valdymo vystymas dažniausiai yra siejamas F. Teiloro sistemos atsiradimu, kuris:

- Sukūrė mokslinio valdymo koncepciją;
- Pažymėjo gamybos proceso nuolatinio tobulinimo būtinumą;
- Įvertino gamybos proceso pokyčių kontrolės svarbą.

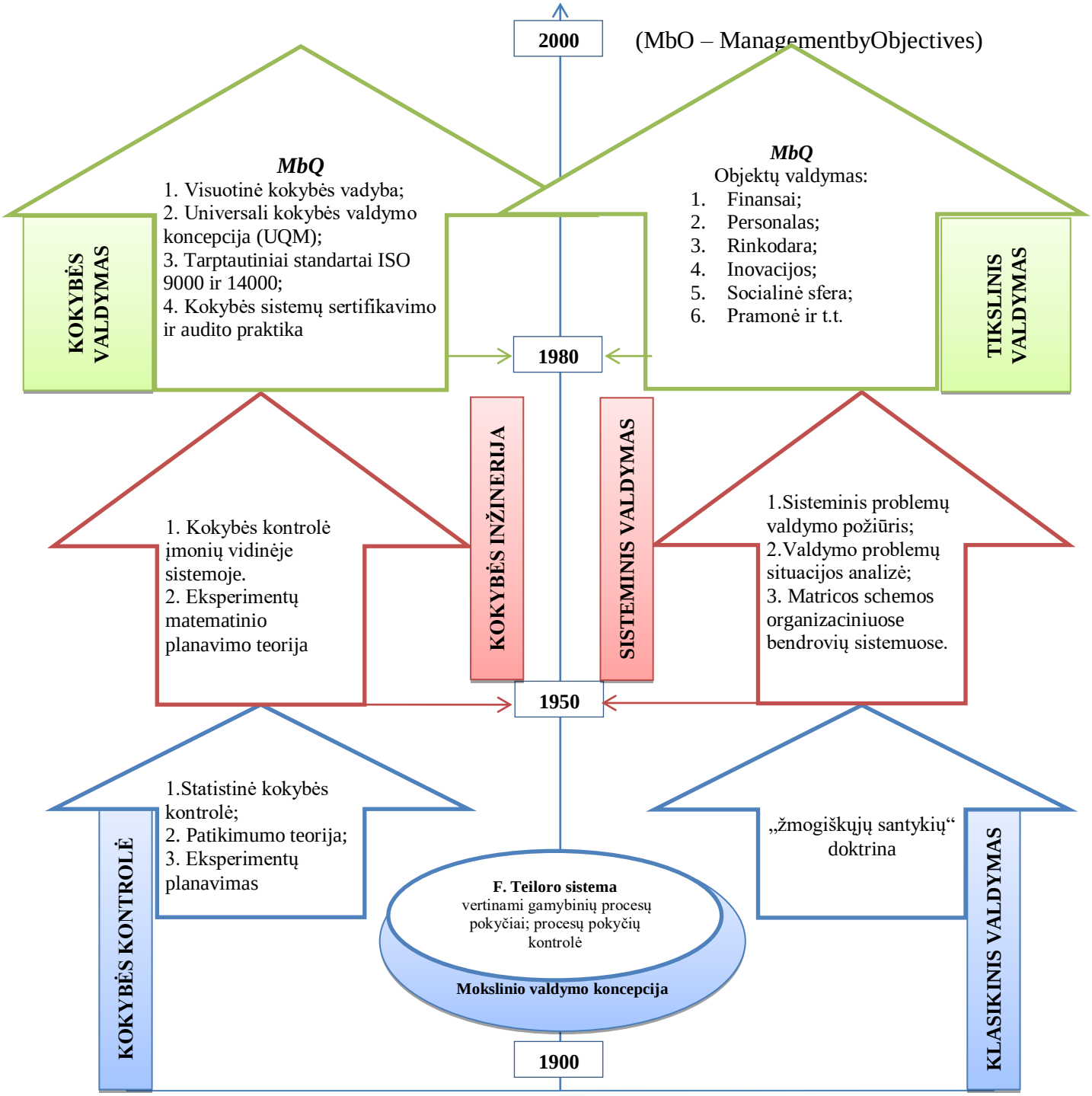
F. Teiloro sistema nagrinėja kokybės viršutinę ir apatinę ribas: nagrinėja tokių kontrolės matavimų priemonių naudojimą kaip: kalibrai, šablonai, pagrindžia būtinumą:

- Sukurti nepriklausomų kokybės inspektorių etatus organizacijose;
- Baudų sistemos taikymą nekokybiškai dirbančiam personalui;
- Skirtingų metodų ir formų kūrimą, siekiant gerinti produkcijos kokybę (Tibetkin, 2017).

F. Teiloro sistema yra kokybės valdymo pagrindas, kurio evoliucijos procesą galima suskaidyti į keturis pagrindinius etapus (Juran, 2004):

1. Teiloro sistemos atsiradimas ir vystymas (1900 – 1920 m.).
2. Antras kokybės valdymo etapas (1920 – 1950 m.), kai klasikiniame valdyme dominuoja „žmogiškųjų santykių“ doktrina, o sprendžiant kokybės klausimus:
    - Atsiranda statistiniai kontrolės valdymo metodai (SQC – Statistical Quality Control)
    - Gamybos procese įvedamos kokybės kortelės ir pagrįsti pasirinktiniai produkcijos kokybės ir technologinių procesų kontrolės metodai.
    - Kuriama patikimumo teorija, atsiranda pirmieji darbai eksperimentų planavimo srityje, kurie tapo eksperimentų matematinio planavimo pagrindu.

3. Trečiam kokybės valdymo evoliucijos etapui priskiriami 1950 – 1980 metai. Šiuo laikotarpiu problemų valdymas tapo sisteminiu procesu: plačiai naudojama situacijos analizė, organizacijos valdymo struktūroje pradėta naudoti matricos schemas (Juran, 1998).
4. Ketvirtame etape 1980 – 2000 m. Kokybės valdymas įgavo dvi kryptis: tikslinis valdymas ir kokybės valdymas.
5. Vėliau 4 punkto dvi kryptys buvo tobulinamos.



1pav. **Kokybės valdymo sistemos evoliucija**

(šaltinis: parengta autorės, remiantis Juran, 1998; Vasin, 2017)

Kokybės valdymo atžvilgiu šis periodas charakterizuojamas įmonių viduje integruotų kokybės kontrolės procesų vystymu, tokių kaip:

- TQC – Total Quality Control – bendra kokybės kontrolė (Feigenbaum) (RAI technology University, interaktyvus);
- CWQC – Cmpany Wide Quality Control – kokybės kontrolė visos kompanijos mastu (Isakava) (Prof. Ishikawa and Quality Control, interaktyvus);
- QC – Quality Circles – kokybės ciklai (Taguti) (Quality Engineering and Taguchi Methods: A Perspective, 1989);
- QFD – Quality Function Deployment – kokybės funkcijų diegimas (Quality Concepts, interaktyvus);
- ZD – zerodefect – „nulis defektų“ sistema (žr. 1 pav.)(Vasin, 2017)

Trečią kokybės valdymo periodą priimta vadinti „kokybės inžinerija“, kadangi valdymo sąvoka dar nebuvo naudojama specialistų leksikone (Juran, 1998)

Trečiam kokybės valdymo periodui būdinga:

- Valdymo mokslinių priemonių platus naudojimas;
- Sprendžiant kokybės užtikrinimo problemas buvo akcentuojami organizaciniai klausimai;
- Organizacijos aukščiausios valdymo grandies išskyrimas sprendžiant produkcijos kokybės klausimus;
- Inžinerinių metodų akcentavimas užtikrinant produkcijos kokybę (Ovsianko, 2011);

Problemų, susijusių su produkcijos kokybės užtikrinimu sprendimas, šioje stadijoje, sąlygoja adekvačios organizacinės struktūros atsiradimą, kuri apima visus organizacijos skyrius, kiekvieną įmonės darbuotoją, visose produkcijos gyvavimo stadijose, pradedant projektavimu ir baigiant utilizacija (Ovsianko, 2011)

Visi trečiai stadijai būdingi pokyčiai kokybės valdymo procese, lėmė TQM (Total Quality Management – visuotinės kokybės vadybos) ir UQM (Universal Quality Management – universalios kokybės vadybos) koncepcijų formavimą, kurios tapo ketvirtos stadijos pradžia (Freidina, 2011).

6. Ketvirtas kokybės valdymo evoliucijos etapas charakterizuojasi tuo, kad kokybės valdymo suvokimas buvo pildomas vis naujais gamybinės sistemos elementais, elementai buvo kaupiami ir integruojami. Kartu, bendrame valdyme atsirado naujos šios disciplinos diferencijavimo tendencijos skirtingose kryptyse: finansai, personalas, inovacijos, marketingas, investicijos ir t.t.; Teoriniu požiūriu bendras valdymas

formuojasi kaip tikslinis – vadyba remiantis tikslais MBO (Management by objectives) – tikslinis valdymas.

Pagrindinę MBO (tikslinio valdymo) idėją sudaro tikslų struktūrizavimas ir nagrinėjimas (tikslų medžio sudarymas), o po to organizacijos motyvacijos ir tikslų siekimo projektavimas. MBO strategija gana populiari ir sutampa su pagrindiniu kokybės valdymo tikslu – kokybės užtikrinimu (Alsaquicy , 2013)

Kokybės valdymo evoliucijos laikotarpiu susiformavo pakankamai daug teorinių ir empirinių priemonių ir metodų. Priemonių, metodų ir sistemų sąveika vadinama MBQ (Quality management) – kokybės valdymas (Kuznecova, 2013):

- Pirma, tai 24 tarptautiniai ISO 9000 ir ISO 14000 šeimos standartai (ekologinis valdymas).
- Antra, tarptautinė kokybės sistemų sertifikavimo praktika, kurią sudaro šimtai akredituotų sertifikavimo organų.
- Trečia, tarptautinis sertifikuotų kokybės sistemų auditorių registras (IRCA), kuriame įregistruoti tūkstančiai specialistų dirbančių skirtingose šalyse.
- Ketvirta, susidarė tarptautinė kokybės vadybos audito sistema su išvystyta struktūra regionų ir nacionaliniu lygiu.
- Penkta, tarptautinėje pasaulinėje rinkoje aktyviai veikia apie 100 000 skirtingų bendrovių, turinčių vidinius kokybės užtikrinimo sertifikatus (Kuznecova, 2013):

Trumpai aptarus kokybės evoliuciją, verta sutelkti dėmesį ties kokybės gerinimo principais ir jų palyginimu. Reikšmingą indėlį į kokybės valdymo teoriją įnešė Demingas, vienas iš „japoniško ekonominio stebuklo“ kūrėjų. Manoma, kad būtent Demingo dėka atsirado kokybiška ir nebrangi produkcija (Lagutkina, 2008; Nikolaeva, 2004; Pronnikov, Ladonov , 2004).

Priimant nuokrypių egzistavimą, būtina sekti dirbtinai atsiradusius nuokrypius ir aiškinti jų atsiradimo priežastis. Demingo idėjos pagrindas - užduočių rezultatų vertinimo panaikinimas. Toks vertinimas sudaro „baimės“ atmosferą, lemia trumpalaikių tikslų orientaciją, ignoruojant ilgalaikius tikslus ir trukdo kolektyviniam darbui (Šonberger, 2003; Nikolaeva, 2004).

Kokybės valdymo principus nagrinėjo ne tik Deming (1 lentelėje pateiktos dar trijų autorių nuomonės, šios nuomonės yra labai populiarios ir plačiai taikomos praktikoje).

1 lentelė. **Kokybės valdymo principai**

(šaltinis: parengta autorės, remiantis Henry; Juran, 1998; Suarez, 1992)

W. E. Deming (Henry: interaktyvus)	**J.E. Juran (Juran, 1998)**	**B. Krosbi (Suarez,1992)**
1. Sekti tikslų nuoseklumą	1. Formuoti suvokimą apie kokybiško darbo būtinumą ir suteikti sąlygas kokybės gerinimui.	1. Griežtai nustatyti vadovybės pareigą kontroliuoti nuolatinį kokybės gerinimą.
2. Priimkite nauja filosofiją: atsisakykite žemos kokybės visose srityse.	2. Nustatyti tikslus nuolatiniam veiklos tobulinimui.	2. Komandinio darbo naudojimas kokybės gerinimui, siekiant įtraukti ir informuoti visus organizacijos darbuotojus apie kokybę.
3. Atsisakykite nuolatinės kontrolės.	3. Sukurti organizaciją, galinčia efektyviai dirbti siekiant tikslų, suformuoti komandas ir pasirinkti koordinatorius.	3. Kokybės įvertinimas, ir einamų ir potencialių kokybės problemų nustatymas.
4. Atsisakykite partnerystės, kuri remiasi tik produkcijos kaina: užmegzkite ilgalaikius partnerystės ryšius, sumažinkite tiekėjų skaičių.	4. Visiems organizacijos darbuotojams suteikti galimybę mokytis.	4. Nustatyti kokybės kainą.
5. Nuolat tobulinkite gamybos ir aptarnavimo sistemą.	5. Įvykdyti projektus problemų sprendimui.	5. Nustatyti nekokybiško darbo kainą ir informuoti apie tai darbuotojus.
6. Praktikuokite mentorystę ir mokymus.	6. Informuoti organizacijos darbuotojus apie pasiekimus.	6. Veiksmų koregavimas.
7. Įdiekite šiuolaikinius valdymo metodus; valdymo funkcijos turi pereiti nuo kiekybinių kontrolės rodiklių prie kiekybinių.	7. Atsidėkoti darbuotojams, labiausiai prisidėjusiems prie kokybės gerinimo proceso.	7. Specialaus komiteto, dirbančio pagal „nulinio broko“ programą kūrimas.
8. Likviduokite baimę	8. Informavimas apie rezultatus	8. Specialistų, kurie diegs „nulinio broko“ programą apmokymas.
9. Pašalinkite barjerus tarp padalinių ir organizacijos darbuotojų.	9. Pasiekimų registravimas.	9. „Nulinio broko dienos“ organizavimas, siekiant išaiškinti programą ir organizacijos požiūrį į kokybės problemą.
10. Atsisakykite lozungų, transparantų ir nurodymų darbuotojams.	10. Pasiekimų, kurių pavyko pasiekti per metus, įdiegimas į nuolat funkcionuojančias organizacijos sistemas ir procesus.	10. Personalo motyvavimas kokybės gerinimo tikslų nustatymui.
11. Atsisakykite kiekybinio darbo vertinimo.		11. Stimuliuoti personalą informuoti apie atsiradusias problemas, trukdančius jiems dirbti be broko.
12. Palaikykite darbuotojų profesionalaus pasididžiavimo jausmą.		12. Visuomeninis pripažinimas tų, kurie pasiekia nustatytus tikslus ir puikiai atlieka darbus.
13. Įdiekite išsilavinimo ir nuolatinio tobulinimo sistemą.		13. Komandos iš profesionalų ir kolektyvų vadovų kūrimas, kurie nuolat palaikys tarpusavio bendravimo ryšį.
14. Perduokite kokybės idėja, kaip pagrindinę veiklos idėją organizacijos valdybai.		14.Nuolatinis punktų 1 – 13 kartojimas, kadangi kokybės gerinimo procesas yra beribis.

Apibendrinant galima teigti, kad tikslo siekimo strateginiai požiūriai, kaip bendrame valdyme, taip ir kokybės valdymo atžvilgiu ketvirtame vystymo etape yra identiški. Kokybės

valdymas – ketvirtos kartos valdymas – tampa tarptautinėje rinkoje sėkmingai veikiančių organizacijų pirmaujanti valdymo forma. Ketvirtame etape galima stebėti integravimo procesą tarp MBO (tikslinis valdymas) ir MBQ (kokybės valdymas), kaip buvo pirmame bendrojo valdymo vystymo etape. Bet šį integracija vykdoma aukštesniame mokslinių disciplinų vystymo lygyje.

W. E. Demingas (Henry, interaktyvus) pagrindinį dėmesį skyrė kokybės gerinimui procesuose ir sistemose. J. E. Juran (1998) išskyrė kiekvieno vadybininko individualumą, siekiant kokybės gerinimo. Juran skatina personalo įtraukimą į procedūrą, skatinant produkcijos kokybės gerinimą. B. Krosbi (Suarez, 1992) akcentuoja organizacijos vadovų svarbą užtikrinant aukštą kokybę, jų pareiga yra informuoti darbuotojus apie nekokybiškos produkcijos neigiamą įtaką organizacijai ir skirti maksimaliai galimas pastangas darbuotojų kvalifikacijos kėlimui.

1.2. Informacijos apsaugos valdymo sistemos atsiradimo gairės, valdymo standartai, kaip pagrindas ISO 27001

1.2.1. Standartų esmės lyginamoji analizė

ISO 900x – tarptautinių standartų serija, aprašanti reikalavimus organizacijos kokybės vadybos sistemai. Standartų ISO 900x serija sukūrė Tarptautinės standartizavimo organizacijos techninis komitetas. Standarto pagrindu tapo pagrindinės visuotinės kokybės vadybos teorija (TQM) (Šahalov, Dorofeev, 2013).

ISO 900x standartų serija liečia skirtingus kokybės valdymo aspektus, į standartų sąrašą įeina ir populiariausias ISO 9001 standartas. Standartus sudaro gairės ir instrumentai skirti organizacijoms, norinčioms, kad jų gaminama produkcija ir teikiamos paslaugos nuolat tenkintų klientų poreikius, o paslaugų ir produkcijos kokybė pastoviai gerėtų. Standartas ISO 9001:2015 - nustato reikalavimus kokybės valdymo sistemai, o ISO 9000 standartą sudaro pagrindinės sąvokos ir žodynas. ISO 9004 standartas akcentuoja dėmesį į kokybės valdymo sistemos efektyvumo didinimą. ISO 19011 – tai vidinio ir išorinio kokybės vadybos sistemos audito atlikimo vadovas (Čekmariov, 2007).

ISO 9001:2015 nustato reikalavimus kokybės valdymo sistemoms ir yra vienintelis standartas, pagal kurį gali būti atlikta išorinė akreditacija (nors tai nėra pagrindinis reikalavimas). Jis gali būti naudojamas bet kurioje organizacijoje, nepriklausomai nuo veiklos sferos (Šestopal, 2010)

Standarto pagrindą sudaro eilė kokybės valdymo principų, didelis dėmesys yra skirtas kliento pasitenkinimui, motyvacijai ir aukščiausiosios grandies vadovų įtraukimui į kokybės

gerinimo procesą, procesiniam požiūriui ir nuolatiniam tobulinimui. ISO 9001:2015 garantuoja, kad vartotojas gauna produkciją ir paslaugas stabiliai aukštos kokybės. Sistemos našumo tikrinimas yra svarbi standarto ISO 9001:2015 dalis. Organizacijos turi atlikinėti kokybės valdymo sistemos patikrinimo vidinius auditus. Organizacija gali priimti sprendimą patikros atlikimui pakviesti nepriklausomą organą (Tarptautiniai standartai ISO serijos, 2015)

ISO/IEC 2700x tarptautinių standartų serija, kurią sudaro informacijos apsaugos standartai paskelbti bendradarbiaujant Tarptautinei Standartizavimo Organizacijai ir Tarptautinei Elektrotechninei komisijai (IEC) (Čobanian, Šahalov, 2013).

Seriją sudaro geriausios praktikos ir rekomendacijos informacijos saugos srityje siekiant kurti, vystyti ir palaikyti informacijos saugos valdymo sistemą. Serija ISO/IEC 2700x demonstruoja visą seriją tarptautinių normatyvinių dokumentų, susidedančių iš taisyklių, saugos priemonių, valdymo principų (Čobanian, Šahalov, 2013).

Vienas populiariausių ir praktiškų standartų ISO/IEC 27001:2005 „Informacinės technologijos – saugos aprūpinimo metodai ir priemonės – Informacinės saugos valdymo sistemos – reikalavimai. Standartas apibrėžia informacinę saugą kaip: „konfidencialumo, bendrumo ir informacijos prieinamumo aprūpinimas; be to gali būti įtrauktos ir kitos savybės, kaip autentiškumas, patikimumas“ (Šahalov, Dorofeev, 2013).

