MYKOLO ROMERIO UNIVERSITETAS

VERSLO IR MEDIJŲ MOKYKLA
(BUSINESS AND MEDIA SCHOOL (BMS))

PAULIUS PELENIS
Kibernetinio saugumo valdymas
Studijų programa 141622

KIBERNETINIO SAUGUMO UŽTIKRINIMO ĮTAKA VERSLO PROCESAMS

Magistro baigiamasis darbas

Darbo vadovas-
prof. dr. Darius Štitilis

Konsultantas-
stud. Paulius Pelenis

VILNIUS, 2015

MYKOLAS ROMERIS UNIVERSITY
BUSINESS AND MEDIA SCHOOL

PAULIUS PELENIS
Cyber security mamagement
Study program 141622

THE INFLUENCE ENSURING CYBER SECURITY IN BUSINESS PROCESSES

Master Thesis

Supervisor: prof. dr. Darius Štitilis

Consultant:stud. Paulius Pelenis

VILNIUS, 2015

TURINYS

ĮVADAS....4
1. KIBERNETINIO SAUGUMO SAMPRATA, KIBERNETINIO SAUGUMO CHARAKTERISKOS IR YPATUMAI....8
1.1. KIBERNETINIO SAUGUMO SAMPRATA....8
1.2. KIBERNETINIO SAUGUMO PROBLEMATIKA....15
2. VERSLO PROCESŲ IR KIBERNETINIO SAUGUMO SĄSAJOS....23
2.1 VERSLO PROCESŲ SAMPRATA....23
2.2 VERSLO PROCESŲ VALDYMAS....28
2.3 KIBERNETINIO SAUGUMO SVARBA VERSLO PROCESUOSE....32
3.KIBERNETINIO SAUGUMO UŽTIKRINIMO ĮTAKA VERSLO PROCESAMS....41
3.1 PAGRINDINIAI VEIKSNIAI LEMIANTYS INFORMACIJOS IR KIBERNETINĮ SAUGUMĄ VERSLO PROCESUOSE....41
3.2. KIBERNETINIO SAUGUMO VALDYMAS VERSLO PROCESUOSE....47
4. DUOMENŲ IR INFORMACIJOS SAUGUMO ORAGANIZACIJOSE ANALIZĖ....49
4.1.TYRIMO METODOLOGIJA....49
4.2. TYRIMO REZULTATAI....51
IŠVADOS....67
REKOMENDACIJOS....70
LITERATŪROS SĄRAŠAS....71
SANTRAUKA....75
SUMMARY....76
PRIEDAI....77
1 PRIEDAS. Anketos pavyzdys....78

ĮVADAS

Temos aktualumas: Terminas „kibernetinis saugumas“ yra populiarus akademinių tyrinėjimų objektas, kuris labiausiai tyrėjus domina iš savo praktinės perspektyvos. Kibernetinis saugumas svarbus ne tik šaliai ir valstybei, bet ir kiekvienam individualiam vartotojui. Taip yra todėl, kad vis labiau paprasti piliečiai naudojasi elektroninėmis ryšių priemonėmis: elektronine bankininkyste, elektroninės komercijos prekybos priemonėmis, socialiniais tinklais ir neišvengiamai susiduriama su kibernetinių tinklų apsaugos reikalingumu. Vis labiau įžūlėjantys kibernetiniai nusikaltimai, kurių metu paveikiamos svarbios visuomenei sritys, tokios kaip: elektros tiekimas, naftos ir dujų gavybos sritys, vandens valdymas ir pasiskirstymas, banko paslaugų tiekimas akcentuoja, kad kibernetinis saugumas ir jo užtikrinimas yra labai svarbus tiek nacionaliniu, tiek ir individualiu mastu.

Egzistuoja daugelis technologijų, kurios gali stipriai pažeisti informacines technologijas, tai dažniausiai būna techniniai gedimai ir virusai. Šiuos gedimus, kurių vyksmas vis dažnėja darosi sunkiau įveikti. Informacinių sistemų gedimai turi didelį poveikį paslaugų tiekimui, o jam sutrikus įmonės negali tinkamai funkcionuoti. Kibernetinės atakos mažina vartotojų pasitikėjimą internetu ir informacinėmis technologijomis. Labai svarbu užtikrinti sklandų tinklų veikimą, kad nuo informacinių technologijų priklausantys įvairūs sektoriai veiktų ne tik sklandžiai, bet būtų patikimi ir stabilūs. Tam pasiekti nuosekliai ruošiamos įvairios kibernetinio saugumo strategijos nacionaliniu ir ES lygiu.