Standartą sudaro informacinės saugos valdymo sistemos diegimo vadovas, taip ir trečios šalies sertifikato, liudijančio, kad saugos valdymo priemonės egzistuoja ir funkcionuoja laikantis standarto reikalavimų gavimo. Standartas apibrėžia informacinės saugos valdymo sistemą, kaip aprėpiančią visokeriopas sritis valdymo sistemą, sudarytą remiantis verslo rizikos principais ir sukurtą saugos valdymo sistemos įdiegimui, eksploatavimui, monitoringui ir palaikymui sudarytą remiantis verslo rizikos principais (Pardo, C; Pino, F.J., Garcia, F., 2016).

9001 ir ISO 27001 panašumai**:**

- Abu standartai sudaryti remianti „procesinio požiūrio“ principu kuriant, diegiant ir gerinant informacinės saugos valdymo sistemos rezultatyvumą. Procesinis požiūris suvokiamas kaip organizacijos naudojama valdymo procesų sistema, užtikrinanti veiksnių tarpusavio sąveiką. Pagrindinis šio požiūrio privalumas yra nenutrūkstantis procesų, jų kombinacijų ir sąveikos valdymas. Viena iš „procesinio požiūrio“valdymo įdiegimo metodikų – yra klasikinis uždaras valdymo ciklas Plan – Do – Check – Act (PDCA, planavimas – vykdymas – tikrinimas – veiksmas), žinomas kaip „Demingo ciklas“, „Demingo – Šuharto ciklas“, kuris ir yra ISO 9001:2008 ir ISO/IEC 27001:2005 pagrindas.

- Abu standartai turi panašų reikalavimų turinį, kas atspindi standarto ISO 27001 A priede. Standartai ISO 27001 ir ISO 9001 turi panašią kokybės sistemos reguliavimo ir informacinės saugos sistemos struktūrą. Tačiau galima padaryti išvadą, kad ISO 27001 yra plačiau naudojamas (Raikova, 2013).

1.2.2. Valdymo standartų integravimas

Kokybės valdymas ir informacinis saugumas – visai skirtingos sritys, tačiau praktikoje jos yra tampriai susijusios ir sudaro vieną bendrą sritį. Klientų poreikių tenkinimas, kokybės atžvilgiu, vis labiau priklauso nuo informacinių technologijų prieinamumo ir nuo duomenų saugos. Šio poreikio tenkinimui ir sukurtas ISO 27001 standartas (Markov, Cirlov, 2012). Čekmariov (2007) analizuojant situaciją ir pažymi, kad ISO 9001 tiksliai atspindi organizacijos korporatyvinius tikslus padedant suteikti informacinės saugos valdymą. Taigi galima išvada, kad kompleksinio požiūrio dėka ISO 27001 gali būti efektyviai integruotas į egzistuojančias kokybės valdymo sistemas arba vykdomas kartu su jomis.

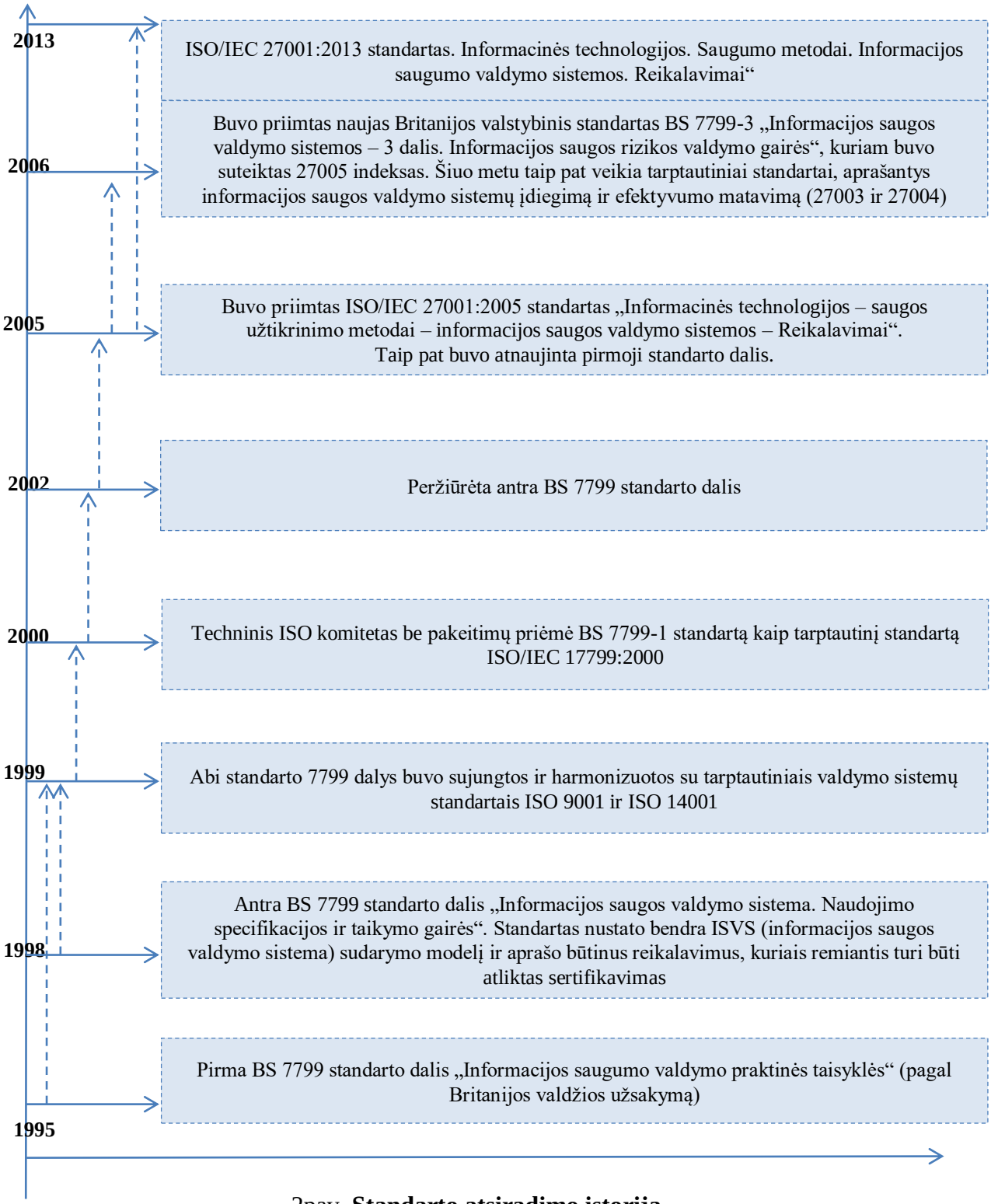
Priklausomai nuo rinkos ir teisinių reikalavimų, vis daugiau organizacijų yra priverstos garantuoti informacinę saugą. Ryšium su tuo, valdymo sistemos integravimas suteikia realias galimybes. Kompleksinis požiūris taip pat domina organizacijas, kurios iki šiol neturėjo jokių valdymo sistemų. ISO standartai: ISO 9001 – kokybės, ISO 14000 – aplinkosaugos, ISO 27001 - informacinės saugos ir ISO 20000 – IT paslaugų valdymas turi analogišką struktūrą ir procesinį požiūrį. Tai suteikia sinergijos efektą, kuris atsiperka: praktikoje integruota valdymo sistema sutaupo 20 – 30 procentų naudojimo išlaidų (Dmitriev, 2014).

Informacinės saugos ir kokybės valdymo standartų tikslinė kryptis – nuolatinis tobulinimas laikantis PDCA modelio. Be to jie turi panašią struktūrą, abejose standartuose apibrėžtos procesinio požiūrio, veiklos sferos, sistemos ir dokumentavimo reikalavimų, administracinės atsakomybės sąvokos. Abejose atvejuose struktūrą užbaigia vidinis auditas, valdymo organų analizė ir sistemos tobulinimas (Grigorjeva, Meškov, 2007)

Apibendrinant galima teigti, kad skirtumai tarp standartų papildo vienas kitą, kas lemia veiklos sėkmės augimą. Pavyzdžiui ISO 9001 reikalauja korporatyvinių tikslų griežto nustatymo, orientacijos į klientą ir uždavinių įvykdymo ir tikslų siekimo matavimo sistemos kūrimo. Šie trys aspektai nėra ISO 27001 interesų pagrindas. Tačiau šis standartas suteikia pirminę rizikos valdymo reikšmę siekiant veiklos tęstinumo ir suteikia išsamią pagalbą realizuojant informacinės saugos valdymo sistemą.

1.3. Standarto ISO/IEC 27001:2013 atsiradimo istorija

Praeito amžiaus pirmoje 90 – ųjų metų pusėje Britanijos standartų institutas (British Standarts Institution, BSI) kartu su keliomis stambiomis komercinėmis organizacijomis (Shell Uk, National Westminster Group, Unilever, British Communications, British Computer Society, Assotiation Of British Insurers, Marks&Spencer, Logica ir kt.) sukūrė BS 7799 standartą, kurį sudarė informacinės saugos normos ir taisyklės, 1995 metais šiam standartui buvo suteiktas valstybinio standarto statusas. Taigi ISO/IEC 27001:2013 formavimo pradžia galima laikyti 1995 metus. 2 paveiksle pateikta ISO/IEC 27001:2013 standarto laiko formavimo eiga (Rajkova, 2013).



2pav. **Standarto atsiradimo istorija**

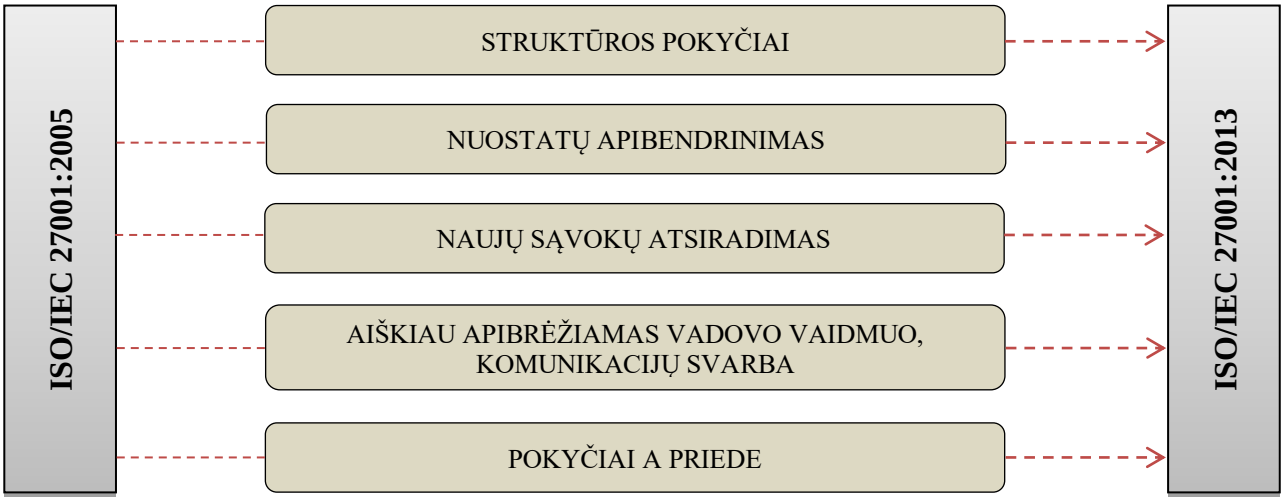
(šaltinis: sukurta autorės, remiantis Šahalov, Dorofeev, 2013)

ISO/IEC 27001:2013 skiriasi nuo praeitų redakcijų pagal turinį ir formą. Nuo praeito amžiaus 80 – ų metų atsirado eilė standartų, skirtų valdymo sistemoms (kokybės valdymas, energetinis valdymas, maisto saugos valdymas ir t.t.). Dažnai šiuolaikinės organizacijos turi

būtinumą diegti valdymo standartus ir užtikrinti efektyvią integruotos valdymo sistemos naudojimą, laikantis skirtingų standartų.

Kadangi standartai buvo kuriami skirtingu laiku ir kūrimui buvo naudojami skirtingų sferų specialistai – atsirado daug neapibrėžtumų, trukdančių vieningos integruotos valdymo sistemos kūrimui. Siekiant unifikuoti esamus standartus buvo priimtas SL priedas (Annex SL) pirmoje direktyvų ISO dalyje, pagal kurį turi būti kuriami nauji ir tobulinami esami valdymo standartai (Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013; interaktyvus)

Siekiant ISO 27001 standartą pritaikyti vieningam valdymo sistemų standartui buvo atlikta eilė pokyčių. Autoriai skiria penkias pokyčių grupes (žr.3 pav.)



3pav. **ISO/IEC 27001:2005 ir ISO/IEC 27001: 2013 skirtumai**

(šaltinis, sukurta autorės remiantis Movingfrom ISO/IEC 27001:2005 to ISO/IEC 27001:2013)

1.3.1. Struktūros pokyčiai

BSI (British Standarts Institution) dokumente „Perėjimas nuo ISO 27001:2005 prie ISO 27001:2013“ plačiai aprašytas 2005 ir 2013 metų standartų palyginimas (struktūra pakeista laikantis SL priedo reikalavimų). Lyginamosios analizės duomenimis, standarto esmė nepasikeitė. Bet būtina atkreipti dėmesį į vieną svarbų aspektą, susijusi su nauja standarto redakcija. ISO 27001:2005 buvo pateiktas Demingo modelis (PDCA arba Plan – Do – Check – Act), 2013 metų standarte Demingo modelio aiškaus konkretaus išdėstymo nėra, tačiau ISO 27001:2013 standarto turinyje galima matyti dalis, einančias viena po kitos (Comparing ISO 27001:2005 to ISO 27001:2013, interaktyvus):

- Planavimas (Plan);
- Funkcionavimas (Operation);
- Rezultatyvumo įvertinimas (Performance evaluation);

- Gerinimas (Improvement) (Comparing ISO 27001:2005 to ISO 27001:2013, interaktyvus).

Apibendrintai galima teigti, kad Demingo modelis standarte išliko ir negalima kalbėti apie modelio aktualumo praradimą. Verta pažymėti, kad šis modelis yra naudingas valdant bet kurią veiklą: pradžioje nuosekliai apgalvojama ką reikia daryti (Plan), po to darom (Do), tikriname ar gauti rezultatai atitinka planuotus (Check), koreguojame, geriname (Act).

1.3.2. Nuostatų apibendrinimas ir naujų sąvokų atsiradimas

ISO/IEC 27001:2005 procesas aprašytas labai plačiai, buvo įtraukti tokie žingsniai kaip aktyvų ir jų savininkų identifikacija, pažeidžiamumas (Dorofeev, 2014)

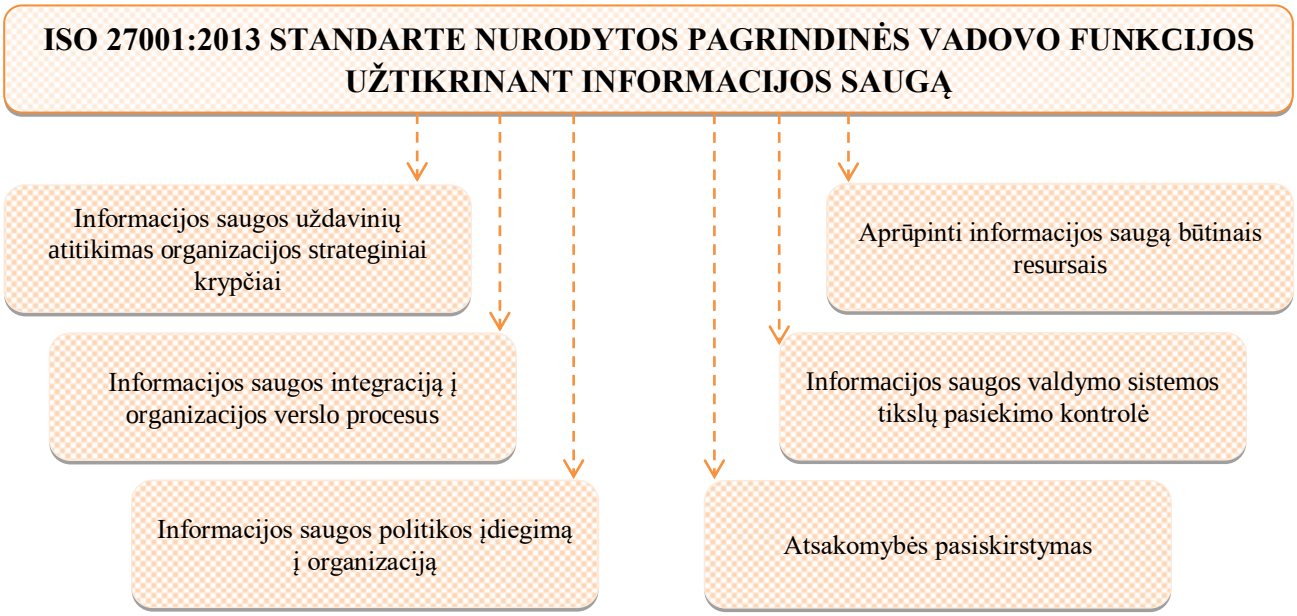
- Naujoje ISO/IEC 27001:2013 versijoje palikti tik pagrindiniai etapai. Dabar rizikos vertinimo proceso reikalavimai atitinka tarptautinį ISO 31000 standartą (Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013, interaktyvus).
- Naujoje versijoje nėra žodžio „asset“ turtas, tačiau negalima įvertinti rizikos nežinant kokiam turtui ji gresia. Tačiau standarte yra frazė: „organizacija turėtų nustatyti ir taikyti informacijos saugumo valdymo sistemos procesus taip, kad identifikuotų informacijos saugumo rizikas: taikydama informacijos saugumo rizikos vertinimo procesą su konfidencialumu, vientisumu ir prieinamumu susijusioms rizikoms identifikuoti informacijos saugumo valdymo sistemos taikymo srityje“ (6.1.2.).(LST ISO/IEC 27001/AC1) Nustatant termino informacija esmę, galima pasinaudoti ISO 27000:2014 standartu, kuriame apibrėžiami terminai, taikomi eilėje standartų. Standarto 27000:2014 punkte 3.2.2. pažymėta, kad informacija – tai turtas. Ši sąvoka neapribojama vien skirtingų formų duomenimis, į ją įeina duomenų perdavimo technologijos. Naujoje standarto versijoje nėra frazės su reikalavimu, neleisti, kad auditoriai tikrintų savo darbą, tačiau ISO 27001:2013 9.2 skyriuje fiksuojami auditorių pasirinkimo ir audito atlikimo reikalavimai, kur pažymėta: organizacija turėtų: pasirinkti auditorius ir vykdyti auditą, užtikrindama auditavimo objektyvumą ir nešališkumą“, taigi panaikintas tik perteklinis tekstas (Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013, interaktyvus).
- Naujoje redakcijoje pateikti nauji terminai ir koncepcijos: „organizacijos kontekstas“.
- Dabar reikalavimai informacijos saugos valdymo sistemų ribos pagrindimui tapo griežtesni, organizacija turi griežtai apibrėžti suinteresuotas šalis ir jų reikalavimus.
- Nauja standarto versija reikalauja, kad siekiant nustatyti informacijos saugos riziką, turi būti identifikuoti rizikos savininkai. ISO žodyno duomenimis, rizikos savininkas – tai

asmuo arba organizacija, kuri atsako už rizikos valdymą ir tam turi būtinas kompetencijas.

- Standarte atsirado nauja sąvoka „Information Sequrity Objectives“ (informacijos saugos uždaviniai). ISO 27001:2013 reikalauja griežto uždavinių planavimo:
    - kas turi būti padaryta;
    - kokių resursų reikia
    - kas atsakingas;
    - terminai;
    - kaip bus vertinami uždavinių įvykdymo rezultatai (Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013, interaktyvus).