Tyrėjai rengia kibernetinio saugumo plėtojimo strategijas, kurios turėtų būti remiamos vyriausybės: užtikrinti sukauptų tam tikro proceso duomenų konfidencialumą, vientisumą ir prieinamumą kurie galėtų būti naudojami tik tam tikrą ribotą laiką; nustatyti duomenų kilmę ir istoriją, jų patikimumą ir įvertinti nepatikimoje aplinkoje; plėtoti saugumo rodiklius.

Informacijos apdorojimo procesai, kurie yra paremti informacinių ir ryšių technologijų pagrindu kartu su internetu sudaro kibernetinę erdvę. Kadangi vis daugiau informacijos perkeliama į elektroninę erdvę tai lėmė, kad kibernetinė erdvė tapo kibernetinių nusikaltimų taikinys. Kibernetinių incidentų sparčiai daugėja. Kibernetinė ataka yra elektroninių informacinių sistemų puolimas naudojant įvairias technologines priemones. Įvairios naujosios technologijos smarkiai įtakoja ir verslo procesus.

Chaotiškas verslo procesas nėra teigiamas reiškinys šiuolaikinėje rinkoje. Todėl verslo procesus valdyti yra būtina. Verslo procesas gali būti suprantamas kaip tam tikros veiklos rinkinys, kuris naudoja vienokius ar kitokius išeities duomenis, išteklius, kurie yra vertingi pirkėjui. Verslo procesas gali apimti daug elementų, tokių kaip: verslo proceso valdymas, darbo pasidalinimas,

užduočių vykdymas, kokybines verslo proceso charakteristikos. Informacinių technologijų apsuptyje verslo procesas yra visuma priemonių susijusių su verslo proceso įgyvendinimu. Tai galėtų būti programinė įranga, kompiuterinė infrastruktūra, elektroninės parduotuvės ir bankininkystės sistemos, duomenų perdavimo infrastruktūra. Yra labai svarbus daugeliui verslo įmonių ir organizacijų nes gerina procesų, susijusių su internetine erdve kokybiškumą, konkurencingumą ir prieinamumą. Taikydama naująsias technologijas įmonė tampa labiau globalesnė, gali supaprastinti verslo procesus, atrasti daugiau nišų savo veiklai internetinėje erdvėje, administruoti savo darbuotojų veiklą. Būtina užtikrinti kibernetinį saugumą įmonėse, nes gali būti prarandama elektroninė informacija.

Nacionalinio elektronikos ryšių tinklų ir informacijos saugumo tyrimo padalinio duomenimis 2014 metais kibernetinių nusikaltimų skaičius Lietuvoje siekė virš 36 tūkstančių, o lyginant su ankstesniais metais, išaugo virš 43 proc. Didžiausia kibernetinio saugumo problema ne tik Lietuvoje, bet ir visame pasaulyje yra tai, kad daugybė kibernetinių įrenginių turi saugumo spragų.

Atsižvelgiant į literatūros analizę ir įvairių mokslininkų keliamus tikslus Lietuvoje svarbu stiprinti ne tik kibernetinio saugumo įstatymus, bet ir aktyvinti privataus ir viešojo sektoriaus iniciatyvas bendradarbiaujant tarpusavyje stiprinti ir užtikrinti kibernetinį saugumą.

Temos naujumas ir mokslinis ištirtumas: iki šiol mokslinėje literatūroje kibernetinis saugumas bei jo įtaka verslo procesams nėra plačiai nagrinėjamas. Temos atžvilgiu naudingi D.Štitilio ir Ž.Paškausko darbai (Štitilis, Paškauskas, 2007), kur nagrinėjamas kibernetinio saugumo teisinis reglamentavimas ir įvairios tarptautinės strategijos. Verslo procesai ir su jais susijusios strategijos bei naujųjų technologijų taikymas verslo procesuose nagrinėjamas R.Kontrimo, S.Valentinavičiaus, S.Juodaičio darbuose. Užsienio mokslininkai yra linkę labiau gilintis į informacinių saugos sistemų diegimą (F.Bjorck (2002), P.Fung, E.Jordan (2002) darbai), verslo procesus atskirai (D.J.Elzinga (2007), B.Hommes (2000) darbai). Vertingi pastaruoju metu (2013-2014 m.) užsienyje atlikti C.Schou, S.Hernandez (2014) bei C.Canongia, R. Mandarino (2014) atlikti kompleksiniai tyrimai, kuriuose kibernetiniam saugumui skiriamas ypatingas dėmesys, nagrinėjama kibernetinio saugumo ir verslo procesų sąveika. Vis dėlto paskutinieji temos atžvilgiu aktualūs tyrimai Lietuvoje atlikti dar 2008-2011 m., o Lietuvos mastu kibernetinis saugumo ir verslo procesų sąsajos, informacinių technologijų poveikis verslui ir su juo susijusiais procesais bendrame kontekste nėra nagrinėtas. Darbo rezultatai leis įvertinti šiuos ypatumus ir kylančias procesines problemas, o tai savo ruožtu leidžia konstatuoti darbo temos naujumą.