1.3.3. Vadovų vaidmuo

Bet kuri valdymo sistema turi būti vertinama bendrovės vadovybės, kadangi sudaryti procesai leidžia sumažinti priklausomybę nuo tam tikrų specialistų poreikio, padidinti organizacijos valdymo lankstumą, aprūpinti sąmoningą bendrovės veiklos planavimą. Kartais susiduriama su situacija, kai organizacijai labiau rūpi sertifikato gavimas, o ne pati valdymo sistema (Rajkova, Šahalov, 2013).



4pav. **Vadovo funkcijos, užtikrinant informacijos saugą (ISO 27001:2013)**

(šaltinis: sudaryta autorės remiantis LST/IEC 27001/AC1)

Jeigu valdymo sistema griežtai neapibrėžia vadovo funkcijų ir atsakomybių, ji bus neveiksminga. Naujos ISO 27001 standarto versijos kūrėjai įvertino šį faktorių ir dabar standartą sudaro išsamus aprašymas ką turi įvykdyti valdymo organai, kad užtikrinti

informacijos saugos valdymo sistemos rezultatyvų funkcionavimą. Vadovybė turi užtikrinti (žr. 4 pav.) (Rajkova, Šahalov, 2013).

1.3.4. Komunikacija informacijos saugos srityje

Labai svarbu, kad kiekvienas įmonės darbuotojas gerai suvoktų, kas yra informacijos sauga, ir kas iš jo reikalaujama skirtinguose situacijose, o tam labai tinka propagandos metodai, kurie dabar moksliškai vadinami komunikacija. Naujoje standarto versijoje atsirado naujas skyrius 7.4. skyrius, skirtas šiam klausimui. ISO 27001: 2013 reikalauja vidinės ir išorinės komunikacijos informacijos saugos klausimais planavimo: įmonė turi nuspręsti ką, kas, kam ir kada komunikuos organizacijoje ir už jos ribų (Comparing ISO 27001:2005 to ISO 27001:2013, interaktyvus).

Pokyčiai standarto A priede

5pav. **ISO 27001:2013 A priedo struktūra**

(šaltinis: sudaryta autorės remiantis LST/IEC 27001/AC1)

ISO 27001:2013 atsirado pokyčiai ir A priede kaip jau anksčiau buvo minėta, kontrolė – tai informacijos saugos rizikos minimizavimas. Iš esmės ISO 27001 yra standartas, kuris aprašo rizikos vertinimo kontrolės mechanizmo pasirinkimą. Standartas turi A priedą, kuriame išvardintos kontrolės rūšys, kurių pagrindu formuojama sistema. Naujoje standarto versijoje pateiktos 114 kontrolės rūšių, suskirstytų į 14 domenų. (Dorofeev, Markov, 2014). Ankstesnėje redakcijoje kontrolės buvo skaidomos į 11 domenų. Naujas standartas papildytas 20 domenų, 11 domenų buvo ištrinti, kai kuriuose pagerintos formuluotės.

BSI (Britanijos standartizacijos institucija) išleido 2017 m. Balandžio mėn. Standartą BS EN ISO / IEC 27001: 2017. Standartas yra ankstesnio standarto BS ISO / IEC 27001: 2013 taisymas. Pagrindinis pasikeitimas, kuris atsirado naujoje standarto versijoje yra „techniniai pataisymai“, Būtent šis punktas kelia nerimą standartą įdiegusioms įmonėms. Techninė pataisa yra leidinys, kurį įdiegė standartizacijos institucijos, siekdamos iš dalies keisti esamą standartą, ištaisyti nedidelius techninius trūkumus, įdiegti patobulinimus arba įtraukti praplėsti standarto įdiegimo ribojimus. Tokie pakeitimai taikomi ir dabar naudojamoms standarto versijoms, t.y. bendrovėms, kurios naudoja senesnes ISO 27001 versijas.

ISO 27001 techniniai klaidų taisymai apima tris pagrindines sritis (tais atvejais, kai klaidų taisymas yra bendrinio pobūdžio, trim skirtingais laikotarpiais):

1. ISO (tarptautinės standartizacijos organizacijos) paskelbti 2014;
2. ISO (tarptautinės standartizacijos organizacijos) 2015 m. paskelbti gruodžio mėnesį;
3. Tarptautinė standartizacijos organizacijos paskelbti 2017 m. Kovo mėn.

Šie klaidų taisymai apima šiuos klausimus:

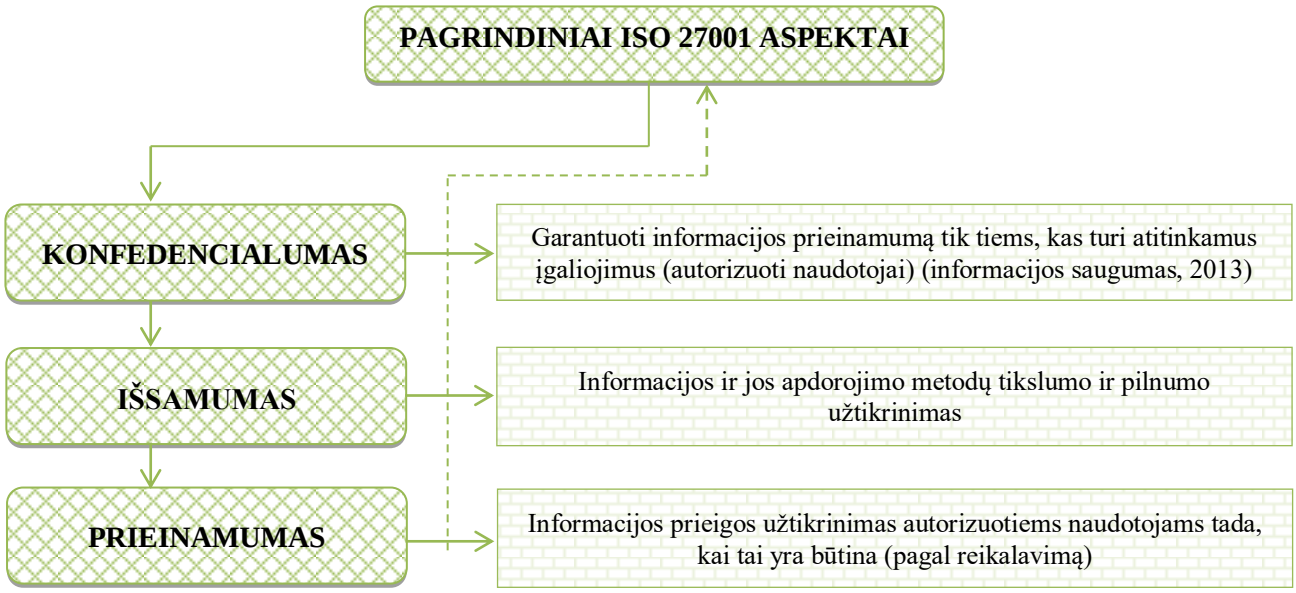
1. 2014 m. Rugsėjo mėn. Techninių klaidų taisymas susijęs su punktu A.8.1.1 ("Turto inventorizacija"), pakeičiant kontrolės objekto tekstą iš:"Turi būti identifikuojami su informacijos ir informacijos apdorojimo įrenginiais susiję turtai ir parengiamas ir prižiūrimas šio turto aprašas" į "Turi būti nustatyta informacija ir kitas turtas, susijęs su informacijos ir informacijos apdorojimo įrenginiais, ir parengiamas ir prižiūrimas šio turto aprašas." *Šiuo pakeitimu aiškiai nurodoma, kad pati informacija taip pat turi būti laikoma turtu, kuris turi būti įtrauktas į inventorių.*
2. 2015 m. Gruodžio mėn. techninių klaidų taisymo koregavimai buvo taikomi 6.1.3 punktui ("Informacijos saugumo rizikos vertinimas"), konkrečiai D punktui. Šiuo atveju tai tik kosmetinis koregavimas, skaidant jau esamą turinį į papunkčius nuo pagrindinės pastraipos į atskirus papunkčius. Šis koregavimas aiškiau nustato, kad SRA (saugumo rizikos vertinimas) turi būti vertinamas nors keturiais elementais.

a. reikiamas kontrolės priemones, skirtas įdiegti informacijos saugumo rizikos vertinimą, atsižvelgiant ne tik į A priede pateiktas, bet ir atsižvelgiant į organizacijos nustatytus reikalavimus, taip pat kitus iš bet kokio šaltinio nurodytus patikrinimus (pvz., NIST SP 800 dokumentų serijų kontrolę);
b. pagrindimas, kaip įtraukti šiuos patikrinimus;
c. kontrolės būsena (pvz., Įdiegta ar ne);
d. bet kurio A priedo kontrolės atmetimo pagrindimas;
e. Paskutinė pataisa nuo 2017 m. Kovo yra susijusi su britų standarto versija (BS ISO / IEC 27001: 2013) – esminių pakeitimų ten nėra. Pakeitimai apima standarto pernumeravimą BS EN ISO / IEC 27001: 2017, kad būtų atspindėtas jos statusas kaip dabar pripažintas "Europos standartas" (žymimas raidėmis "EN") Pripažinimą "Europos standartu" patvirtino CEN / CENELEC (Europos standartizacijos komitetas - CEN ir Europos elektrotechnikos standartizacijos komitetas - CENELEC), Europos Sąjungos pripažintos Europos standartizacijos institucijos.

Apibendrinant galima teigti, kad skyriuje apžvelgti ISO 27001 pokyčiai ir nurodo tas organizacijos sritis informacijos saugos valdymo sistemoje, kurios reikalauja išskirtinio dėmesio pereinant prie naujesnės versijos arba diegiant standartą organizacijoje. Iš vienos pusės standartas tapo griežtesnis ir įgijo daugiau konkretumo (reikalavimai vadovams, informacijos saugos uždaviniai), iš kitos pusės, jame buvo panaikintos kai kurios detalės (niuansai, rizikos vertinimas, vidinis auditas), kurie taikomi praktikoje. Organizacijoms, kurios rimtai nagrinėja informacijos saugos valdymo sistemos įdiegimo procesą, nekils jokių problemų derinant esamą sistema su naujais reikalavimais. Nauja standarto versija reikalauja aiškiai ir struktūrizuotai aprašyti informacijos saugos valdymo sistemos sritį (International Organization for Standardization).

1.4. Pagrindiniai ISO/IEC 27001 serijos aspektai

Šiuolaikinis verslas negali egzistuoti be informacinių technologijų. Žinoma, kad apie 70 proc. pasaulinio nacionalinio produkto tuo ar anuo atžvilgiu priklauso nuo informacijos, saugomos informaciniuose sistemose. Platus kompiuterių naudojimas sukūrė ne tik žinomus visiems darbo privalumus ir patogumus, bet ir eilę problemų, svarbiausia iš jų yra informacinės saugos problema (Markov, Cirlov, 2007).



6 pav. **Pagrindiniai ISO 27001 aspektai**

(šaltinis: sudaryta autorės, remiantis Dmitriev, 2014)

Bendrovių vadovai turi suvokti informacinės saugos svarbą, išmokti prognozuoti tendencijas šioje srityje ir jas valdyti. Šiam tikslui pasiekti gali padėti informacinės saugos valdymo sistemos įdiegimas, kuris pagal savo struktūrą turi vystymo potencialą, valdymo skaidrumą, lankstumą pokyčiams. Kartu su kompiuterių ir kompiuterinių tinklu valdymo elementais ISO 27001 standartas skiria didelį dėmesį saugos politikos formavimui, darbui su personalu, nenutrūkstamo gamybos proceso aprūpinimui, normatyviniams reikalavimams (Kabay, 2002).

ISO 27001 standartas informacijos saugą traktuoja kaip „informacijos konfidencialumo, bendrumo ir prieinamumo išsaugojimą; be to gali būti apimtos ir kitos savybės, tokios kaip: autentiškumas, draudimas atsisakyti autorystės, patikimumas“ (Dmitriev, 2014).Standartas ISO 27001 harmonizuoja su kokybės valdymo sistemomis ISO 9001:2000 ir ISO 14001:2004 ir remiasi jų pagrindiniais principais ir procesiniu požiūriu.Be to, būtinos ISO 9001 standarto procedūros reikalaujamos ir ISO 27001 standartams. ISO 27001 dokumentavimo struktūra yra analogiška ISO 9001 reikalavimų struktūrai. Didžiausia dalis dokumentacijos, reikalaujamos

pagal ISO 27001, jau galėjo būti parengta ir naudojama ISO 9001 sistemoje. Taigi, jeigu organizacija jau yra įdiegusi valdymo sistemą, pvz. ISO 9001 arba ISO 14001, tai patartina vykdyti ISO 27001 standarto reikalavimus jau įdiegtų sistemų ribose (Rajkova, Šahalov, 2013).

ISO 27001 turi eilę privalumų:

- Galimybė nustatyti rizikas ir priimti veiksmus jų optimizavimui arba šalinimui.
- Adaptavimo lankstumas bet kuriai veiklos sferai;
- Klientų ir suinteresuotų asmenų pasitikėjimas, jų duomenų saugumo užtikrinimo dėka;
- Atitikimas standartams garantuoja privilegijuoto tiekėjo statusą;
- Bet kokių lūkesčių patenkinimas standarto reikalavimams atitikimo dėka (Inter Cert, 2017).

Informacijos saugumo esmė yra rizikos valdymas. Bankams ir kitų sferų organizacijoms šis terminas yra gerai pažįstamas. Rizikos valdymo sąvoką sudaro rizikų nustatymas, įvertinimas, veiksmai rizikos minimizavimui arba šalinimui. Galima teigti, kad rizika – tai incidento tikimybės ir jo pasekmių derinys. Pavyzdžiui organizacijos kompiuterinė sistema gali būti infekuota kompiuteriniu virusu, šio įvykio pasekmės gali turėti įtakos verslo aplinkai ir sąlygoti finansinius sunkumus. Todėl kompiuterinio viruso ataka yra susijusi su didele rizika ir organizacinė, programinė ir techninė apsauga yra būtina (Dmitriev, 2013).

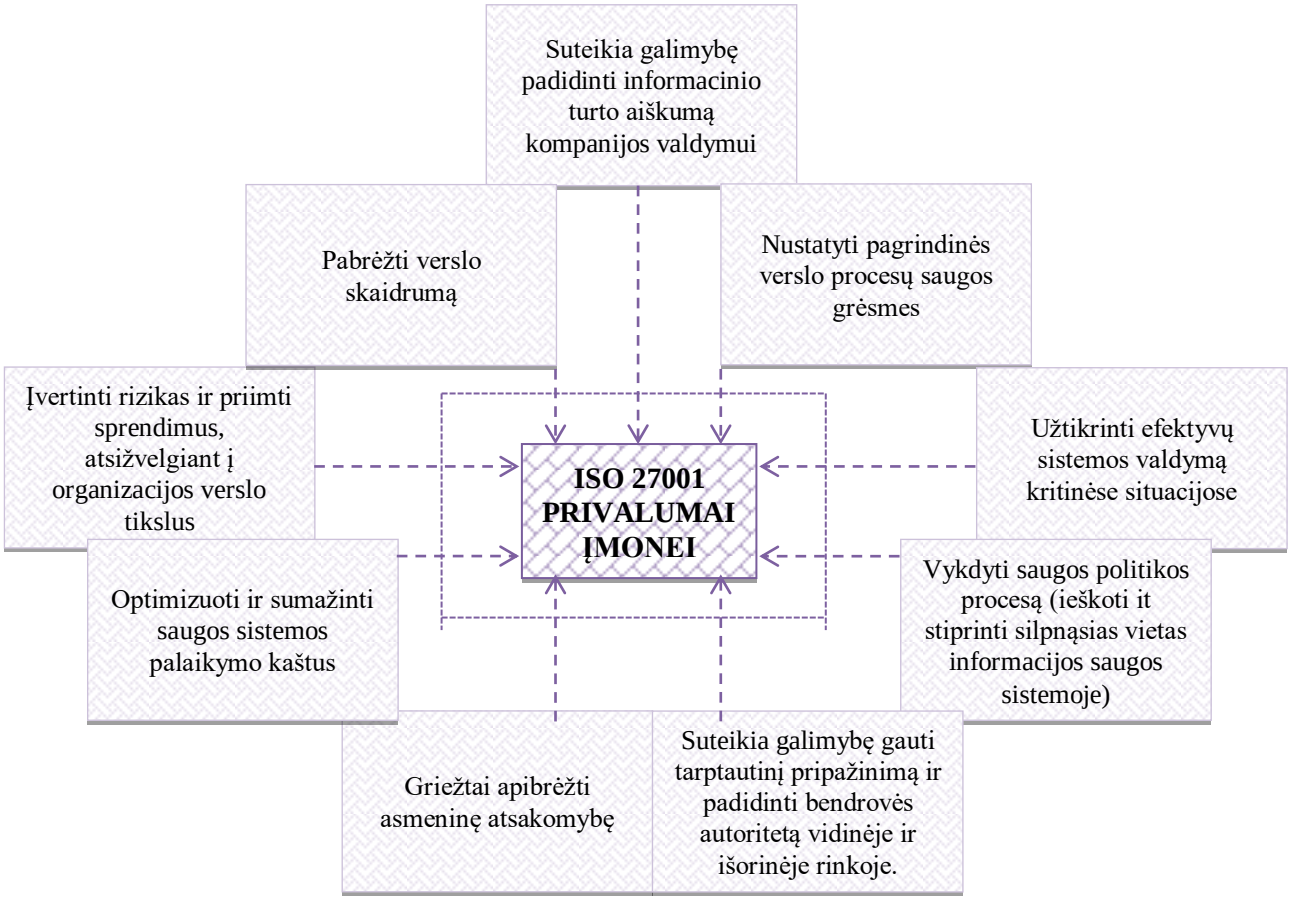
ISO/IEC 27001 integruoja du metodus – PDCA ir rizikos valdymą. Tai suteikia galimybę sudaryti optimaliai rezultatyvią valdymo sistemą. Rizikos valdymo metodai yra integruoti į PDCA ciklą, siekiant juos naudoti kuriant, tikrinant, palaikant ir tobulinant informacijos saugos valdymo sistemą. ISO/IEC 27001 pasiūlo darbo struktūrą naudojant geriausią tarptautinę praktika informacijos saugos valdymo sistemų srityje, t.y. siekiant suvokti kur tam tikros informacijos saugos priemonės gali būti taikomos. Be to, organizacijų vadovai turi pripažinti, kad informacijos sauga bus rezultatyvi ir efektyvi su sąlyga, kad visi struktūriniai padaliniai ir visi darbuotojai bus įtraukti į informacijos saugos užtikrinimo procesą. Šis požiūris, remiasi bendra organizacine rizika ir atspindi ISO/IEC 27002:2005 standarte „Informacinės technologijos – saugumo užtikrinimo metodai – informacijos saugos valdymo praktinės taisyklės. Naujausi OECD (ekonominio bendradarbiavimo ir vystymo organizacija) reikalauja „saugos kultūros“ kūrimo organizacijos viduje (Douglas, Landoll, 2011).

ISO/IEC 27001 siūlo priemones informacijos saugumo valdymo sistemos rezultatyviam įdiegimui, atitinkančiam organizacijos tikslus ir verslo poreikiams. Informacijos saugos valdymo sistemos esmė turi atitikti egzistuojančias ir potencialias saugumo rizikas, techninius

ir technologinius reikalavimus, informacinių sistemų ir verslo procesų galimybes, teisines normas, normatyvinius ir kontraktinius reikalavimus (Cosutic, 2017).

ISO/IEC 27001 standartas yra lankstus, jį galima naudoti informacijos saugos valdymo sistemos įdiegimui į egzistuojančias valdymo sistemas, o taip pat kokybės valdymo sistemas (Dmitriev, 2014). PDCA ciklas integruojamas į bet kurias egzistuojančias ISO 27001 rizikos valdymo metodikas ISO 27001. Informacijos saugos valdymo metodai yra plačiai taikomi teikiant valstybines paslaugas, realizuojant elektroninės valdžios programas (Dmitriev, 2014).

Naudojant ISO/IEC 27001, kaip ir taikant ISO 9001, organizacija įkurti, įdiegti ir sertifikuoti savo valdymo sistemą, atitinkantį tarptautinį standartą. Sertifikavimo vertė verslui taip pat atspindi griežtai apibrėžtas standarto eiliškumas, kuriame aprašyti saugos valdymo kūrimo procesai, metodologijos, instrumentai ir šablonai, kuriuos galima naudoti organizacijos praktikoje ne vieną kartą – saugos planavimas, įdiegimas, funkcionavimas, monitoringas, stebėjimas, atskaitomybės paruošimas (30th Conference of Directors of EU Paying Agencies. ISO 27001:2005 & ISO 9001:2008 Benefit for the organization, interaktyvus).



7pav. **ISO 27001 standarto taikymo privalumai įmonei**

(šaltinis: sudaryta autorės remiantis 30th Conference of Directors of EU Paying Agencies, [interaktyvus])

Tarptautinių standartų įdiegimas sąlygoja technologinius, ekonominius ir socialinius privalumus. Jie padeda subalansuoti prekių ir paslaugų technines charakteristikas, didina verslo sričių efektyvumą ir padeda šalinti kliūtis vykdant tarptautinę prekybą. Tarptautinių standartų laikymasis padeda įtikinti vartotoją, kad jiems siūlomi patikimi, efektyvūs, nekenksmingi aplinkai produktai (Grigorjeva, Meškov, 2006)

Stebėjimo ir atskaitomybės priemonės, remiasi srities standartais, tokiais kaip ISO, palengvina audito atlikimą, kas lemia išlaidų audito atlikimui mažinimą ir audito sėkmingo atlikimo tikimybės didinimą. Standarto ISO 27001 teikiamos galimybės įmonėms (30th Conference of Directorsof EU Paying Agencies. ISO 27001:2005 & ISO 9001:2008 Benefits for the organization, interaktyvus).

Apibendrinant galima teigti, kad ISO 27001 yra organizacijos praktinis vadovas, kuris padeda suformuoti saugos reikalavimus reikiamo saugos lygio aprūpinimui ir konkrečių saugos tikslų vykdymui. Standartas yra tam tikras įrodymas, kad korporatyvinio valdymo programos remiasi geriausia, tarptautine praktika. Dauguma griežtai reguliuojamų sferų, tokių kaip finansai arba internetinės paslaugos, tiekėjo pasirinkimas gali būti ribojamas tomis organizacijomis, kurios jau yra sertifikuotos pagal ISO 27001.

Procesinio požiūrio dėka galimas organizacijoje vykdomų procesų optimizavimas, kas lemia naudojamų resursų minimizavimą. Be to informacinės saugos valdymo sistema naudoja PDCA modelį, kas leidžia reguliariai tikrinti visos sistemos būseną, atlikti analizę ir tobulinti valdymo sistemą.

ISO 27001 sertifikavimas atveria organizacijai platų galimybių spektrą: išėjimą į tarptautines rinkas, naujus partnerystės ryšius, didelis klientų skaičius, naujos sutartys.Nepriklausomai nuo procesų, naujų technologijų pokyčių – informacinės saugos valdymo sistemos pagrindas yra veiklus. ISVS lengvai pritaikoma naujovėms, modernizuojant esamas ar diegiant naujas atsakomąsias priemones.

1.5. ISO/IEC 27001:2013 naudojimo teorinis modelis

Baigiamajame darbe aptariamos Dmitriev (2014); Cirlov (2008), Markov, Cirlov (2007), Šahalov (2012) nuomones dėl ISO 27001:2013 diegimo organizacijoje ypatumų vieningame teoriniame modelyje, kuris taps tyrimo instrumento pagrindu ir tam tikra logiška tyrimo atlikimo schema (žr. 8 pav.)

ISO/IEC 27001:2013 naudojimo ypatumai skirtingų autorių skaidomi į skirtingą naudojimo etapų skaičių.

1. Standarto naudojimo auditas;
2. Informacijos rizikos įvertinimas ir analizė;

3. Rizikų valdymas;
4. Pakartotinas auditas
5. Periodinis sertifikavimas (Markov, Cirlov, 2007) ;

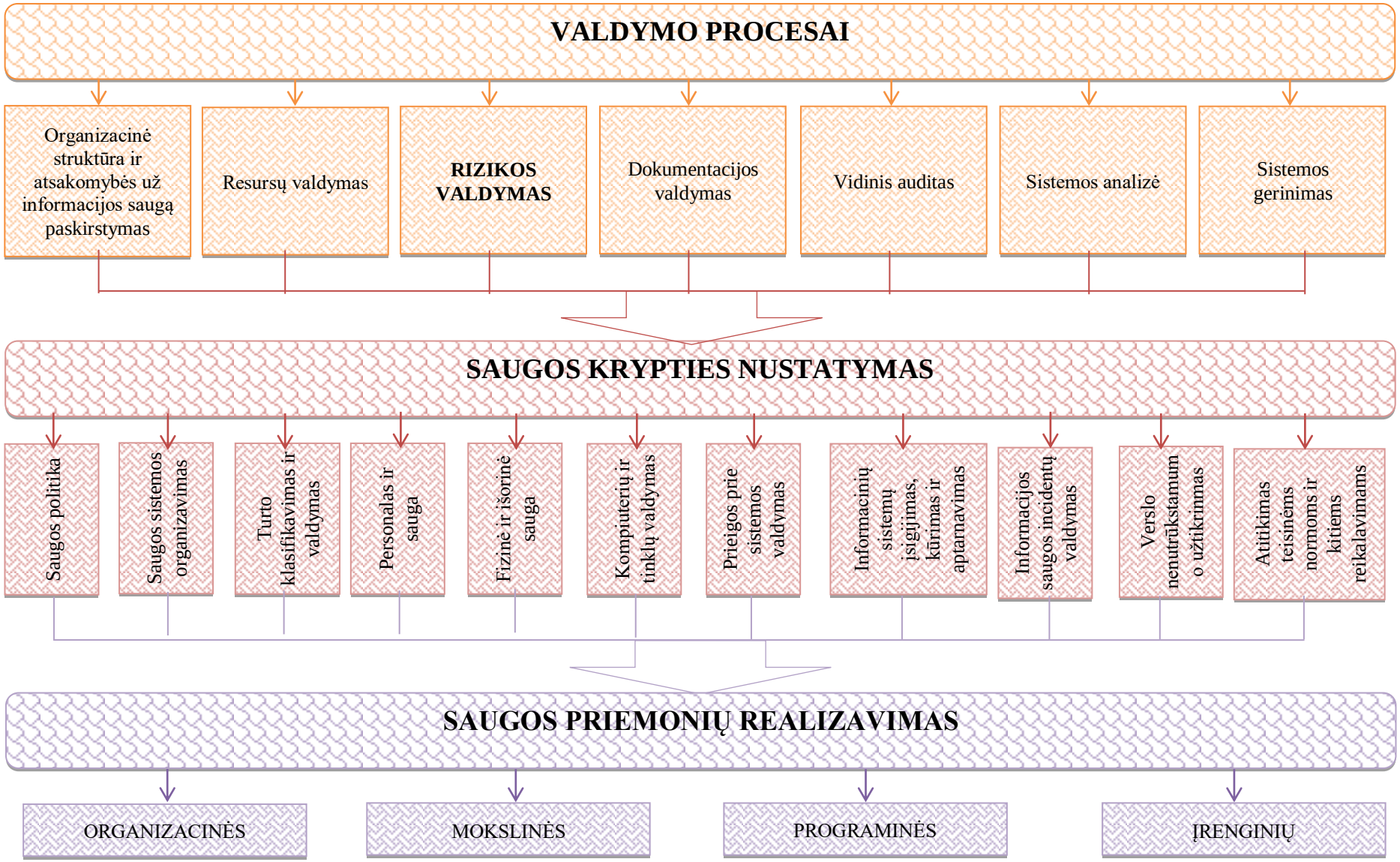
Arba į 10 etapų:

1. Planavimas ir pasiruošimas;
2. Atitikimo ISO 27001 tikrinimas;
3. Dokumentų analizė;
4. Informacijos saugos analizė;
5. Ateities planų kūrimas ir realizacija;
6. Norminių ir organizacinių dokumentų paruošimas;
7. Informacijos saugos realizavimas ir efektyvumo vertinimas;
8. Personalo apmokymas;
9. Analizės rezultatų sisteminimas;
10. Rekomendacijų informacijos saugos gerinimui pasiūlymas (Šahalov, 2012).

Šahalov (2012) ir Markov, Cirlov (2007) nuomonės buvo pasirinktos ryšium su tuo, kad jos „tarsi“ apjungia kitų autorių nuomones ir pateikia susitemintą, išsamią, informaciją apie standarto naudojimo etapus.

Remiantis 8 pav. pateiktu modeliu bus sudarytas tyrimo instrumentas – interviu scenarijus. Paveikslas buvo suformuotas, remiantis teorinėmis prielaidomis, kurios buvo aptartos teorinėje baigiamojo darbo dalyje:

- Valdymo procesai buvo išskirti, remiantis Dmitriev (2014); Cirlov (2008), Markov, Cirlov (2007), Šahalov (2012) atliktais tyrimais.
- Jeigu yra informacinės saugos valdymo procesai, jiems turi būti taikomos saugos užtikrinimo kryptys, schemoje jos pateiktos remiantis ISO 27001: 2013 standarte aprašytomis prielaidomis.
- Informacijos sauga realizuojama taikant saugos priemones: saugos priemonės grupės buvo išvardintos, remiantis ISO 27001: 2013 medžiaga ir autorių Dmitriev (2014); Cirlov (2008), Markov, Cirlov (2007), Šahalov (2012) tyrimų rezultatais.



8pav. **ISO 27001:2013 teorinis naudojimo modelis**

(šaltinis: sudaryta autorės, remiantis Dmitriev (2014); Cirlov (2008), Markov, Cirlov (2007), Šahalov (2012); ISO 27001: 2013

2. ISO 27001:2013 NAUDOJIMO TYRIMO METODOLOGIJA

Tyrimo tikslas: identifikuoti ISO 27001:2013 naudojimo ypatumus Lietuvoje esančiose organizacijose.

Tyrimo populiacija: Organizacijos įdiegusios ISO 27001:2013

Tyrimo laikas: 2017 m. rugsėjo mėnesis – 2018 metų balandžio mėnuo

Tyrimo vieta: Tyrimo objekto būstinės.

Tyrimo rūšis: ekspertinis, pusiau struktūrinis interviu.

Tyrimo eiga: Tyrimas vyko be esminių sunkumų, tačiau buvo labai sunku surasti respondentus, kurie gali suteikti reikiamą informaciją apie ISO 27001 serijos standartą, todėl tyrime dalyvavo tik 4 respondentai, tačiau buvo siekta gauti kuo išsamesnę informaciją, todėl tyrimas gavosi pakankamai išsamus.

Priežastys, dėl kurių pasirinktas kokybinis tyrimas:

Apžvelgus interviu metodo ypatybes, teigtina, kad tai ilgą laiką taikomas ir itin plačiai paplitęs informacijos gavimo būdas.

- Interviu dalyviai visada bendrauja pagal „klausimo-atsakymo“ schemą.
- Tam tikro interviu tipo pasirinkimas priklauso nuo mokslinių tyrimų projekto tikslų ir uždavinių. Empirinės sociologijos praktikoje egzistuoja daug įvairių interviu metodų, kurie priskiriami dešimčiai skirtingų klasifikacijų. S. Hackers ir C. Warren išskiria tris interviu tipus, besiskiriančius interviuotojo ir respondento pažinimo lygiu ir klasifikacija. J. Adamsas ir J. Schwaneweldt išskiria istoriškai suformuotą ir literatūroje naudojamą interviu tipų klasifikaciją - orientuotą, neremiamąjį, klinikinį ir telefoninį (Veselkova, 1995). Be formalizavimo laipsnio, yra ir kitų interviu klasifikavimo būdų. Tarp tokių pagrindinių klasifikacijos tipų yra šie: pagal tikslinę paskirtį, respondentų rūšį, apklausiamų respondentų skaičių, procedūrą, sociologo ir respondento bendravimo formą, interviu vietą, tyrimo tikslą, atsakymų registravimo būdą (Gricanos, 2003).
- Kuo mažesnis yra interviu formalizavimo laipsnis, tuo pokalbio dalyvio laisvės laipsnis didesnis, o mokslininkas gauna galimybę tiksliau suprasti asmens motyvus ir, atitinkamai, veiksmus, todėl tyrimui atlikti buvo pasirinktas ekspertinis, giluminis, pusiau struktūrinis interviu.

1. ISO 27001:2013 įdiegusių įmonių nėra daug. Tikslaus skaičiaus rasti nepavyko. Jis nėra viešai skelbiamas.
2. Vykdant interviu tyrimą galima laviruoti, pakrypti pokalbį reikiamą linkme, įterpti interviu scenarijuje nepateiktų klausimų, stebėti respondento reakciją į užduotą klausimą;

Respondentų skaičius: respondentų skaičius priklauso nuo atsakymų turinio, interviu tyrimas bus vykdomas tol, kol atsakymai į interviu klausimus nepradės kartotis;

Tyrimo duomenų fiksavimas: interviu įrašyti raštu bei diktafonu, pažymint visus respondentų aspektus.

Interviu rezultatų pateikimas darbe: interviu transkripcija.

Interviu etapai ir gautų duomenų apdorojimo būdai:

1. Duomenų rinkimas;
2. Interviu transkripcijos sudarymas;
3. Duomenų grupavimas į tris dalis: valdymo procesai; saugos krypties nustatymas; saugos priemonių realizavimas;
4. Duomenų lyginamoji analizė;
5. Išvadų pateikimas, remiantis logiškumo principu.

Interviu instrumentas – klausimynas. Klausimyną sudaro 4 dalys:

1. Bendrieji klausimai;
2. Valdymo procesai;
3. Saugos krypties nustatymas;
4. Saugos priemonių realizavimas (žr. 2 lentelę)

2lentelė. **Tyrimo instrumento pagrindimas**
(šaltinis: sudaryta autorės)

Tikslas	Pagrindiniai klausimai	Numatomi pagalbiniai klausimai
Nustatyti kokie valdymo procesai taikomi bendrovės veikloje	1. Aprašykite organizacijoje vykstančius valdymo procesus?	▪ Kokia organizacinė struktūra vyrauja organizacijoje? ▪ Kas atsakingas už informacijos saugą? ▪ Kas valdo informacinius resursus? ▪ Su kokia informacijos rizika buvo susidurta, kaip rizika buvo valdoma? ▪ Kaip veikia sistemos kontrolės sistema? ▪ Kaip gerinama informacijos saugos sistema? Kaip dažnai jį tobulinama?
Nustatyti organizacijos saugos kryptis	2. Aprašykite informacijos saugos politikas, kurios taikomos bendrovės veikloje?	▪ Trumpai apibūdinkite organizacijos saugos politiką bei saugos sistemos organizavimo procesus? ▪ Kaip užtikrinama vidinė ir išorinė informacijos apsauga, kas atsakingas už jos užtikrinimą? ▪ Kaip valdomi kompiuteriai, tinklai, prieiga prie sistemų? ▪ Kaip kuriama, derinama ir aptarnaujama informacinę sistemą, valdo informacijos saugos incidentus, kaip tai vykdoma? ▪ Kas stebi standarto atitikimą norminiams teisės aktams?
Informacijos saugos priemonių realizavimas ir realizavimo rezultatai	3. Kokios priemonės yra taikomos organizacijos veikloje, siekiant užtikrinti	▪ Kokias informacijos saugos priemones naudojate praktikoje? ▪ Jūsų darbuotojai yra supažindinti su ISO/IEC 27001:2013 reikalavimais, kaip dažnai vykdomi apmokymai ta tema, kaip dažnai?

	informacijos saugą? Aprašykite gautus rezultatus realizavus saugos priemones	▪ Kaip dažnai atnaujinama antivirusinė programinė įranga, kas už tai atsakingas. ▪ Jūsų bendrovės teritorijoje yra kameros? ▪ Kaip dažnai remontuojami lokaliniai tinklai? Kas tuos darbus atlieka? Kaip dažnai atliekamas remontas? ▪ Kokie rezultatai buvo pasiekti realizavus saugos priemones?
Nustatyti bendrąsias respondentų charakteristikas	4. Trumpai aprašykite bendrovės veiklą, savo pareigas, išvardinkite standartus, kurie yra įdiegti bendrovėje?	▪ Kokia veiklą vykdo Jūsų atstovaujama bendrovė? ▪ Kokias pareigas užimate? ▪ Jūsų bendrovėje įdiegta ISO/IEC 27001:2013? ▪ Jūsų bendrovėje yra įdiegti kiti ISO standartai? ▪ Kokie sunkumai kilo diegiant ISO 27001:2013 standartą?

Remiantis 2 lentelėje pateikta medžiagą, baigiamojo darbo tyrimo metodika suskirstyta į keturias pagrindines grupes: 1 - valdymo procesų, taikomų bendrovės veikloje nustatymas, 2 – informacijos saugos užtikrinimo krypčių identifikavimas, 3 – informacijos saugos priemonių nustatymas, 4 – respondentų bendrųjų charakteristikų analizė.

3. INFORMACIJOS SAUGOS NAUDOJIMO YPATUMŲ EMPIRINIŲ DUOMENŲ ANALIZĖ

3.1. Ekspertų bendrosios charakteristikos

Tyrimo metu buvo nustatyta, kad ekspertų interviu dalyvavo keturių, skirtinga veikla užsiimančių, organizacijųatstovai; vykdantys IT skyriaus vadovo, departamento viršininko, informacijos saugos departamento ir informacijos saugos vadovo pareigas.

3 lentelė. **Ekspertų bendrosios charakteristikos**

(šaltinis: sudaryta autorės)

Kategorija	Subkategorija	Respondentų nuomonė pagrindžiantys teiginiai
Bendrovės veiklos aprašymas	Veikla	„medicinos sektorių“ (R1) „aš atstovauju banką“ (R2) nenorėčiau skleisti šios informacijos, tai specifinė veikla (R3) vykdo spaudos darbus (R4)
	Pareigos	„IT skyriaus vadovo pareigas“ (R1) užimu saugos departamento viršininko pareigas (R2) esu informacijos saugos departamento viršininkas (R3) Aš esu informacijos saugos vadovas (R4)
	Kiti ISO standartai	„ISO 9001 standarto“ (R1) Banke yra įdiegti ISO 9001 (R2) buvo įdiegtas ir kitas ISO standartas (R3) kiti ISO standartai: 9001, 14001, 14298 (R4)
	Sunkumai diegiant ISO	„didelių sunkumų neiškilo, tačiau daug laiko užėmė personalo apmokymai ir adaptacija“ (R1) Negaliu pasakyti, kad diegiant standartą iškilo tam tikri sunkumai (R2) Mes ilgai ieškojome bendrovės, kuri apsiimtų dokumentų tvarkymu ir palengvintų standarto įdiegimo procesą (R3) nepakankamas resursų skyrimas veiklos funkcijoms atlikti, kritinių sprendimų dėl IT infrastruktūros atnaujinimo priėmimas, darbuotojų mokymai ir pasipriešinimas, laikymasis naujų tvarkų, kaip yra dokumentuota, aktualios dokumentacijos palaikymas (R4)

R1 atstovauja medicinos sektorių, užima IT skyriaus vadovo pareigas, bendrovėje ISO 27001 standartas yra įdiegtas nuo 2014 metų, jis buvo derintas prie jau turimo ISO 9001 standarto. Respondentas pažymėjo, kad diegiant informacijos saugos standartą didelių sunkumų neiškilo, tačiau daug laiko užėmė personalo apmokymai ir adaptacija.

R2: „aš atstovauju banką, užimu saugos departamento viršininko pareigas. Kada tiksliai banke įdiegtas ISO 27001 standartas negaliu tiksliai pasakyti, nes dirbu šiame banke tik 4 metus, tačiau žinau, kad gana senai, nuo 2006 metų tikrai. Banke yra įdiegti ISO 9001“.

„Negaliu pasakyti, kad diegiant standartą iškilo tam tikri sunkumai, gal sunkiau laikytis šių reikalavimu ir užtikrinti nuolatinę informacijos saugą banke, nes dažnai keičiasi personalas, seni darbuotojai išeina, nauji ateina ir reikia nuolat stebėti, kad jų žinoma informacija liktų banko nuosavybe ir nepasiektų kitų asmenų“.