Temos problematika: Kibernetinio saugumo užtikrinimas yra labai svarbus verslo procesams. Literatūroje pateikiama verslo proceso samprata teigia, kad tai yra tam tikra veiklos seka susieta ryšių, kurie yra reikalingi norint sukurti produktą ar paslaugas. Pateikiamas informacijos saugumo tikslas apibrėžia informacijos konfidencialumą ir prieinamumą. Literatūroje pateikiamos informacijos saugumo sampratos leidžia suprasti, kad kibernetinio saugumo sąvoka formavosi veikiant technologinėms informacinėms problemoms. Tačiau mokslinėje literatūroje kibernetinio saugumo užtikrinimo ir verslo procesų sąsajų ir analizių moksline tematika pateikiama gana nedaug. Svarbu apibrėžti ne tik kibernetinio saugumo sampratą, pagrindines charakteristikas bet ir atskleisti sąveiką ir jos poveikį verslo procesams. Norint apsaugoti informaciją būtina pasitelkti informacines saugos priemones. Mokslinėje literatūroje pateikiamos ir analizuojamos įvairios informacijos saugojimo metodikos, standartai ir strategijos. Darbe taip svarbu išnagrinėti klausimus, susijusius su informacijos ir kibernetine sauga bei verslo procesais. Neretai kibernetinio saugumo priemonių taikymas tapatinamas su elektroninių duomenų, informacijos sauga, todėl iki šiol Lietuvos įmonėse pakankamai sudėtinga nustatyti kibernetinio saugumo priemonių taikymo intensyvumą ir paplitimą. Tai savo ruožtu apsunkina verslo procesų saugą kibernetinio saugumo prasme: nepakankamai įvertinamos galimos grėsmės, galimi incidentai bei jų pasekmės tiek įmonės, tiek valstybiniu mastu.

Darbo objektas: Kibernetinio saugumo poveikis verslo procesams.

Darbo tikslas: Įvertinti kibernetinio saugumo užtikrinimo poveikį verslo procesams.

Darbo hipotezė: Kibernetinis saugumas užtikrina teigiamą ir sklandžią verslo procesų veiklą.

Darbo uždaviniai:

1) Atskleisti kibernetinio saugumo sampratą, pagrindines kibernetinio saugumo charakteristikas bei problematiką;
2) Apžvelgti ir pateikti pagrindines verslo procesų sampratas, jų asociacijas su kibernetiniu saugumu;
3) Atlikus mokslinės literatūros apžvalgą aptarti pagrindinius kibernetinio saugumo užtikrinimo kriterijus ir aspektus, kurie labiausiai įtakoja verslo procesus
4) Atlikti kokybinį kibernetinio saugumo poveikio įvertinimo tyrimą organizacijose. Išanalizuoti ir susisteminti rezultatus, koks yra duomenų ir kibernetinio saugumo lygis organizacijose

Darbo metodai:

Nagrinėjant kibernetinio saugumo užtikrinimo įtaką verslo procesams problematiką bei formuojant šio darbo išvadas bus remiamasi analizės, aprašomuoju, lyginamuoju istoriniu, loginiu, lyginamuoju, sisteminiu metodais.

Analizės metodas bus naudojamas apžvelgti kibernetinio saugumo užtikrinimo įtakos verslo procesams pagrindines sampratas.

Aprašomasis metodas yra naudojamas pateikti kibernetinio saugumo ir verslo procesų pagrindines charakteristikas ir tarpusavio sąveikas.

Lyginamasis metodas naudojamas atskleisti kibernetinio saugumo poveikį verslo procesams, lyginamos šių dviejų sąvokų pagrindinės charakteristikos ir tarpusavio poveikiai.

Loginis metodas būtinas atskleidžiant bet kokio mokslinio tiriamojo darbo tikslus, aiškinantis pateikiant išvadas bei apibendrinimus.