R (3) – „nenorėčiau skleisti šios informacijos, tai specifinė veikla, susijusi su investicine birža. Aš asmeniškai esu informacijos saugos departamento viršininkas. Bendrovėje ISO 27001 įdiegtas nuo 2014 metų, iš karto kai buvo įkurta bendrovė, tuo pačiu metu buvo įdiegtas ir kitas ISO standartas.

Negalėčiau pasakyti, kad kilo sunkumai diegiant ISO 27001. Mes ilgai ieškojome bendrovės, kuri apsiimtų dokumentų tvarkymu ir palengvintų standarto įdiegimo procesą, tačiau likome patenkinti jų veikla ir reikalui esant kreipiamės pagalbos“.

R (4) – „Aš esu informacijos saugos vadovas ir mano atstovaujama Bendrovė vykdo spaudos darbus. Bendrovė įdiegė ISO 27001 prieš kelis metus. Be šio standarto įmonėje įdiegti kiti ISO standartai: 9001, 14001, 14298.

Diegiant ISO 27001 buvo iškilę keli sunkumai: nepakankamas resursų skyrimas veiklos funkcijoms atlikti, kritinių sprendimų dėl IT infrastruktūros atnaujinimo priėmimas, darbuotojų mokymai ir pasipriešinimas, laikymasis naujų tvarkų, kaip yra dokumentuota, aktualios dokumentacijos palaikymas“.

3.2. Informacijos resursų valdymo procesų įmonėse analizė

Pirmas ekspertinio interviu klausimų blokas buvo skirtas organizacijose vykstantiems darbo procesams aprašyti: nustatyti organizacijose vyraujančią valdymo struktūra, identifikuoti kas bendrovėse yra atsakingas už informacijos saugą, kaip vykdomas informacinių resursų ir rizikos valdymas, kai veikia rizikos kontrolės sistemos valdymas.

4 lentelė. **Informacijos resursų valdymo procesų įmonėse analizė**

(šaltinis: sudaryta autorės)

Kategorija	Subkategorija	Respondentų nuomonė pagrindžiantys teiginiai
	Organizacijos valdymo struktūra	„esame sveikatos priežiūros įstaiga“.... .<...> atstovaujamos įmonės valdymo struktūra yra hierarchinio pobūdžio (R1) „esu banko atstovas“ <...> banke vyrauja tiesioginio pavaldumo organizacinė valdymo schema (R2) „bendrovė užsiima investiciniais fondais“ <...> „bendrovės organizacinė struktūra yra labai sudėtinga, kadangi valdoma yra visai iš kitos šalies ir tai yra bendrovė sujungta iš kelių bendrovių“ (R3) „ mes užsiimame informacinių sistemų kūrimu ir duomenų priežiūra“ <...> Organizacijoje vyrauja funkcinė organizacinė struktūra <...> (R4)
	Atsakingumas už informacijos saugą	„informacinės sistemos saugą, administravimą ir priežiūrą paskirta informacinių technologijų tarnybai“ (R1) „atsakomybė už informacijos saugą atitenka taip pat kiekvienam banko darbuotojui“ (R2) „bendrovė turi informacinės rizikos saugos departamentą, kuris savo kompetencijų rėmuose atlieka visus darbus, susijusius su bendrovės informacijos saugą“ (R3) „Bendrovėje yra informacijos saugos padalinys <...> ir atsako už informacijos saugos politikos laikymąsi bendrovėje“ (R4)
	Informacinių resursų valdymas	„informaciniai resursai sveikatos apsaugos sektoriuje yra labai plati sąvoka <...> kalbant apie resursų valdymą ir administravimą negalima išskirti vieną konkretų asmenį arba tarnybą (R1) „informacijos saugos valdymą vykdo kuratorius“ (R2) „bendrovėje informacinius resursus valdo informacijos saugos komitetas“ (R3)

Organizacijoje vykstantys valdymo procesai		„informacinius resursus valdo patys resursų savininkai, jie ir yra atsakingi už jų turimos informacijos saugą“ (R4)
	Informacinė rizika ir jos valdymas organizacijoje	„bendrovė dažnai susiduria su skirtinga informacijos rizika. Dažniausiai pažeidžiami įrašai apie pacientus“<...> rizikos valdymas vykdomas naudojant duomenų klasifikavimo politiką, <...>naudojama šifravimo politika <...> kruopščiai rūpinamasi tinklo apsauga ir visada yra paruoštas avarinis duomenų atstatymo planas. (R1) „banke kaupiama, renkama ir saugoma informacija yra labai vertinga, ir jos riziką galima suskirstyti į tris dalis<...> „valdymas vykdomas atliekant monitoringą“ (R2) „informacinė rizika yra skirtingų rūšių“ <...> „informacijos saugos incidentų valdymas yra aprašytas atitinkamame dokumente, kiekvienu atveju į incidentą reaguojama skirtingai“ (R3) „netinkamas informacijos klasifikavimas“ <...> „informacijos praradimas sugedus kompiuterinei įrangai“ <...> informacijos atskleidimas siunčiant ją elektroniniu būdu <...> informacinės saugos sistema kontroliuojama griežtai apibrėžiant darbuotojų funkcijas (R4)
	Rizikos kontrolės sistemos veikimo principas	„šifruojamos korporatyvinės platformos, biometrinės technologinės autenfikacijos, o taip pat sistemos sekančios įtartiną efektyvumą“ (R1) „Vidinės kontrolės departamentas vykdo esamos politikos laikymosi kontrolę, atliekant vidinius informacijos saugos auditus“ (R2) „Bendrovėje nuolat vyksta sistemos monitoringas“ (R3) „Informacinės saugos sistema kontroliuojama griežtai apibrėžiant darbuotojų funkcijas, vaidmenis ir atsakomybes“ (R4)
	Informacijos saugos sistemos gerinimas, tobulinimas	„vien atsarginių priemonių diegimas nėra pakankama priemonė, būtina išskirtinį dėmesį skirti personalo apmokymui, susijusiems su informacijos sauga“ (R1) „sistemos gerinimas banke yra vykdomas nuolat, atsiradus naujovėms ar atsiradus tam tikram poreikiui“ (R2) „Pati informacijos saugos politika yra kuriama 3 metams, tačiau tobulinimai vyksta nuolat“ (R3) Informacijos saugos sistema tobulinama nuolatos atsižvelgiant į rizikas ir kitus įtakojančius veiksnius, finansines galimybes (R4)

„Medicinos bendrovėje vyrauja hierarchinio pobūdžio valdymo struktūra. Generalinis direktorius užima aukščiausią poziciją struktūros schemoje, jam pavaldūs visi kiti skyriai ir padaliniai, kuriems vadovauja paskirti direktoriaus pavaduotojai (R1).

Kalbant apie atsakomybę už informacijos saugą pažymėta, kad:“ už informacinės sistemos saugą, administravimą ir priežiūrą paskirta informacinių technologijų tarnyba“(R1) Vadovas išsako savo nuomonę, teikia informacijos valdymo pasiūlymus. Bendrovės generalinis direktorius kontroliuoja sistemos rezultatyvumą ir aprūpinimą reikalingais resursais (tai gali būti naujas personalas, arba naujų technologijų įsigijimas. Pagrindinis bendrovės tikslas nukreiptas į gydymo įstaigos informacijos saugą, yra sistemos atitikimas ISO 27001 reikalavimams. Atitikimas standarto reikalavimams kiekvienais metais pagrindžiamas atliekant nepriklausomą auditą.(R1)“

„Analizuojant informacinių resursų valdymo schemą buvo pažymėta, kad informaciniai resursai sveikatos apsaugos sektoriuje yra labai plati sąvoka: (R1) „tai popieriniai, elektroniniai arba kiti informaciniai resursai apie žmogaus sveikatą ir sveikatos institucijų veiklą. Duomenys yra laikomos bibliotekose, archyvuose, fonduose, failuose, duomenų bazėse ir kituose šaltiniuose, todėl kalbant apie resursų valdymą ir administravimą negalima išskirti vieną konkretų asmenį arba tarnybą.<...> Galima drąsiai teigti, kad informacinius resursus valdo visi ligoninės darbuotojai. Tik tas valdymas, kiekvieno darbuotojo atžvilgiu, yra skirtingo mąsto ir turinio“ (R1)

Pokalbio su medicinos įstaigos darbuotoju metu paaiškėjo, kad bendrovė dažnai susiduria su skirtinga informacijos rizika. Dažniausiai pažeidžiami įrašai apie pacientus. Elektroniniuose medicininiuose resursuose fiksuojama skirtinga informacija: kreditinių kortelių duomenys, elektroninio pašto adresai, socialinio draudimo numeriai, informacija apie paciento darbo vietą, ligos istorijos ir kita konfidenciali informacija. R1: „Mūsu įstaigoje duomenų vogimo atveju nebuvo, tačiau remiantis pasauline praktika, informacija pavogta iš medicininių archyvų juodojoje rinkoje kainuoja 50 kartų brangiau nei bet kokia kita informacija. Dažnai kreditinių kortų duomenų praradimas sprendžiamas gana greitai: blokuojant kortą arba gaunant naują, o medicininę informaciją galima naudoti kelis metus ar net dešimtmečius“. Pagrindinės grėsmės, su kuriomis yra susiduriama valdant informacinius resursus mūsų įstaigoje yra kenksmingos programos ir taip vadinamos DOS – atakos, tarnautojų nerūpestingumas, silpna mobilių įrenginių apsauga, darbas su nuosavais mobiliais įrenginiais sudaro didelę grėsmę informacijos konfidencialumui.

„Duomenų praradimas kiekvienai organizacijai yra didelė problema, medicinos informacijos praradimas ne tik neigiamai veikia gydymo efektyvumą, bendrovė moka dideles

baudas už duomenų praradimą, brangiai kainuoja ir advokatų samdymas, prarandama įstaigos reputacija“.

(R1) „Mūsų įstaigoje vyrauja duomenų klasifikavimo politika, siekiant užtikrinti duomenų vientisumą, naudojama šifravimo politika, kruopščiai rūpinamasi tinklo apsauga ir visada yra paruoštas avarinis duomenų atstatymo planas. Pagrindinės technologinės priemonės, naudojamos informacijos saugai užtikrinti yra: šifruojamos korporatyvinės platformos, biometrinės technologinės autenfikacijos, o taip pat sistemos sekančios įtartiną efektyvumą. R1 pažymėjo, kad vien atsarginių priemonių diegimas nėra pakankama priemonė, būtina išskirtinį dėmesį skirti personalo apmokymui, susijusiems su informacijos sauga“.

R2 – „Kalbant apie banko struktūrą, galima pažymėti, kad banke vyrauja tiesioginio pavaldumo organizacinė valdymo schema. Pavaldumo viršuje yra akcininkai, akcininkams pavadus auditorius, direktorius, revizijos komisija. Direktoriui pavaldi banko valdyba ir valdymo pirmininkas, kuris vadovauja banko komitetui, direktoriaus pavaduotojams, patarėjams, personalo valdymo padaliniui, dukteriniams bankams ir t.t.“

„Už informacijos saugą banke atsakingas banko informacijos saugos departamento viršininkas. Informacijos saugos valdymą vykdo kuratorius. Atsakomybė už informacijos saugos palaikymą aktualioje būsenoje, kūrimą, įdiegimą, koordinavimą ir pokyčius informacijos saugos procesuose suteikta atsakingam padaliniui“ (R2).

„Atsakomybė už informacijos saugą atitenka taip pat kiekvienam banko darbuotojui. Darbuotojų atsakomybė už esamos politikos vykdymą aprašyta darbo sutartyje, o taip pat vidiniuose normatyviniuose banko dokumentuose.

Banke kaupiama, renkama ir saugoma informacija yra labai vertinga, ir jos riziką galima suskirstyti į tris dalis:

1. Grėsmės, susijusios su žmogaus veikla. Jų tarpe galima išskirti grėsmes dėl žmogiškųjų faktorių, asmeniui neatsakingai dirbant su informacijos laikmenomis. Dažniausiai asmenys nesąmoningai daro klaidas, bet būna atvejų, kai incidentai atsiranda dėl sąmoningos darbuotojų veiklos.
2. Antra grupė – tai technologinės grėsmės, kai grėsmės objektą įtakoja objektyvūs fiziniai procesai techninio charakterio. Technologinėms grėsmėms galima priskirti sistemų gedimus.
3. Trečia grėsmių grupė – tai natūralios gamtinės grėsmės: audros, stichinės nelaimės ir t.t.“

„Kalbant apie kontrolės sistemą, verta pabrėžti, kad banko informacijos saugos bendrą kontrolę vykdo kuratorius. Valdymas vykdomas atliekant monitoringą ir banke įvykusių

incidentų valdymą. Vidinės kontrolės departamentas vykdo esamos politikos laikymosi kontrolę, atliekant vidinius informacijos saugos auditus“

„Informacijos saugos sistemos gerinimas banke yra vykdomas nuolat, atsiradus naujovėms ar atsiradus tam tikram poreikiui. Tačiau sistema negali būti naujinama neįbandžius naujovių ir šis procesas yra griežtai reglamentuojamas vidiniais banko dokumentais: surašomi bandymų protokolai, rezultatai ir t.t. Bandymus vykdo IT blokas arba sistemos kūrėjas. Visų naujovių diegimo faktas fiksuojamas banko tvarkoje“.

R3 – (investiciniai fondai):“ mūsų bendrovės organizacinė struktūra yra labai sudėtinga, kadangi valdoma yra visai iš kitos šalies ir tai yra bendrovė sujungta iš kelių bendrovių. Manau, kad atsakymas į šį klausimą neturės didelės įtakos nagrinėjant klausimus, susijusius su informacijos sauga bendrovėje, kadangi aš galiu komentuoti tik klausimus, kuriuos galima pritaikyti Lietuvoje veikiančioje bendrovėje“.

„Realizuojant, eksploatuojant, kontroliuojant ir palaikant atitinkamą informacijos saugos lygį. Bendrovė turi informacinės rizikos saugos departamentą, kuris savo kompetencijų rėmuose atlieka visus darbus, susijusius su bendrovės informacijos saugą: įvairiais būdais mažina riziką, valdo jį, organizuoja informacijos saugos kūrimą, kontroliuoja eksploatavimo atitikimą norminiams dokumentams. Minėtas departamentas taip pat planuoja sąnaudas, kurių reikės informacijos saugos politikos įgyvendinimui“.

„Informacijos saugos techninių priemonių realizavimą vykdo IT blokas kartu su informacinės rizikos saugos departamentu. Informacijos saugos tikslų atitikimą bendrovės tikslams kuruoja informacinės rizikos saugos viršininkas. Užtikrinant informacinę saugą, bendrovėje yra eilė kitų darbuotojų, kurių kiekvienas turi savo funkcijas:

- Nepertraukiamos veiklos aprūpinimo sistemos vadybininkas yra atsakingas už nepertraukiamą sistemos veiklą.
- Incidentų valdymo vadybininkas atsakingas už reagavimą į informacinės saugos procesų organizavimą, incidentų nustatytą ir jų analizę.
- Auditorius – atsako už įdiegtos sistemos atitikimą bendrovės normatyviniams dokumentams ir ISO standartui.
- Apmokymo vadybininkas – organizuoja, planuoja, reguliariai atlieka darbuotojų apmokymus informacijos saugos srityje“.

„Bendrovėje informacinius resursus valdo informacijos saugos komitetas. Galima teigti, kad informacinė rizika yra skirtingų rūšių: rizika, kad informacija bus kopijuojama ar perduodama naudojant kitus techninius kanalus, kartais informacija yra įrašoma į diktofoną ir ją naudojimąsi savo asmeniniais tikslais, ar ji skelbiama kituose vietose, perduodama kitiems fiziniams ar juridiniams asmenims. Buvo atveju, kad dingdavo įrašai iš kamerų“.

„Informacijos saugos incidentų valdymas yra aprašytas atitinkamame dokumente, kiekvienu atveju į incidentą reaguojama skirtingai. Dažniausiai, pirmoje eilėje, nustatomas incidento šaltinis: jis gali būti vidinis arba išorinis. Vidines rizikas identifikuoti yra lengviau, nes priėjimas prie bendrovės duomenų bazių yra griežtai kontroliuojamas skirtingomis priemonėmis. Bendrovėje nuolat kaupiama ir analizuojama informacija apie incidentus, tos informacijos pagrindu informacijos saugos politika yra koreguojama, aptinkamos labiausiai pažeidžiamos vietos. Bendrovėje yra nustatytos formalios procedūros, kurių būtina laikytis aptikus neatitikimus įmonės informacijos saugos sistemoje, užfiksavus incidentus“.

„Bendrovėje nuolat vyksta sistemos monitoringas“.(R3):“ Monitoringo tikslas yra greitas klaidų nustatymas apdorojant informaciją, operatyvi reakciją į informacijos saugos pažeidimus, įvykusius ir neįvykusius incidentus. Kompanijoje reguliariai, ne rečiau nei 1 kartą per metus vykdoma informacijos saugos sistemos analizė. Analizės metu vertinami audito rezultatai, statistika ir papildoma informacija apie įvykusius informacijos saugos incidentus, informacijos saugos procesu efektyvumo įvertinimo rezultatai, o taip pat svarstomi visų suinteresuotų šalių pasiūlymai ir komentarai“.

„Pati informacijos saugos politika yra kuriama 3 metams, tačiau tobulinimai vyksta nuolat. Saugos sistema yra tobulinama, jeigu audito metu nustatomas informacijos saugos lygio sumažėjimas, jeigu keičiasi organizacinė ir technologinė infrastruktūra“.

R (4) :“Organizacijoje vyrauja funkcinė organizacinė struktūra. Kiekvienas padalinys turi savo griežtai apibrėžtas funkcijas, kurias privalo atlikti kokybiškai ir laiku. Bendrovėje yra informacijos saugos padalinys, kurį valdo informacijos saugos vadovas, jis tiesiogiai pavaldus generaliniam direktoriui ir atsako už informacijos saugos politikos laikymąsi bendrovėje“.

„Informacinius resursus valdo patys resursų savininkai, jie ir yra atsakingi už jų turimos informacijos saugą“.

„Per įmonės egzistavimo laiką buvo susidurta su daugybę skirtingų rizikų, tačiau galima pažymėti kelias, kurios atsitinka dažiausiai:

- Netinkamas informacijos klasifikavimas, kas sąlygoja informacijos atskleidimą asmenims, kurie neturėtų su informacija susipažinti. Tokia rizika valdoma apibrėžiant informacijos klasifikavimą, per darbuotojų mokymus, nuolatinę kontrolę ir vidaus auditus;
- Informacijos praradimas sugedus kompiuterinei įrangai. Rizika valdoma per valdymo planavimą ir atsarginių kopijų darymą;

- Informacijos atskleidimas siunčiant ją elektroniniu būdu (el. paštu, kitomis priemonėmis). Rizika valdoma šifruojant jautrią informaciją, kuri perduodama elektroniniais kanalais“;

„Informacinės saugos sistema kontroliuojama griežtai apibrėžiant darbuotojų funkcijas, vaidmenis ir atsakomybesatliekant vidaus ir išorės auditus įvertinat funkcijų, vaidmenų ir atsakomybių atitikimą standarto reikalavimams.

Informacijos saugos sistema tobulinama nuolatos atsižvelgiant į rizikas ir kitus įtakojančius veiksnius, finansines galimybes. Bent kartą per metus yra atliekami vidaus ir išorės auditai, atliekamas vertinimas, kaip funkcionuoja vadybos sistema, vertinamos rizikos. Atitinkamai formuojami metiniai tikslai ir jų įgyvendinimo planas (užduotys)“.

Apibendrinant galima teigti, kad respondentai pakankamai daug dėmesio skiria informacijos saugai, taiko naujausias ir populiariausias priemones. Informacinės saugos sistemas diegia didelės bendrovės, kuriuose yra specialus IT padalinys.

3.3. Organizacijos informacijos saugos krypčių analizė

Antras klausimų blokas buvo skirtas apibrėžti informacijos saugos politiką, vyraujančią ekspertų atstovaujamose organizacijose. Buvo nustatyti organizacijos saugos politika ir procesai, kaip organizuojama vidinė ir išorinė informacijos apsauga, kompiuterių, tinklų ir prieigų valdymas, informacinių sistemų kūrimas, derinimas ir aptarnavimas, standartų atitikimo norminiams teisės aktams stebėjimas.