Sisteminis metodas naudojamas darbe aptariant ir analizuojant kibernetinio saugumo užtikrinimo poveikio verslo procesams mokslinės literatūros analizės sisteminimą.

Darbo struktūra:

Pirmojoje darbo dalyje atskleidžiama kibernetinio saugumo samprata, pagrindžiamos kibernetinio saugumo charakteristikos ir ypatumai. Antrojoje darbo dalyje įvertinamos verslo procesų ir kibernetinio saugumo sąsajos, aptariama verslo procesų samprata, valdymas, saugumo svarba verslo procesams. Trečiojoje dalyje pristatoma kibernetinio saugumo užtikrinimo verslo procesuose specifika: nustatomi pagrindiniai veiksniai, lemiantys informacijos saugumą verslo procesuose, kibernetinio saugumo valdymo etapai. Ketvirtojoje dalyje atliekama kibernetinio saugumo analizė pasirinktose mažose ir vidutinio dydžio įmonėse: pristatoma tyrimo metodika ir rezultatai.

1. KIBERNETINIO SAUGUMO SAMPRATA, YPATUMAI IR PROBLEMATIKA

Šiame skyriuje siekiant tinkamai įvertinti kibernetinio saugumo sampratą, įvertinamas informacijos saugumo poreikis, saugumo garantijos problematika bei specifika. Informacijos saugumas turėtų būti suprantamas kaip pamatas kibernetiniam saugumui, todėl būtina įvertinti saugą garantuojančias priemones, procedūras, organizacines struktūras bei programinės įrangos funkcijas.

1.1. KIBERNETINIO SAUGUMO SAMPRATA

Terminas kibernetinis saugumas ilgą laiką buvo populiarus akademinių tyrimų objektas. Remiantis visa susisteminta literatūra apie kibernetinį saugumą matyti, kad terminas yra gana dažnai vartojamas ir plačiai apibrėžiamas, kurio sąvoka yra gana kintanti, nes su kibernetiniu apibrėžimu susijusios sąvokos yra gana subjektyvios o kartais ir visai neinformatyvios.

Kibernetinio saugumo sąvoka paplitusi praeitojo amžiaus pabaigoje pirmiausia apibrėžė technologinius kompiuterių pažeidimus. Vėliau šią sąvoką imta naudoti norint apibrėžti neigiamą poveikį visuomenei, kuris kyla dėl skaitmeninių technologijų pažeidimų.

Glaustų ir plačiai priimamų terminų apie kibernetinį saugumą nebuvimas, kurie jį apibrėžia, trukdo stiprinti mokslo ir technologijų pažangą, kuri siekia išspręsti sudėtingas kibernetinio saugumo iššūkius. Pavyzdžiui, egzistuoja techniniai sprendimai, kurie palaiko elektroninį saugumą. Vis dėl to šie pavieniai sprendimai neužtikrina problemos sprendimo. Egzistuoja daug pavyzdžių ir nemaža mokslo darbų, kurie atskleidžia kibernetinio saugumo problemas, susijusias su organizacijų ekonominiais, socialiniais, politiniais ir kitokiais aspektais (Goodall, Lutters ir kt., 2009).

Tyrėjo M.D.Cavelty (2012) teigimu, „*kibernetinis saugumas gali būti suprantamas kaip sritis kuri tarpusavyje apjungia skirtingus diskursus*“. Terminas „kibernetinis saugumas“ gali būti suprantamas kaip tam tikras dviejų žodžių „kibernetinis“ ir „saugumas“ susijungimo sričių erdvė, kuri atskleidžia bendrus šiems terminams klausimus. Terminas „kibernetinis“ nurodo terminą susijusį su kibernetine erdve, bei atspindi virtualios realybės ir elektroninių tinklų ryšių sąveiką.

Terminas „kibernetinė erdvė“ buvo išplatintas tyrėjo W.Gibson (2008) pasirodžiusiame darbe, kuriame jis aprašo kibernetinę erdvę kaip trimatę erdvę, kurioje cirkuliuoja informacija, kuri perduodama tarp kompiuterio vartotojų ir informacijos klasterių, kur žmonės yra suvokiami kaip informacijos vartotojai. Pagal Kanados viešojo saugumo organizaciją „kibernetinė erdvė“ yra apibrėžiama kaip „*elektroninis pasaulis, kuris sukuriamas tarpusavyje susijungus informacinėms*

technologijoms tinkluose“ (Buzan, et. Al., 1997). Panašiai „kibernetinę erdvę“ apibrėžia tyrėjai R.Deibert ir R.Rohozinski, kurie teigia kad ji „*nėra statiška; tai yra dinamiška, besivystanti, daugiapakopė fizikinės infrastruktūros ekosistema, ji apima programinę įrangą, reglamentus, idėjas, inovacijas ir tarpusavio vartotojų ryšius*“ (Deibert, Rohozinski, 2010). Kibernetinė erdvė gali būti apibrėžiama kaip tam tikra sritis, kuri apima elektroninių ir elektromagnetinių signalų spektrą, kuris reikalingas kaupti ir dalintis informacija per tam tikrą sistemų tinklą. Tokią sąvoką pateikė Jungtinių Amerikos Valstijų gynybos departamentas.

Terminas „saugumas“ literatūroje aiškiai apibrėžia B.Buzan, kurio teigimu *„saugumas apima ir siekia suprasti saugumo (grėsmių) klausimus, kuriuos jie siekia užtikrinti*“ (Buzan, 1997). Pagal Oksfordo žodyną tai yra terminas, kuris siekia užtikrinti laisves nuo gresiančio pavojaus.

Atlikus literatūros analizę, galima pateikti susistemintas kibernetinio saugumo sąvokas, kurios pateikiamos 1 lentelėje.

1 lentelė. Kibernetinio saugumo sąvoka ir jos variacijos

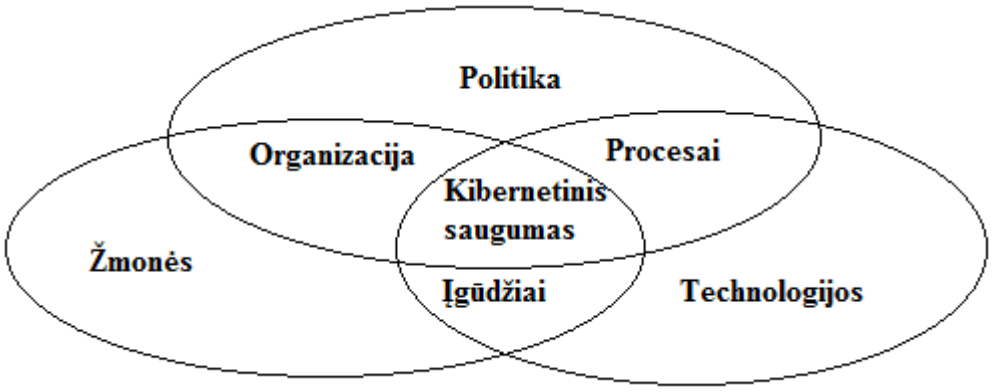
Autorius	Apibrėžimas (sąvoka)
Kemmerer (2003)	Kibernetinis saugumas apima būdus ir metodus, kurie apibrėžia kaip aptikti ir apsisaugoti nuo kibernetinių įsibrovėlių.
Lewis (2006)	Kibernetinis saugumas apibrėžia kompiuterinių tinklų ir informacijos apsaugą nuo įsibrovėlių ir tyčinės žalos darymo, trikdymo.
Amoroso (2006)	Kibernetinis saugumas apima ir siekia sumažinti kenksmingą pavojų prieš programinės įrangos, kompiuterinių tinklų atakas. Taip pat jis apima naudojamus aptikti įsilaužėliams įrankius, prieigas virusų plitimų sustabdymui, užtikrinti autentiškumą, bei saugų ryšį.
ITU (2009)	Kibernetinis saugumas yra tam tikrų įrankių visuma, apimanti politikos, saugumo užtikrinimo gaires, rizikos valdymo metodus, veiksmus, mokymus, technologijas kurios gali būti naudojamos siekiant apsaugoti kibernetinę aplinką jos organizavimą ir vartojimo informaciją.
Kanados viešojo saugumo organizacija (2014)	Kibernetinis saugumas gali būti laikomas kaip technologijų, procesų, procedūrų kūnas, kuris skirtas apsaugoti kompiuterinius tinklus, kompiuterius, programas ir duomenis nuo atakų, sugadinimų ar neleistinų priėjimų, kad būtų užtikrintas konfidencialumas ir prieinamumo vientisumas.
Canonigia, Mandarino (2014)	Kibernetinis saugumas suvokiamas kaip tautos informacinės visuomenės egzistavimo užtikrinimas ir tęstinumas, garantuojant ir apsaugojant elektroninę erdvę, jos informaciją, turtą bei ypatingos svarbos infrastruktūrą.
DHS (2014)	Kibernetinis saugumas yra procesas, veikla arba būsena pagal kurią informacijos ir ryšių sistemos yra saugomos nuo sugadinimo, neteisėto naudojimo ar modifikuotų pakeitimų.