5 lentelė. **Organizacijos informacijos saugos krypčių analizė**

(šaltinis: sudaryta autorės)

Kategorija	Subkategorija	Respondentų nuomonė pagrindžiantys teiginiai
Informacinės saugos politika	Organizacijos saugos politika ir procesai	„politikos esmė - programinės – techninės priemonės turi būti funkcionalios“ <....> „procesai skirstomi į 3 pagrindinius etapus.....“ (R1) „ informacijos saugos reikalavimai turi atitikti banko veiklos rezultatus ir būti sukurti tam, kad sumažinti riziką, susijusią su informacijos sauga“<.....>„rizikos faktoriai informacinėje banko sferoje yra susiję su jo korporatyviniu valdymu, verslo procesų organizavimu ir realizavimu, bendradarbiavimu su klientais ir kontrahentais“ (R2) „Bendrovėje taikoma informacijos saugos politika yra neatsiejama visos organizacijos politikos dalis. Politika remiasi informacijos saugos vertinimu ir skirta bendrovės informacijos saugos kūrimui, realizavimui, eksploatavimui, monitoringui, analizei, tobulinimui“ (R3) „Bendrovės informacijos saugos politika apima kelias pagrindines sritis....“ <...> užtikrinti, kad jautri informacija būtų apsaugota nuo atskleidimo, paviešinimo, pakeitimo, sunaikinimo ar praradimo, <....>vadovybės ir darbuotojų (R4)
	Vidinė ir išorinė informacijos apsauga	„Naudotojo lokalinė autorizacija <...> „ administratorius turi iš anksto sutikrinti personalinio identifikatoriaus atitikimą konkrečiam naudotojui“ (R1) „Bankas naudoja labai daug skirtingų priemonių informacijos saugai užtikrinti.....“ (R2) „Užtikrinant bendrovės informacijos apsaugą realizuojami keturios procesų grupės....“ (R3) „ taikomos administracinės priemonės <...> ugniasienės, tinklo infrastruktūros planavimas, tinklų atskyrimas, antivirusinės, atsarginių kopijų darymo, informacijos šifravimas, prieigos kontrolės ir pan.) ir kitos priemonės informacijos apsaugai (vidaus ir išorės auditai ir pan.)(R4)
	Kompiuterių, tinklų ir prieigų valdymas	„administratorius turi iš anksto sutikrinti personalinio identifikatoriaus atitikimą konkrečiam naudotojui“ (R1) „yra sukurta <...> valdymo tvarka,(R2) „Informacijos saugos klausimai turi būti sprendžiami kompleksiškai ir blokuoti visus informacijos nutekėjimo kanalus (R3) „Prieiga prie informacijos ir informacinių resursų skiriama vadovaujantis principu „Būtina žinoti“ (R4).
	Informacinių sistemų kūrimas, derinimas ir aptarnavimas	„Informacinė sistema kuriama ir atnaujinama pagal poreikį, pavyzdžiui įvedant naują paieškos filtrą/pjūvį“ (R1) „Tvarkoje incidentų valdymo procesas suskaidytas į 6 žingsnius....“(R2) kuriama taip vadinama kompleksinė informacijos sauga, organizacinių ir inžinerinių, programinių – aparatinių priemonių sąveika, kurie užtikrina informacijos saugą automatizuotose sistemose“ (R3) „Įmonėje yra sukurtos ir įdiegtos atitinkamos tvarkos informacinių sistemų kūrimui“ (R4)
	Standartų atitikimo norminiams teisės aktams stebėjimas	„Standarto atitikimą reikalavimams stebi audito komisija“ (R1) „Už informacinės banko saugos atitikimą ISO 27001 reikalavimams atsako atsakingas padalinys<...> (R2) „Standarto atitikimas norminiams teisės aktams stebimas organizacijos atstovas kokybei“ (R3) „Informacijos saugos vadovas stebi standarto atitikimą reikalavimams“(R4)

„Programinės – techninės priemonės turi būti funkcionalios ir turi suteikti galimybę paskirstyti prieigas prie informacijos pagal tam tikrus kriterijus, garantuojant naudotojo prieiga tik prie tos informacijos ar programos, kuri yra būtina profesionalių funkcijų vykdymui. Teisių paskirstymo technologija leidžia turėti taip vadinamą „super naudotoją“ – administratorių, kuris gali prieiti prie visų duomenų. Administratoriaus pareiga yra suteikti ar apriboti visų kitų darbuotojų prieiga prie sistemos. Minėtą procesą galima suskirstyti į 3 pagrindinius etapus R1 (medicinos įstaiga):“

1. „Naudotojo identifikacija;
2. Ryšio su serveriu nustatymo seansas, kurio metu sistema nustato, kuriai grupei priklauso naudotojas;
3. Sistema tikrina kokią užklausą padarė naudotojas, ar kokius duomenis nori gauti ir leidžia arba draudžia naudotis duomenimis“.

„Naudotojo lokalinė autorizacija, įvedant ar apdorojant paciento duomenis, vykdoma po PIN kodo įvedimo, jeigu PIN kodas įvestas teisingai, operacinė sistema pradeda krovimo procesą. Naudotojo prieigos prie terminalinio serverio apribojimai vykdomi naudojant programines – aparatines informacijos saugos priemones, funkcionuojantys terminaliniu režimu.

Siekiant sėkmingai atlikti naudotojo autorizaciją terminaliniame serveryje, administratorius turi iš anksto sutikrinti personalinio identifikatoriaus atitikimą konkrečiam naudotojui. Taigi, norint dirbti su terminalinio serverio resursais, naudotojui reikia atlikti identifikavimo procedūrą terminaliniame serveryje, pateikiant personalinį identifikatorių ir įvedant PIN kodą. Informacinė sistema kuriama ir atnaujinama pagal poreikį, pavyzdžiui įvedant naują paieškos filtrą/pjūvį“.

„Siekiant valdyti informacijos saugos incidentus, nustatoma koks kompiuteris yra incidento šaltinis, galima net nustatyti koks vartotojas buvo prisijungęs incidento laiku, aišku jei tai yra vidinio pobūdžio informacinė ataka. Išorinių atakų valdymas ne mūsų kompetencijoje“.

„Šios sistemos funkcionavimas, kaip jau buvo minėta, tikrinamas kas metus, vykdant nepriklausomą auditą, tačiau sistema yra naujinama nuolat, kelis ar keliasdešimt kartų per metus. Atnaujinimai vyksta priimant ar atleidžiant iš darbo darbuotojus, nuolat vykdomi sistemos diagnostikos darbai, diegiamos moderniausios antivirusinės programos. Standarto atitikimą reikalavimams stebi audito komisija“.

„Banko valdymo institucijos labai gerai suvokia informacijos saugos vystymo ir gerinimo būtinumą, o taip pat būtinybę vystyti realizuojamas banko technologijas. Informacijos saugos reikalavimų laikymasis suteikia bankui papildomus konkurencinius

pranašumas, užtikrina finansinį stabilumą, rentabilumą, atitikimą teisiniams, reguliuojantiems ir sutartiniams reikalavimams, kelia banko imidžą“.R – 2 (bankas).

„Informacijos saugos reikalavimai, iškelti banko valdymo organų atitinka banko veiklos rezultatus ir sukurti tam, kad sumažinti riziką, susijusią su informacijos sauga. Rizikos faktoriai informacinėje banko sferoje yra susiję su jo korporatyviniu valdymu, verslo procesų organizavimu ir realizavimu, bendradarbiavimu su klientais ir kontrahentais“.

„Bankas naudoja labai daug skirtingų priemonių informacijos saugai užtikrinti: vykdoma slaptažodžio priskyrimo ir pakeitimo politika, griežtai draudžiama palikti techninius įrenginius be priežiūros įvedus informaciją ir neatsijungus, saugos administratorius periodiškai konfigūruoja operacinę sistemą ir vykdo periodinę nustatymų kontrolę; reguliariai diegiamos informacinės sistemos naujinimai (ServicePacks; Hotfit ir t.t.), nuolat naujinama antivirusinė bazė ir nagrinėjami informaciniai resursai, siekiant laiku minimizuoti pavojingas pasekmes. Bankas organizuoja ir naudoja audito sistemą, plačiai analizuojami audito rezultatai“.

„Svarbi informacija yra papildomai saugoma USB laikmenose arba e – Token sistemoje. Informacija yra klasifikuojama, klasifikuojama ir naudotojų prieiga prie duomenų. Kiekvienas įrenginys yra apsaugotas reikalingą antivirusinę programa.Pažymėtina, kad banke yra sukurta informacinės saugos incidentų valdymo tvarka, joje aprašyta, kaip reikia reaguoti į incidentus, personalo informavimo apie incidentų aptikimo informavimo eiga, joje parašyta, kad personalas pastebėjęs kompiuterio darbo anomalijas turi iškarto pranešti atsakingam asmeniui. Periodiškai personalas dalyvauja seminaruose, kuriuose aptariami informacijos saugos incidentų valdymo scenarijai. Tvarkoje incidentų valdymo procesas suskaidytas į 6 žingsnius:

1. Incidentų apdorojimo politikos ir procedūrų kūrimas, kuriuose aprašyta darbuotojų apmokymo tvarka ir paskirstoma atsakomybė už iškilusio incidento valdymą.
2. Personalo incidento valdymui paskyrimo procedūrą.
3. Vadovo pareigų ir atsakomybių nustatymas incidento metu.
4. Incidentą valdantys asmenys dalyvauja testuojant incidentų valdymo scenarijus.
5. Incidento valdytojai praneša apie scenarijaus testavimo rezultatus valdymo organams.
6. Banko valdymo organai praneša apie incidentą Valstybės teisėsaugos organams, jeigu tai yra būtina“.

„Už informacinės banko saugos atitikimą ISO 27001 reikalavimams atsako atsakingas padalinys, esant reikalui gali būti įtraukti kiti padaliniai: pvz. finansų skyrius, auditoriai ir t.t.

Bendrovėje taikoma informacijos saugos politika yra neatsiejama visos organizacijos politikos dalis. Politika remiasi informacijos saugos vertinimu ir skirta bendrovės

informacijos saugos kūrimui, realizavimui, eksploatavimui, monitoringui, analizei, tobulinimui. Organizacijos informacijos saugos politikos veiklos sritis yra bendrovės verslo procesai: sandorių organizavimas, kliringo paslaugos ir atstovavimas fondų, valiutų ir kt. rinkose. Informacinės saugos politika taikoma pritraukiant potencialų klientą, suteikiant galimybę (juridinės, organizacinės, techninės sąlygos) potencialiam klientui dalyvauti sandoriuose ir kliringo procesuose, dalyviui vykdant prekybines operacijas rinkoje, dalyviui gaunant ataskaitą apie įvykdytas operacijas ir kliringo rezultatus“R (3) – (investiciniai fondai).

„Informacijos saugos politikos sritis apima ir informacinius aktyvus (konfidenciali ir viešai prieinama informacija), kurie priklauso bendrovei. Kompanija užtikrina reikiamą informacinių aktyvų apsaugą kiekviename informacinių technologijų hierarchijos lygyje, naudojant skirtingas apsaugines priemones. Informacinių technologijų hierarchiją sudaro informaciniai aktyvai, informacinių technologijų elementai (informacinės technologijos, programinė, apdorojimo, saugojimo, perdavimo ir naudojimo įranga), bendrovės turimų informacijos aktyvų apdorojimo procesai, reglamentai ir procedūros, bendrovės darbuotojai“.

„Užtikrinant bendrovės informacijos apsaugą realizuojamostrys procesų grupės:

1. Planavimo etape vykdomas informacijos saugos politikos formavimas, nustatoma politikos veiklos sfera, įvertinama informacijos saugos rizika, parenkamos apsaugos priemonės ir formuojami jų realizavimo planai.
2. Realizavimo etape įvykdomi visi planai, susiję su informacijos saugos politikos kūrimu, realizavimu, tobulinimu ir apsaugos priemonių įdiegimu.
3. Tikrinimo etape tikrinamas parinktų saugos priemonių atitikimas nustatytiems informacijos saugos reikalavimams“.

„Tikrinimo etapas yra pagrindinis, kurio metu priimami sprendimai dėl korekcinių ir prevencinių priemonių realizavimo. Bendrovės valdymo organai, suvokiant informacijos saugos svarbą, inicijuoja, palaiko, analizuoja ir kontroliuoja informacijos saugos procesų atlikimą, skatina verslo vystymo sąlygų formavimui su leidžiama rizika.

Informacijos saugos klausimai turi būti sprendžiami kompleksiškai ir blokuoti visus informacijos nutekėjimo kanalus. Skirtingų priemonių realizavimas dažnai nedidina informacinės sistemos saugos. Šitą teiginį galima paaiškinti paprastu pavyzdžiu. Turime namą ir įstatome neperšaunamas duris, bet palikome atidarytus langus. Ar mes apsaugojome savo gyvenamąjį namą? Ne. Iš kitos pusės, jei tai ne privatus vieno aukšto namas, o 125 aukštas, tai tam tikru laipsniu mes padidinome informacijos saugą. Informaciniuose sistemose situacija analogiška: iš vienos pusės tarptinklinis ekranas gali reikšmingai padidinti informacinės sistemos apsaugą, iš kitos gali nesuteikti jokios naudos“.

„Tam, kad nesuklysti pasirenkant saugos metodus ir priemones, kuriama taip vadinama kompleksinė informacijos sauga, organizacinių ir inžinerinių, programinių – aparatinių priemonių sąveika, kurie užtikrina informacijos saugą automatizuotose sistemose.

„Nemažą svarbą apsaugant informaciją turi organizacinės priemonės. Nežiūrint į tai, kad daugybė organizacijų jas ignoruoja, iš tikro jos yra labiau svarbios nei inžinerinės – techninės“

„Organizacinės priemonės – tai informacijos saugos oficialios politikos kūrimas: vartotojų ir aptarnaujančio personalo pareiginių instrukcijų sudarymas, sistemos komponentų administravimo, apskaitos, laikymo, platinimo, konfidencialios informacijos laikmenų šalinimo taisyklių kūrimas, naudotojų identifikavimas, veiksmo planų kūrimas, aptikus nesankcionuotą prieigą prie tinklo resursų, sugedus apsaugos priemonėms, įvykus avarinei situacijai ir pagaliau informacijos saugos principu paaiškinimas naudotojams.“

„Dažnai nepataisomi informacinės sistemos pažeidimai ar jų ilgas atkūrimas ir yra organizacinių priemonių nebuvimo priežastis, netgi realizuojant tam tikras technines priemones, atliekant reguliarų rezervinį kopijavimą, naudojant RAID – masyvus ir klasterius.“

„Įvykus avarinei situacijai administratorius gali pasimesti, atlikti nekorektiškus veiksmus. Kaip pasekmė, jei informacija ir nebus prarasta, jos atstatymas užims ilgą laiką. Tačiau jeigu jis būtų sumodeliavęs situaciją, sukurtų būtinus diskus ar kitas laikmenas, dokumentiškai apiformintų duomenų atstatymo procedūrą, nebūtų jokių problemų. Įsivaizduokite situaciją, kai sistemą sukuria vienas administratorius, o ją atstato kitas – tokių atveju pasekmės gali būti dar didesnės. Standarto atitikimas norminiams teisės aktams stebimas organizacijos atstovas kokybei.“

R (4) (investiciniai fondai) – „Bendrovės informacijos saugos politika apima kelias pagrindines sritis:

- Tikslus (užtikrinti, kad jautri informacija būtų apsaugota nuo atskleidimo, paviešinimo, pakeitimo, sunaikinimo ar praradimo);
- Atsakomybė ir įsipareigojimai (vadovybės ir darbuotojų);
- Taikymo sritys (politika taikoma visiems procesams ir apima visus informacinius resursus, žodinę bei rašytinę informaciją, informacines sistemas, fizinę aplinką, darbuotojus ir trečių šalių asmenis)“.

„Bendrovėje visi darbuotojai yra atsakingi už informacijos apsaugą, siekiant įgyvendinti šią užduotį yra taikomos administracinės priemonės (pareigybinės, konfidencialumo susitarimai ir pan.), fizinės priemonės (patekimo į patalpas ir prieigos kontrolė), IT (ugniasienės, tinklo infrastruktūros planavimas, tinklų atskyrimas, antivirusinės,

atsarginių kopijų darymo, informacijos šifravimas, prieigos kontrolės ir pan.) ir kitos priemonės informacijos apsaugai (vidaus ir išorės auditai ir pan.)“.

„Prieiga prie informacijos ir informacinių resursų skiriama vadovaujantis principu „Būtina žinoti“. Prieigos suteikimą atlieka IT vadovas, sprendimus dėl prieigos priima informacinių resursų vadovas arba informacijos saugos vadovas“.

„Įmonėje yra sukurtos ir įdiegtos atitinkamos tvarkos informacinių sistemų kūrimui. Taikomųjų sistemų kūrimui turime atskiras aplinkas, kuriose jos kuriamos ir testuojamas ir tik ištestuotos įdiegiamos į realią darbinę aplinką. Informacinių sistemų pakeitimai vykdomi vadovaujantis patvirtinta tvarka.Informacijos saugos incidentus registruoja IT vadovas ir informacijos saugos vadovas, fizinės saugos incidentai registruojami apsaugoje. Incidentai yra analizuojami, vertinamos rizikos ir, jei reikia, imamasi atitinkamų priemonių, kad panašūs incidentai ateityje nepasikartotų“.

„Informacijos saugos vadovas stebi standarto atitikimą reikalavimams. Juridinis skyrius atsakingas už teisės aktų registro aktualumą. Atsiradus naujam teisės aktui ar jo pakeitimui, kuris gali turėti įtaką informacijos saugos vadybos sistemai, teisės aktas yra vertinamas ir priimami sprendimai dėl reikalingų pakeitimų informacijos saugos vadybos sistemoje“.

Apibendrinant, galima teigti, kad informacijos saugos kontrolė vykdoma sistemingai atliekant auditą, diegiant informacinių sistemų naujinimus, papildomai saugant duomenis išorinėse laikmenose. Informacijos saugos politika kuriama sudarant pareiginius nuostatus, formuojant konkrečius tikslus, paskirstant atsakomybes ir įsipareigojimus tarp bendrovės padalinių, pasirašant konfidencialumo sutartis.

3.4. Informacinės saugos priemonių realizavimo rezultatų analizė

Trečia struktūrinė klausimų dalis buvo skirta nustatyti informacijos saugos priemonių realizavimui ir rezultatams, įdiegus standartą, nustatymui. Buvo nustatyta kokios informacijos saugos priemonės naudojamos, kaip dažnai atnaujinamos antivirusinės programos, atliekamas lokalinių tinklų remontas.