(sudaryta autoriaus, 2015)

Bendrai vertinant mokslininkų pateikiamus kibernetinio saugumo sąvokos variacijas, konstatuotina, jog dauguma jų kibernetinį saugumą vertina dvejopai: orientuojamasi į

technologinius sprendimus (Kemmerer (2003), Kanados viešojo saugumo organizacija (2014)), įrankius (ITU (2009), Amoroso (2006)) arba pateikiami konceptualios sąvokos (Canonigia, Mandarino (2014), DHS (2014)). Vis dėlto, visos sąvokos grindžiamos apsauga nuo įsibrovėlių ir galimos žalos, konfidencialumo siekiu ir garantija, prieinamumo siekiu.

Pagal tyrėjo Rosentalio kibernetinio saugumo užtikrinimo programą, kibernetinio saugumo apibrėžimas gali būti sudaromas remiantis kertinėmis sąvokomis, kurios pateikiamos 1 paveiksle.



1 pav. Kibernetinio saugumo samprata pagal Rosentalio kibernetinio saugumo užtikrinimo programą

Pateiktame 4 paveiksle iliustruojama kibernetinio saugumo sampratos sudėtingumas, kuris apima daug sudėtingų elementų. Gali būti išskiriami esminiai elementai, kurie apibrėžia kibernetinį saugumą. Šie elementai yra politika, organizavimas, procesai, žmonės, įgūdžiai ir technologijos. Tai elementai kurie geriausiai apibrėžia kibernetinio saugumo sampratą. Iš pateiktos schemos matyti, kad šie elementai yra glaudžiai tarpusavyje susiję.

Kibernetinio saugumo samprata gali būti dažnai painiojama su elektroninė informacijos saugos ir dokumentų saugumo sampratomis. Iš ties tai tarpusavyje labai panašios sąvokos. *Informacijos duomenų apsauga* turi apimti visus informacijos apsaugojimo aspektus dirbant kompiuteriu. Dažniausiai tai yra apsauga nuo virusų, įsilaužėlių. Taip pat tai yra politika, apimanti slaptažodžių registravimo politiką, o taip pat kelianti reikalavimus daryti dokumentų kopijas.

Terminas „*kibernetinis saugumas*“ yra palyginti nauja sąvoka, kuri iš esmės pakeitė kompiuterinio bei informacijos saugumo sampratas. Kibernetinis saugumas dažnai painiojamas su informacijos užtikrinimo ir informacijos saugumo sąvokomis. Kibernetinis saugumas yra naudojamas apibūdinti priemones, kurių imamasi siekiant apsaugoti elektronines informacines sistemas nuo neteisėtų prieigų ir atakų. Tuo tarpu informacijos saugumo užtikrinimas turėtų būti suprantamas kaip užtikrinimas, kuomet informacinėse sistemose tvarkoma informacija bus apsaugota ir, kad „*valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti – šiuo atveju garantuojamas tinkamas konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus*

prisiėmimo ir autentiškumo lygis" (Europos vadovų Taryba. 2015). O informacijos saugumas apima visus apsaugojimo aspektus dirbant kompiuteriu, t.y. apsaugą nuo virusų ir įsilaužėlių, teisingą slaptažodžių ir registravimosi vardų politiką bei reikalavimą pastoviai daryti svarbios informacijos kopijas.

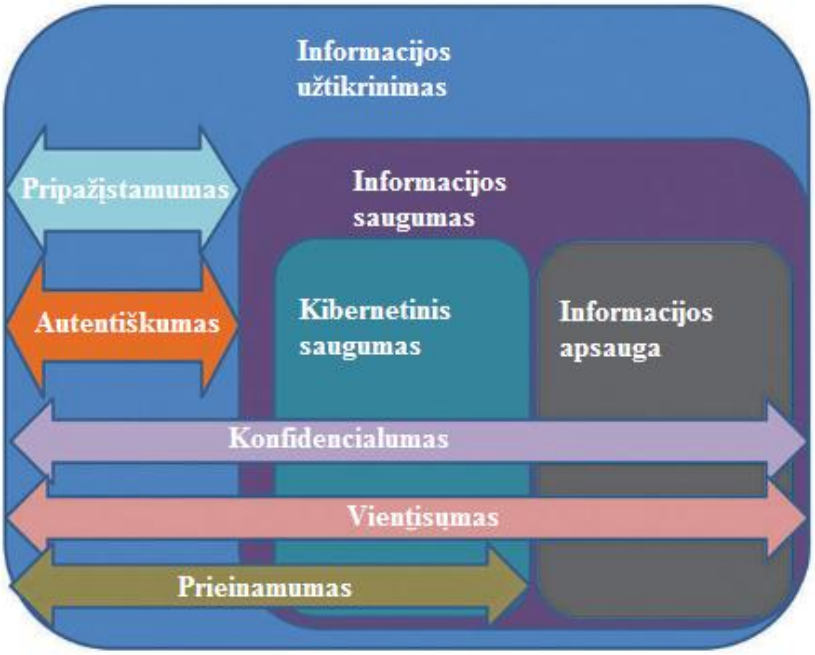
Siekiant tinkamai ir iki galo identifikuoti kibernetinio saugumo koncepciją, 1 lentelėje pateikiami kibernetinio saugumo, informacijos saugumo bei elektroninės informacijos saugumo sampratų skirtumai bei panašumai:

1 lentelė. Kibernetinio saugumo, duomenų saugos, elektroninės informacijos saugumo sampratų palyginimas

	Charakteristika	Skirtumai
Kibernetinis saugumas	Visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti (Morkūnienė, 2014).	Labiausiai specifinė ir konkreti sąvoka, kuri apima techninių priemonių, kibernetinių incidentų, elektroninių ryšių tinklų, etc. valdymą, tobulinimą ir priežiūrą.
Informacijos sauga	Informacijos bei sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams (Kiškis et al., 2006).	Apima tiek kibernetinį saugumą, tiek informacijos elementų saugą plačiąja prasme.
Elektroninės informacijos sauga	Elektroninės informacijos ir elektroninės informacijos infrastruktūros apsauga (Štitilis, 2012)	Apima tiek kibernetinį saugumą, tiek informacijos saugą virtualioje erdvėje.
Informacinių technologijų saugumas	Ribotos prieigos prie kibernetinėje erdvėje pateikiamų duomenų užtikrinimas, tinkamas informacinių išteklių valdymas (Sadowsky ir kt., 2003).	Apima ir kibernetinį saugumą, labiau orientuota į technologinius sprendimus.

(sudaryta autoriaus, 2015)

Kibernetinis saugumas pirmiausiai yra susijęs su tais pačiais tikslais, kaip ir informacijos saugumas. C.Schou, S.Harnandez (2014) pateikia svarbiausius kibernetinio saugumo elementus - koks yra ryšys tarp kibernetinio saugumo, informacijos saugumo, informacijos saugumo užtikrinimo ir jų santykis su konfidencialumu, vientisumu, prieinamumu iliustruojama 2 paveiksle.



2 pav. Kibernetinio saugumo užtikrinimo santykis su konfidencialumu, vientisumu ir pripažįstamumu (Schou C., Harnandez S., 2014)

Autoriai pažymi, jog kibernetinis saugumas kartu su informacijos apsauga formuoja įmonės informacijos saugumo strateginių veiksmų rinkinį – šiam rinkiniui bendri konfidencialumo bei vientisumo principai, tačiau vien tik kibernetinis saugumas turi garantuoti prieinamumą. Bendrai įmonės informacijos saugumo koncepcija įmonėje turi būti it pripažįstama bei autentiška – visi šie elementai formuoja aiškią įmonės informacijos užtikrinimo strategiją. Akivaizdu, jog kibernetinis saugumas įmonėje negali būti vertinamas atsietai nuo bendros informacijos saugumo užtikrinimo strategijos,

Bendra informacijos saugos strategija įmonėje labai glaudžiai susijusi su informacijos klasifikacijos principais, taikomais įmonėje, o ir pati informacijos klasifikacija yra labai svarbi kibernetinio saugumo užtikrinimui. Įmonėse informacija gali būti klasifikuojama į klientų informaciją, finansinę ar rinkodaros informaciją. Informacija turi būti pakankamai kokybiška, jog tiktų verslo procesams. Informacijos klasifikaciją patogu pateikti pagal hierarchinę klasifikaciją. Kibernetinio saugumo tikslai turėtų būti sutelkti į tai, jog šis saugumas gali prisidėti prie įmonės misijų ar vizijos tikslų įgyvendinimo. Kibernetinio saugumo tikslai nėra 100 proc. pasiekiami. Paprastai jais siekiama užtikrinti ir parodyti, kad bet kokia kibernetinio saugumo strategija ar politika, kuri yra nustatoma turi turėti bent kokią, apčiuopiamą vertę. Išskiria kibernetinio saugumo tikslus:

1) Padaryti operacijas saugias nuo įsilaužėlių;

2) Užtikrinti, kad informacija nebūtų vagiama;
3) Sekti kibernetinės erdvės vagysčių ir sukčiavimo atvejus.