6 lentelė. **Informacinės saugos priemonių realizavimo rezultatų analizė**

(šaltinis: sudaryta autorės)

Kategorija	Subkategorija	Respondentų nuomonė pagrindžiantys teiginiai
Informacijos saugos priemonių realizavimas ir realizavimo rezultatai	Darbuotojų susipažinimas su ISO/IEC 27001:2013 reikalavimais	„Visi bendrovės darbuotojai , turintys prieigą prie pacientų informacijos yra supažindintas su ISO 27001 reikalavimais“(R1) „visi mūsų darbuotojai yra supažindini su informacijos saugos politika“ (R2) „Todėl kiekvienas darbuotojas, atėjęs dirbti į mūsų bendrovę turi susižinti su įmonėje taikoma informacijos saugos politiką“ (R3) Visi bendrovės darbuotojai yra supažindinti su ISO/IEC 27001:2013 reikalavimais (R4)
	Antivirusinės programos atnaujinimo dažnumas	„Bendrovėje yra nuolat atnaujinama antivirusinė programa“ (R1) „Antivirusinės programos atnaujinimas vykdomas nuolat, iškilus incidentui <...>“ (R2) „Antivirusinė programa atnaujinama reguliariai“ (R3) „Antivirusinė programa yra atnaujinama iš karto, kai yra išleidžiami duomenų bazės atnaujinimai“ (R4)
	Kameros saugumui	„Visoje įmonės teritorijoje ir ligoninės patalpose (koridoriuose, kai kuriuose kabinetuose) yra kameros“ (R1) „Incidentai valdomi ir stebint darbuotojus ir klientus per įrengtas vaizdo kameras“(R2) „Šioje salėje yra kameros, įrašai peržiūrimi esant poreikiui ar įvykus įvykiui“ (R3)
	Lokalinių tinklų remontavimo dažnumas	Pagal poreikį (R1) „Lokalinių tinkų funkcionalumui palaikyti vieną kartą per mėnesį vykdomi profilaktiniai darbai“ (R2) „Lokaliniai tinklai remontuojami tik esant poreikiui, jei įvyksta gedimas“ (R3) Lokaliniai tinklai tvarkomi pagal poreikį (R4)
	Rezultatai realizavus priemones	„Pati bendrovė jaučiasi saugesnė, įdiegus ISO 27001 standartą, dalis klientų....(„R1) „Realizavus saugos priemones ženkliai sumažėjo incidentų skaičius dėl darbuotojų kaltės... „(R2) „Sunku atsakyti į šį klausimą, kadangi tie pokyčiai nėra apčiuopiami. Gal verta pabrėžti klientų pasitikėjimo bendrove padidėjimą“ (R3) „Sunku įvertinti rezultatus įdiegus ISO 27001, nes rezultatai nėra pamatuojami“ (R4)

„Visi bendrovės darbuotojai, turintys prieigą prie pacientų informacijos yra supažindintas su ISO 27001 reikalavimais, apmokymai vykdomi kas metus, personalas gauna sertifikatus apie išklausytą seminarą“ (R1).

„Bendrovėje yra nuolat atnaujinama antivirusinė programa, mūsų specialistai stebi situaciją IT rinkoje, už tai yra atsakingas tas pats „super“ naudotojas – administratorius, jis taip pat tvarko sistemos gedimus ir atnaujina lokalinius tinklus. Visoje įmonės teritorijoje ir ligoninės patalpose (koridoriuose, kai kuriuose kabinetuose) yra kameros. Įrašai iš kamerų yra saugomi, todėl iškilus konfliktinėms situacijoms ar kažkokiems įvykiams, įrašus galima peržiūrėti.

Įdiegus saugos priemones, informacijos naudotojai tapo atsargesni, nes žino, kad jie atsako už informacijos saugą. Pati bendrovė jaučiasi saugesnė, įdiegus ISO 27001 standartą, dalis klientų, kurie nori išsaugoti paslaptį apie savo ligą kreipiasi būtent į mūsų ligoninę, kadangi mes turime informacijos saugos garantą – taigi galima sakyti, kad standarto įdiegimas kelia bendrovės prestižą ir plečia klientų ratą“.

R2 (bankas) – „visi mūsų darbuotojai yra supažindini su informacijos saugos politika, punktai apie informacinės saugos politikos laikymąsi ir atsakomybę yra įtraukti į darbo sutartis, nuolat vykdomi personalo apmokymai tuo klausimu“.

„Antivirusinės programos atnaujinimas vykdomas nuolat, iškilus incidentui, atliekant kompiuterinės įrangos profilaktinius darbus, atsiradus naujoms antivirusinėms programoms. Incidentai valdomi ir stebint darbuotojus ir klientus per įrengtas vaizdo kameras, analizuojamas įtartinas personalo ir klientų elgesys, incidento šaltiniai ir t.t.

Lokalinių tinkų funkcionalumui palaikyti vieną kartą per mėnesį vykdomi profilaktiniai darbai, tuos darbus atlieka specialus padalinys. Remontuojami tinklai nėra dažnai, nes jų funkcionalią būseną stengiamasi palaikyti nuolat atliekant monitoringą ir profilaktiką“.

„Realizavus saugos priemones ženkliai sumažėjo incidentų skaičius dėl darbuotojų kaltės, nes įvesti specialus duomenų apdorojimo filtrai, kurie atpažįsta klaidingai įvestą informaciją ir informuoja apie tai darbuotojus. Aišku mažiau pasitaiko ir technikos gedimo atveju“.

R (3) – „Nežiūrint į tai, kad mes jau plačiai aptarėm naudojamas priemones, galiu išvardinti pagrindines:

- Tikslinių sistemų ir apsaugos priemonių incidentų ir log - failų monitoringas;
- Leistinos prieigos prie informacinių resursų sistemos realizavimas;
- Vartotojų įėjimo į patalpas, kur randasi techninės priemonės, apdorojančios personalines duomenis, o taip pat saugomos informacijos laikmenos, apribojimas.

- Naudotojų ir aptarnaujančio personalo veiklos registravimas, naudotojų nesankcionuotos prieigos ir veiksmų kontrolė.
- Portatyvinių informacijos laikmenų saugojimas ir apskaita;
- Techninių priemonių rezervavimas, masyvų ir informacijos laikmenų dubliavimas.
- Reikalavimams atitinkančių informacijos apsaugos priemonių naudojimas;
- Apsaugotų ryšio kanalų naudojimas;
- Techninių priemonių naudojimas, leidžiančių įvykdyti personalinių duomenų apdorojimą, apsaugotos teritorijos ribose.
- Fizinis patalpos apsaugos ir techninių priemonių, leidžiančių apdoroti personalinęinformacijąorganizavimas.
- Antivirusinių programų naudojimas.
- Aišku būtinas ir personalo apmokymas“.

„Dažnai darbuotojai nesuvokia informacijos saugos svarbos, ar paprasčiausiai neskiria tam pakankamai dėmesio. Suvokimas ateina tik tada, kai įvykis įvyko ir reikia šalinti jo padarinius. Todėl kiekvienas darbuotojas, atėjęs dirbti į mūsų bendrovę turi susižinti su įmonėje taikoma informacijos saugos politiką ir pasirašyti atitinkamus dokumentus. Strateginiame bendrovės plane yra numatytos mokymų valandos, kurių metu pasakojama apie informacijos saugos politiką, naujoves, būdus kaip kontroliuoti riziką ir sumažinti neigiamus padarinius. Kiekvienas bendrovės darbuotojas yra atsakingas už informacijos saugą įmonėje ir turi laikytis nustatytos tvarkos.“

„Antivirusinė programa atnaujinama reguliariai, vykdomas ir kompiuteriu monitoringas, už tai yra atsakingas informacinės rizikos saugos departamentas, o konkrečiai departamento vadovas. Mūsų bendrovėje taikomos ir kitos saugos priemonės: darbuotojai dirba vienoje salėje. Kiekviena darbo vieta yra atskirta stikline siena. Šioje salėje yra kameros, įrašai peržiūrimi esant poreikiui ar įvykus įvykiui. Tačiau bendrovės direktorius gali pažiūrėti kaip dirba darbuotojai tiesiogiai, per savo darbinį kompiuterį.“

„Lokaliniai tinklai remontuojami tik esant poreikiui, jei įvyksta gedimas. Stengiamasi kuo mažiau liesti tinklus, siekiant neprarasti reikalingos informacijos. Remontą atlieką techninis darbuotojas, kuris irgi priklauso informacijos saugos departamentui.“

Kokie pokyčiai įvyko įdiegus ISO 27001? Sunku atsakyti į šį klausimą, kadangi tie pokyčiai nėra apčiuopiami. Gal verta pabrėžti klientų pasitikėjimo bendrove padidėjimą“.

R (4) „Praktikoje, siekiant užtikrinti informacijos saugą, naudojama fizinė sauga, fizinės prieigos ribojimas (praėjimo kontrolė), vaizdo stebėjimas, IT priemonės (ugniasienė, tinklų atskyrimas, prieigos prie resursų valdymas, duomenų ir serverių atsarginių kopijų darymas, antivirusinė programinė įranga ir t.t.), administracinės priemonės (įdiegtos

procedūros ir tvarkos, kuriomis vadovaujantis turi dirbti darbuotojai, konfidencialumo pasižadėjimai) ir visos kitos priemonės, reikalaujamos pagal standartą.

Visi bendrovės darbuotojai yra supažindinti su ISO/IEC 27001:2013 reikalavimais. Bendri mokymai atliekami kartą į 2 metus, ar pagal poreikį dažniau.

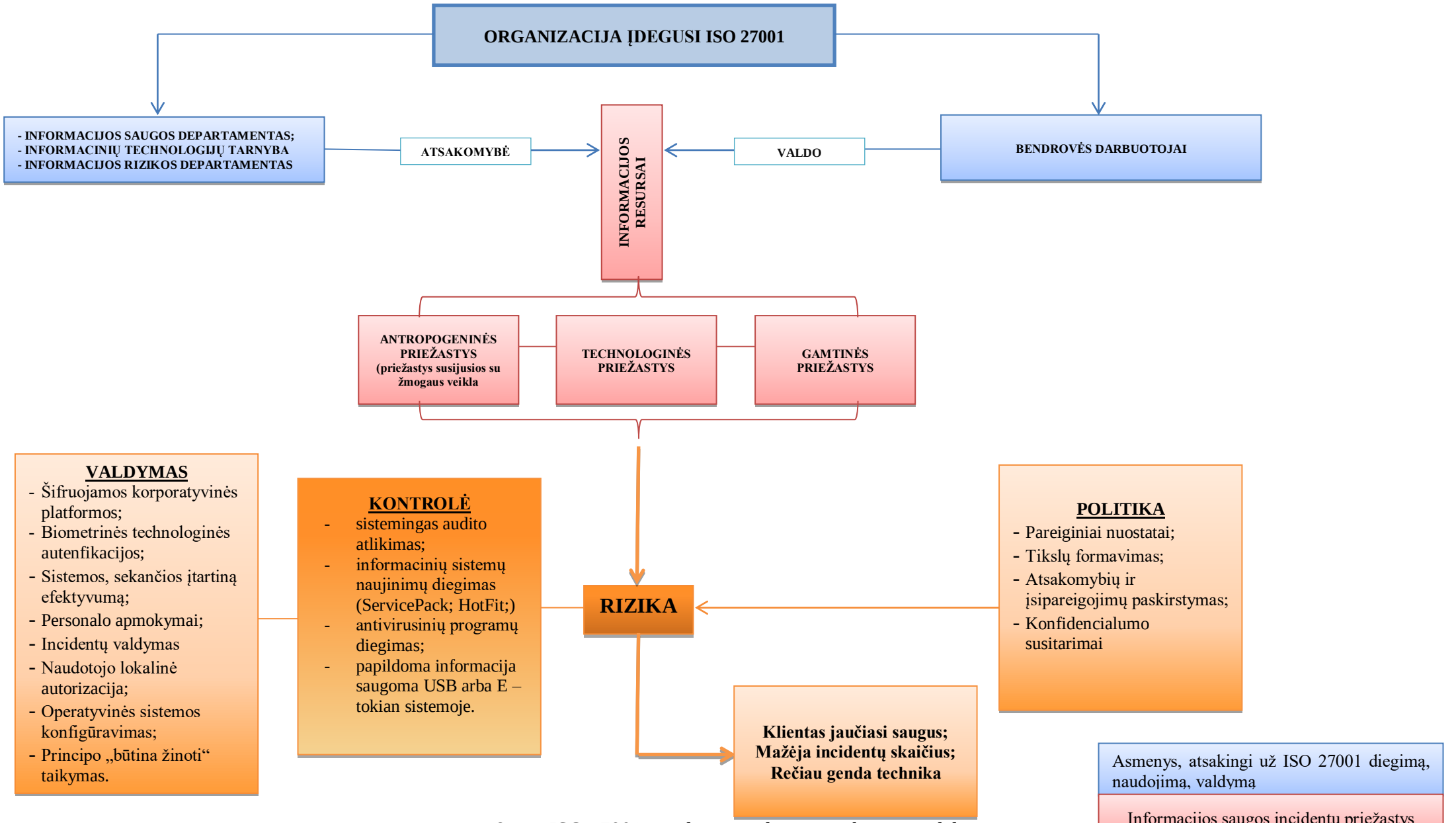
Antivirusinė programa yra atnaujinama iš karto, kai yra išleidžiami duomenų bazės atnaujinimai. IT skyriaus vadovas yra atsakingas už antivirusinės bazės atnaujinimą. Įmonėje vykdomas perimetro ir kiemo, gamybinių ir sandėliavimo patalpų vaizdo stebėjimas.

Lokaliniai tinklai tvarkomi pagal poreikį (reikalavimus), keičiant ar atnaujinant techninę ar programinę įrangą ar įvykus kokiems nors incidentams.

Sunku įvertinti rezultatus įdiegus ISO 27001, nes rezultatai nėra pamatuojami. Įdiegtos priemonės užtikrina informacijos saugą taip, kaip Bendrovė ir planuoja ją užtikrinti. Nebuvo nei vieno rimto informacijos praradimo ar atskleidimo, kritinių saugos incidentų per pastaruosius metus taip pat nėra užfiksuota. Vadybos sistema funkcionuoja kaip numatyta“.

Apibendrinant tyrimo rezultatus, buvo sukurta ISO 27001 tyrimo rezultatų schema, kurioje galima matyti, kad už informacijos saugą bendrovėse atsakingas specialiai sukurtas padalinys arba priskirtas atsakingas darbuotojas, tačiau informacinius resursus valdo visi darbuotojai prieinantys prie duomenų bazės.

Informacijos saugos valdymas vykdomas skirtingomis priemonėmis: šifruojamos korporatyvinės platformos, taikomos biometrinės technologinės autenfikacijos ir principas „būtina žinoti“, sistemos, sekančios įtartiną efektyvumą, valdomi incidentai, konfigūruojamos operatyvinės sistemos.



9pav. ISO 27001 standarto naudojimo praktinis modelis

Schemoje pateiktas tyrimo apibrėžimas remiasi kokybinio tyrimo rezultatais. Tyrimas buvo atliekamas apklausiant skirtingas veiklas vykdančias bendroves: medicinos įstaiga, bankas, leidykla, investicinis fondas. Pabrėžiama, kad ISO 27001 reikalavimai vykdomi visose nagrinėjamuose bendrovėse, tačiau reikalavimai vykdomi skirtingai: taikomos skirtingos priemonės: vienose bendrovėse tos priemonės paprastesnės, lengvai diegiamos, kitose sunkios technologinės priemonės.

3.5 Mokslinė diskusija ir ateities tyrimų kryptys

Tyrimo rezultatai visiškai atitinka mokslinius tyrimus; Markov, Cirlov, 2007; Kabay, 2002; Raikova, Šahalov, 2013; Dmitriev, 2013; Douglas, Landoll, 2011; Cosutic, 2017, Grigorjeva, Meškov, 2006 ir kt., respondentų teigimu, informacinės saugos standarto naudojimassuteikia galimybę bendrovėms pritraukti didesnį klientų kiekį, užtikrina klientų pasitenkinimą ir saugumą. ISO 27001 ne tik kokybės standartas – tai yra dar ir įmonės stilius. Bendrovės, diegiančios informacijos saugos standartus, dažniausiai yra didelės, turinčios daugybę padalinių, iš kurių vienas svarbiausias yra IT saugą užtikrinanti skyrius.Stebėtina, kad kiekvienoje bendrovėje taikomos skirtingos informacijos saugos priemonės, jos parenkamos atsižvelgiant į Bendrovės veiklos specifiką.

Empiriniame tyrime dalyvaujantys respondentai visiškai pagrindžia Markov ir Cirlov, 2007 tezę dėl informacijos saugos sistemos taikymo būtinumo esant šiuolaikiniam techniniam vystymui ir informacinių technologijų sparčiai sklaidai.

Respondentai, atsakant į interviu klausimus, irgi pažymi incidentų prognozavimo programų būtinumą, plačiai aprašo jų veikimo būdus. Kabay, 2002, Dvitriev, 2013, pabrėžia, kad maža įdiegti informacijos saugos sistemą, svarbu suvokti jos svarbą, prognozuoti galimus incidentus ir iš anksto numatyti jų šalinimo būdus.

Tyrimo metu buvo nustatyta, kad visi darbuotojai apklaustuose bendrovėse yra supažindinti su informacijos saugos aspektais, be to šios žinios periodiškai yra papildomos ir atnaujinamos, darbuotojai irgi yra informacijos saugos užtikrinimo garantai. Douglas, Landoll, 2011 pažymi, kad siekiant efektyviai valdyti informacinę riziką būtina didelį dėmesį kreipti į visus bendrovės darbuotojus, jų erudiciją informacijos saugos srityje.

Atlikus interviu tyrimą, reikšmingų skirtumų tarp teorinio (8 paveiksle) pateikto modelio ir tyrimo rezultatų nustatyta nebuvo, kadangi pats tyrimo klausimynas buvo sudarytas , remiantis 8 pav. pateiktu modeliu ir tyrimo metu analizuojami aspektai buvo analogiško pobūdžio, tačiau tyrimas atskleidė daug išsamesnę informaciją, sukonkretino kiekvieną 8 paveikslo bloką, remiantis praktikoje taikomais procesais, saugos priemonėmis ir t.t.

Tyrimo rezultatai suteikia pakankamai išsamią informaciją apie ISO 27001 naudojimą, tačiau, vienareikšmiškai yra žymiai daugiau naudojimo ypatumų. Būtų galima panagrinėti ISO 27001 standarto diegimą valstybinėse institucijose , pvz. tokias kaip registrų centrą, kadangi šis reiškinys nėra pakankamai išsamiai ištirtas. Baigiamojo darbo rašymo metu nebuvo rasta jokios medžiagos dėl ISO 27001 taikymo valstybės valdomose institucijose.

Dar vienas aspektas, kurio analizė reikalauja didesnio dėmesio yra visa informacijos saugos valdymo sistema ir jos naudojimas. Šiuo metu sistema apima:

- ISO / IEC 27000: 2009 "Informacinės technologijos. Saugumo užtikrinimo metodai. Informacijos saugumo valdymo sistemos“.
- ISO / IEC 27001: 2005 "Informacinės technologijos. Saugumo užtikrinimo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“.
- ISO / IEC 27002: 2005, "Informacinės technologijos. Saugumo užtikrinimo metodai. Informacinio saugumo valdymo kodeksas. Geriausiai praktiniai patarimai dėl informacijos saugumo valdymo.
- ISO / IEC 27003: 2010, "Informacinės technologijos. Saugumo užtikrinimo metodai. Informacijos saugumo valdymo sistemos įdiegimo vadovas.
- ISO / IEC 27004: 2009 "Informacinės technologijos. Saugumo užtikrinimo metodai ir priemonės. Informacijos saugumo valdymas. Matavimai: skirti informacinės saugos valdymo sistemos metrikai ir vertinimui.
- ISO / IEC 27005: 2011 „Informacinės technologijos. Saugumo užtikrinimo metodai. Informacijos saugumo rizikos valdymas.
- ISO / IEC 27006: 2011, "Informacinės technologijos. Saugumo užtikrinimo metodai. Reikalavimai įstaigoms, teikiančioms informacijos saugumo valdymo sistemų auditą ir sertifikavimą.
- ISO / IEC 27007: 2011. "Informacinės technologijos. Saugumo užtikrinimo metodai. auditavimo informacijos saugumo valdymo sistemų vadovas, kuriame aprašomi pagrindiniai informacijos saugumo reikalavimai;
- ISO / IEC TR 27008: 2011. "Informacinės technologijos. Apsaugos metodai. Vadovas informacijos saugumo valdymo auditoriui", kuria siekiama, visų pirma, patikrinti informacijos saugumo kontrolę ir glaudžiai susijusi su ISO / IEC 27002;
- ISO / IEC 27011: 2008, "Informacinės technologijos. Apsaugos metodai. ISO / IEC 27002 pagrįstų telekomunikacijų paslaugų organizacijų informacijos apsaugos valdymo gairės;
- ISO / IEC 27031: 2011, "Informacinės technologijos. Saugumo užtikrinimo metodai. Informacinių ir komunikacinių technologijų pasirengimo verslo tęstinumui gairės.

- ISO 27799: 2008 "Informatika visuomenės sveikatos srityje. informacijos saugumo valdymo sveikatai naudojant ISO / IEC 27002 ", pateikiami nurodymai dėl ISO / IEC 27002 įgyvendinant sveikatos priežiūros pramonėje.

IŠVADOS IR PASIŪLYMAI

IŠVADOS

1. Remiantis literatūros apžvalgos rezultatais galima daryti išvadą, kad ISO 27001 gali būti pateiktas modelio pavidalu. Šis modelis aprašo pagrindinius informacinės saugos valdymo procesus: kurių pagrindiniai: informacijos saugos ir atsakomybių už ją paskirstymas tarp darbuotojų, resursų valdymas, rizikos valdymas, dokumentacijos valdymas, vidaus auditų organizavimas, siekiant užtikrinti ISO 27001 reikalavimų vykdymą, informacinės saugos sistemos analizė ir jos tobulinimo galimybių numatymas. Modelyje aprašytos ir informacijos saugos užtikrinimo kryptys, kurių tarpe verta išskirti saugos politikos ir sistemos organizavimo būtinumą, personalo dalyvavimo būtinumą politikos vykdyme, techninių, prieigos ir informacijos saugos incidentų valdymo poreikį. Modelyje pateiktos ir saugos sistemos realizavimo gairės, kurios, remiantis moksline literatūra skaidomos į keturias grupes: organizacines, mokslines, programines, įrenginių.
2. Pusiau struktūruotas interviu yra tinkamas ISO 27001 naudojimo tyrimo įrankis, nes jo pagalba buvo atskleisti ISO 27001 serijos naudojimo praktiniai aspektai, buvo nustatytos priemonės, kurios taikomos informacijos saugai užtikrinti, atskleisti vidiniai ir išoriniai veiksniai, turintys įtakos, kaip neigiamos, taip ir teigiamos, bendrovių informacijos saugai.
3. Empirinio tyrimo rezultatų modelis atitinka Literatūros apžvalgos pagrindu sudarytą modelį. Tai leidžia daryti išvadą, kad ISO 27001 standartas bendrovėse naudojamas atsižvelgiant į visus jo taikymui nurodytus reikalavimus. Pagrindiniai reikalavimai yra vykdomi visose tyrime dalyvavusiuose bendrovėse, tačiau kiekviena įmonė šiuos reikalavimus vykdo savaip, taikant jos veiklai priimtinas priemones ir būdus
4. ISO 27001:2013 turi eilę privalumų organizacijoms, kurios jį įdiegė: suteikia galimybę nustatyti rizikas ir priimti veiksmus jų optimizavimui arba šalinimui, garantuoja adaptavimo lankstumą bet kuriai veiklos sferai, užtikrina klientų ir suinteresuotų asmenų pasitikėjimą. Atitikimas standartams garantuoja privilegijuoto tiekėjo statusą. Sertifikavimo vertė verslui taip pat atspindi griežtai apibrėžtas standarto eiliškumas, kuriame aprašyti saugos valdymo kūrimo procesai, metodologijos, instrumentai šablonai, kuriuos galima naudoti organizacijos praktikoje ne vieną kartą.

5. Remiantis tyrimo metu surinktų duomenų analizės rezultatais galima teigti, kad už informacijos saugą bendrovėse atsakingas specialiai sukurtas padalinys arba priskirtas atsakingas darbuotojas, tačiau informacinius resursus valdo visi darbuotojai prieinantys prie duomenų bazės. Informacijos saugos valdymas vykdomas skirtingomis priemonėmis: šifruojamos korporatyvinės platformos, taikomos biometrinės technologinės autenfikacijos ir principas „būtina žinoti“, sistemos, sekančios įtartiną efektyvumą, valdomi incidentai, konfigūruojamos operatyvinės sistemos, informacijos saugos kontrolė vykdoma sistemingai atliekant auditą, diegiant informacinių sistemų naujinimus, papildomai saugant duomenis išorinėse laikmenose. Galima teigti, kad informacijos saugos politika kuriama sudarant pareiginius nuostatus, formuojant konkrečius tikslus, paskirstant atsakomybes ir įsipareigojimus tarp bendrovės padalinių, pasirašant konfidencialumo sutartis.

PASIŪLYMAI

1. Remiantis gautais tyrimo rezultatais, siūloma kiekvienai bendrovei taikyti savo informacijos saugos naudojimo principus, prieš tai įvertinus įmonės veiklos analizę ir jos išskirtinumą, veiklos specifiką.
2. Parenkant naudojimo priemones būtina pasidomėti kokias saugos priemones naudoja analogiška veikla užsiimančios organizacijos, išanalizuoti jų privalumus ir trukumus.

LITERATŪROS SĄRAŠAS

1. Alsaquicy, D. (2013). A strategic approach to the implementation of management by objectives in the government sector in the sultanate of oman. Prieiga per internetą:http://usir.salford.ac.uk/30658/1/Mahmood_MPhil_FINAL_COMPLETED_26-11-2013.pdf (žiūrėta 2017 gegužės 1 dieną).
2. Cosutic, D. (2017). Four key benefits of ISO 27001 implementation. Prieiga per internetą: https://advisera.com/27001academy/knowledgebase/four-key-benefits-of-iso-27001-implementation/ (žiūrėta 2017 m. gegužės 16 dieną).
3. Douglas J.Landoll. (2011). *The security risk assessment hand book*, Second Edition. CRC Press.
4. Henry R. N. Deming's 14 Points for Management: Frame work for Success. Prieiga per internetą: http://www2.fiu.edu/~revellk/pad3003/Neave.pdf (žiūrėta 2017 m. gegužės 22 dieną)
5. Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (ISO/IEC 27001:2013)
6. Inter Cert (2017) Prieiga per internetą: http://www.intercert.kz/index.php?option=com_content&view=article&id=36:iso-27001&catid=8&Itemid=116&lang=ru (žiūrėta 2017 m. gegužės 20 dieną)
7. Juran, J. (1998). Juran‘s quality handsbook. Prieiga per internetą: http://www.pqm-online.com/assets/files/lib/books/juran.pdf (žiūrėta 2017 gegužės 17 dieną)
8. Kabay, M.E. (2002). What's Important for Information Security: A Manager'suide. Preiga per internetą: http://www.mekabay.com/infosecmgmt/mgrguidesec.pdf (žiūrėta 2017 m. gegužės 05 dieną)
9. Kumar, M. P., , Raju, N. V. S., Kumar, M. V. S., Quality of Quality Definitions – AnAnalysis. *International Journal of Scientific Engineering and Technology*. Prieiga per internetą: https://ijset.com/ijset/publication/v5s3/IJSET_2016_304.pdf (žiūrėta 2017 gegužės 17 dieną)
10. Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013. Prieiga per internetą: https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf (žiūrėta 2017 m. gegužės 25 dieną)
11. Pardo, C., Pino, F.J., Garcia, F. (2016). Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2. *Standards. International Journal of Software Engineering and Its Applications*, Vol. 10, No. 9, p. 217-230

12. Prof. Ishikawa and Quality Control. Prieiga per internetą: https://www.juse.or.jp/english/archives/pdf/Ch08_Ver2a_150803.pdf (žiūrėta 2017 m. gegužės 10 dieną)
13. RAI Technology University. Total Quality management. Prieiga per internetą: http://164.100.133.129:81/econtent/uploads/total_quality_management.pdf (žiūrėta 2017 gegužės 07 dieną)
14. Smen Bisgaard. Quality Engineering and Taguch Methods: A Perspective. Prieiga per internetą: http://www.ame.org/sites/default/files/target_articles/89Q3A2.pdf (žiūrėta 2017 gegužės 15 dieną).
15. Suarez, J.G. (1992) Three Expertson Quality Management: Philip B. Crosby W. Edwards Deming Joseph M. Juran. Prieiga per internetą: http://www.dtic.mil/dtic/tr/fulltext/u2/a256399.pdf (žiūrėta 2017 m. gegužės 15 d.)
16. Quality Engineering and Taguchi Methods: A Perspective. (1989). Prieiga per internetą: http://www.ame.org/sites/default/files/target_articles/89Q3A2.pdf (žiūrėta 2017 gegužės 07 dieną)
17. Quality Concepts. Cambridge University Press. Prieiga per internetą: http://assets.cambridge.org/97805215/15221/excerpt/9780521515221_excerpt.pdf (žiūrėta 2017 gegužės 08 dieną)
18. Васин, С. Г. (2017). *Управление качеством. Всеобщий подход*. Москва: Издательство Юрайт.
19. Григорьева, В. А., Мешков, В. И. (2006). *Управление информационной безопасностью предприятия на основе стандарта ISO 27001* .Национальный горный университет
20. Дмитриев, А., (2014). Определение контекста организации – базовый шаг внедрения системы менеджмента информационной безопасности. Prieiga per internetą: https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxpc28yN2NvbXxneDoxMTMyNjEzNTM4ZDI2NDZm (žiūrėta 2017 m. gegužės 06 d.)
21. Дмитриев, А., (2014). ISO/IEC 27001 – Путь к информационной безопасности. Особенности внедрения на отечественных предприятиях. Prieiga per internetą: https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxpc28yN2NvbXxneDo0ODBkMTY0NjgxZGMwOTE5 (žiūrėta 2017 m. gegužės 06 d.)

22. Дорофеев А.В. Марков А.С. (2014). Менеджмент ИБ: основные концепции. *Вопросы кибербезопасности,* nr. 1(2), с.67-73.
23. Кузнецова, Н. В. (2013). *Управление качеством*. Москва: Флинта, Наука
24. Лагуткина, Т.П. (2008). Принципы управления качеством в деятельности аптечной организации. (žiūrėta 2017 m. gegužės 22 dieną)
25. Марков, А.С., Цирлов, В.Л. (2007), Управление рисками –нормативный вакуум информационной безопасности. *Открытыесистемы. СУБД, nr. 8,* с. 63-67.
26. Марков, А.С., Цирлов, В.Л. (2012). *Методы оценки несоответствия средств защиты информации.*Москва: Радио и связь.
27. Международные стандарты ИСО серии 9000 и статистические методы. (2006). Сборикматериалов 13-ой международной конференции. Нижний Новгород : Приоритет, 2006
28. Николаева,Э.К. (2004).*Семь инструментов качества в японской экономике.* Санкт Питербург: Нева
29. Овсянко Д.В. (2011). *Управление качеством.* Санкт Питербург: Высшая школа менеджмента
30. Пронников, В.А., Ладанов, И. Д. (2004). *Управление качеством в Японии.* Москва: БЕК
31. Райкова, Н. О. (2013). Об интеграции систем менеджмента информационной безопасности и качества. *Вопросы кибербезопасности*, nr. 3, с. 47-53
32. Райкова Н.О., Шахалов И.Ю. (2013). Сравнение ISO/IEC 27001:2005 И ISO/IEC 27001:2013. Prieiga per internetą: http://www.itstandard.ru/Soderganie_gurnalov/%D0%A1%D0%A0%D0%90%D0%92%D0%9D%D0%95%D0%9D%D0%98%D0%95%20ISO.IEC%2027001.2005%20%D0%98%20ISO.IEC%2027001.2013.pdf (žiūrėta 2017 m. gegužės 17 dieną)
33. Тебекин, А. В. (2017). *Управление качеством*. Москва: Издательство Юрайт,
34. Фрейдина Е. В. (2012). *Управление качеством*. Москва: Омега-Л,
35. Цирлов, В.Л. (2008). *Основы информационной безопасности.* Ростов на Дону: Феникс
36. Цирлов, В.Л., Марков, А.С. Управление рисками – нормативный вакум информационной безопасности. *Открытие системы. СУБД.*нр. 8, с. 63-67
37. Чекмарев, А.И.(2007).Оценка качества продукции на динамически развивающихся рынках. *Москва: РИА "Стандарты и качество"* nr. 12,с. 31-37.

38. Чобанян, В.А., Шахалов, И.Ю. (2013). Анализ и синтез требований к системе безопасности критической информационной инфраструктуры. *Вопросы кибербезопасност, ,*nr.1(1), с. 17-27
39. Шахалов, И.Ю.,Дорофеев, А.В. (2013). Основы управления информационной безопасностью современной организации. *Правовая информатика*, Нр. 3, с. 4-14
40. Шахалов И.Ю. (2012). *Лицензирование в области защиты информации: новые требования.*Сочи: Инфо Берег
41. Шестопал, Ю.Т. (2010). Конкурентоспособность и качество. *Стандарты и качество, nr.* 2, с. 62-65.
42. Шонбергер, Р. (2003). *Японские методы управления производством.* Москва: Экономика.

INFORMACIJOS SAUGOS VADYBOS SISTEMOS NAUDOJIMO YPATUMAI

Margarita STRAŽNICKIENĖ

Magistro darbas

Kokybės vadybos programa

Vilniaus universiteto Ekonomikos fakulteto Vadybos katedra

Darbo vadovas: asistentas D. Ruželė

Vilnius, 2018

SANTRAUKA

59 puslapiai, 6 lentelės, 9 paveikslai, 42 literatūros šaltinių nuorodos.

Magistro darbo tikslas: Atlikus tyrimą, nustatyti standarto ISO 27001:2013 naudojimo ypatumus.

Darbo tikslui pasiekti buvo keliami ir įvykdyti trys uždaviniai:

1. Atlikus mokslinės literatūros analizę, suformuoti ISO 27001 naudojimo teorinį modelį;
2. Atlikus pusiau struktūrinio interviu tyrimą, nustatyti standarto naudojimo praktinius aspektus.
3. Susisteminus interviu turinio rezultatus sukurti ISO 27001:2013 standarto naudojimo Lietuvos bendrovėse praktinį modelį.

Darbe naudojami tokie tyrimo metodai, kaip: mokslinės literatūros analizė, duomenų lyginamoji analizė, pusiau struktūrinis ekspertų interviu, duomenų sisteminimas ir interpretavimas.

Literatūros analizė atskleidė, kad ISO 27001 gali būti efektyviai integruotas į egzistuojančias kokybės valdymo sistemas arba vykdomas kartu su jomis. Mokslinės literatūros analizė padėjo pagristi lengvą ISVS pritaikomumą naujovėms modernizuojant esamas ar diegiant naujas atsakomąsias priemones. Pabrėžiama, jog ISO 27001 reikalauja, griežto sąlygų laikymosi, informacijos saugos kontrolė vykdoma sistemingai atliekant auditą, diegiant informacinių sistemų atnaujinimą, papildomai saugant duomenis išorinėse laikmenose. Bendrovėse saugos politika kuriama sudarant pareiginius nuostatus, formuojant konkrečius tikslus, paskirstant atsakomybes ir įsipareigojimus tarp bendrovės padalinių, pasirašant konfidencialumo sutartis.

Baigiamajame darbe buvo taikytas kokybinis empirinis tyrimas. Su įmonių atstovais, kuriuose naudojamas ISO 27001 standartas buvo atliktas interviu tyrimas, kurio metu buvo nustatyti standarto naudojimo ypatumai. Tyrimo pagalba buvo atskleisti ISO 27001 serijos naudojimo praktiniai aspektai, buvo nustatytos priemonės, kurios taikomos informacijos saugai užtikrinti, atskleisti vidiniai ir išoriniai veiksniai, turintys įtakos, kaip neigiamos, taip ir teigiamos, bendrovių informacijos saugai. Tyrimas padėjo atskleisti informacijos sagos politikos įgyvendinimo kryptis, priemones, politikos formavimo gaires.

Tyrimo metu paaiškėjo, kad ISO 27001:2013 turi eilę privalumų organizacijų veiklai: suteikia galimybę nustatyti rizikas ir priimti veiksmus jų optimizavimui arba šalinimui, garantuoja adaptavimo lankstumą bet kuriai veiklos sferai, užtikrina klientų ir suinteresuotų asmenų pasitikėjimą. Atitikimas standartams garantuoja privilegijuoto tiekėjo statusą. Sertifikavimo vertė verslui taip pat atspindi griežtai apibrėžtas standarto eiliškumas, kuriame aprašyti saugos valdymo kūrimo procesai, metodologijos, instrumentai šablonai, kuriuos galima naudoti organizacijos praktikoje ne vieną kartą.

Reikšmingi žodžiai: ISO 27001,informacijos sauga, kokybės sistema,naudojimas, priemonės, taikymas, standartas.

PECULIARITIES OF USE INFORMATION SECURITY MANAGEMENT SYSTEMS

Margarita STRAŽNICKIENĖ

Paper for the Master's thesis

Quality Management Master's Program

Vilnius University, Faculty of Economics, Management Department

Supervisor – prof. J. Ruževičius

Vilnius, 2018

SUMMARY

59 pages, 6 charts, 9 pictures, 42 references

The aim of Master's Thesis: To determine the peculiarities of using the standard ISO 27001: 2013.

To achieve the aim of Master's Thesis were raised three objectives:

1. Analyze scientific literature, and form the theoretical model for peculiarities of using the standard ISO 27001;
2. Perform a semi-structured interview study and determine the practical aspects of using the standard.
3. Systematize the results of the interviews and create a practical model for using the standard ISO 27001: 2013 in Lithuanian companies.

In Master's Thesis are used such research methods as: analysis of scientific literature, data comparative analysis, semi-structured expert interviews, data systematization and interpretation.

Literature analysis reveal that ISO 27001 can be effectively integrated with existing quality management systems or implemented with them. The analysis of scientific literature helped to base easy adaptation of ISMS to innovations by modernizing existing ones or introducing new countermeasures. It is emphasized that ISO 27001 requires strict conditions compliance, information security control is carried out by systematic audit, installing information system updates, additional storage of data on external media. Company's safety policy is developed through the establishment of job regulations, shaping specific goals, distributing responsibilities and obligations between the company's departments, by signing confidentiality agreements.

In Master's Thesis was applied qualitative empirical study. An interview was conducted with representatives of companies using the ISO 27001 standard, which identified the peculiarities of using the standard.

The study helped to uncover the practical aspects of using the ISO 27001 series; measures were taken to ensure the safety of information, to reveal internal and external factors that have an impact on both the negative and the positive safety of company information. The study helped to reveal the directions, tools, policy making guidelines of the information guidelines.

The study revealed that ISO 27001: 2013 has a number of benefits for organizations: it allows identify the risk and action to optimize or eliminate them, ensures adaptation flexibility for any field of activity, ensures the confidence of clients and stakeholders.

Key words: ISO 27001, information security, quality system, use, tools, standard application.

PRIEDAI

Priedas Nr. 1. Klausimynas

1. Kokia organizacinė struktūra vyrauja organizacijoje?
2. Kas atsakingas už informacijos saugą?
3. Kas valdo informacinius resursus?
4. Su kokia informacijos rizika buvo susidurta, kaip rizika buvo valdoma?
5. Kaip veikia sistemos kontrolės sistema?
6. Kaip gerinama informacijos saugos sistema? Kaip dažnai jį tobulinama?
7. Trumpai apibūdinkite organizacijos saugos politiką bei saugos sistemos organizavimo procesus?
8. Kaip užtikrinama vidinė ir išorinė informacijos apsauga, kas atsakingas už jos užtikrinimą?
9. Kaip valdomi kompiuteriai, tinklai, prieiga prie sistemų?
10. Kaip kuriama, derinama ir aptarnaujama informacinę sistemą, valdo informacijos saugos incidentus, kaip tai vykdoma?
11. Kas stebi standarto atitikimą norminiams teisės aktams?
12. Kokias informacijos saugos priemones naudojate praktikoje?
13. Jūsų darbuotojai yra supažindinti su ISO/IEC 27001:2013 reikalavimais, kaip dažnai vykdomi apmokymai ta tema, kaip dažnai?
14. Kaip dažnai atnaujinama antivirusinė programinė įranga, kas už tai atsakingas.
15. Jūsų bendrovės teritorijoje yra kameros?
16. Kaip dažnai remontuojami lokaliniai tinklai? Kas tuos darbus atlieka? Kaip dažnai atliekamas remontas?
17. Kokie rezultatai buvo pasiekti realizavus saugos priemones?
18. Kokia veiklą vykdo Jūsų atstovaujama bendrovė?
19. Kokias pareigas užimate?
20. Jūsų bendrovėje įdiegta ISO/IEC 27001:2013?
21. Jūsų bendrovėje yra įdiegti kiti ISO standartai?
22. Kokie sunkumai kilo diegiant ISO 27001:2013 standartą?