Konstatuotina, jog kibernetinio saugumo tikslų įgyvendinimo sparta priklauso nuo tinkamai parinktų saugumo priemonių – pastarosios skirstomos į tam tikras grupes: teisines, moralines – etines, organizacines, fizines ir technines (aparatines programas).

1) *Teisinės apsaugos priemonės* naudojasi šalyje galiojančiais įstatymais, įsakymais ir norminiais aktais, kurie apibūdina informacijos naudojimosi taisykles, reguliuoja informacinių santykių dalyvių teises ir pareigas naudojantis informacija. Teisės aktai taip pat nusako atsakomybes jei taisyklės yra pažeidžiamos.
2) *Moralinės – etinės* apsaugos priemonės yra tam tikros normos, kurios susiformuoja šalyje ir visuomenėje didėjant informacinių technologijų paplitimo lygiui. Moralinių – etinių normų laikymasis nėra griežtai aprašytas, kaip teisės aktų, tačiau jų nesilaikymas menkina žmogaus, organizacijos autoritetą ir prestižą. Jos yra visuotinai pripažįstamos bendru susitarimu, arba įtvirtintos organizacijos tam tikruose taisyklių rinkiniuose.
3) *Organizacinės apsaugos* priemonės apibūdina duomenų apdorojimo sistemų funkcionuojančius procesus. Jos charakterizuoja išteklių naudojimą, vartotojų sąveikos su informacija tvarką.
4) *Fizinės informacijos apsaugos* priemonės įgyvendinamos naudojant įvairius mechaninius įrengimus, kurios skirtos užkirsti kelią ir apsisaugoti nuo įvairių fizinių kliūčių, potencialių pažeidimų. Šios priemonės užkerta kelią prieigai prie informacijos, jos sistemos komponentų.
5) *Techninės (programinės)* įrangos naudoja įvairius elektroninius įrenginius ir kompiuterines programas, kurios įeina į kompiuterių ir jų tinklų sudėtį ir vykdo apsaugos funkciją. Šių priemonių pagalba galima atskleisti vartotojus, juos identifikuoti ir autorizuoti, suteikti prieigas prie informacijos išteklių ar juos apriboti, šifruoti informaciją ir panašiai.

Pastaruoju metu vis daugiau dėmesio skiriama informacijos saugumo užtikrinimui. Galima taikyti labai daug įvairių informacijos saugumą užtikrinančių priemonių (Paulauskas ir kt., 2009). Autoriaus teigimu, bendriausiai jos gali būti skirstomas į fizines priemones, tinklo lygmens priemones, transporto lygmens priemones bei programinės įrangos lygmens priemones.

1) Fizinis lygmuo;

Fizinė apsauga. Fizinė apsauga yra skirta apsaugoti informacinės sistemos komponentus nuo vagystės, gaisro ar gamtos stichijos.

2) Tinklo lygmuo;

Paketų filtravimas. Paketų filtravimo sistema blokuoja arba praleidžia paketų srautą remiantis prievado numeriu, IP adresu, protokolu arba kitokia informacija. Paketų filtravimas gali būti įgyvendintas panaudojus skirtingas apsaugos sistemas.

Demilitarizuota zona. Tinklo dalis, kuri yra už vidinės tinklo ribos, bet yra pajungta į ugniasienę, vadinama demilitarizuota zona. Demilitarizuotoje zonoje gali būti viešai prieinami serveriai. Dažnai tai yra vadinama servisų potinkliu arba perimetro tinklu.

Ugniasienės. Ugniasienė skirta apsaugoti kompiuteryje esančius duomenis nuo įsilaužėlių. Ugniasienės būna aparatinės ir programinės.

Atakų atpažinimo ir prevencijos sistema. atakų atpažinimo sistemos panaudojimas leidžia atpažinti dar iki šiol nežinomas atakas, kurios gali patekti į tinklą. Atakų atpažinimo sistema yra paremta atakų požymių arba anomalijų tinkle atpažinimu bei administratoriaus informavimu apie tinkle atsirandančius įvykius

3) Perdavimo lygmuo;

Virtualus ir privatus tinklas. Bendrovės, kurios dalinasi bylomis arba apsikeičia konfidencialia informacija tarp padalinių, dažniausiai naudoja dedikuotus tinklo sujungimus siūlomus telekomunikacijų bendrovių. Labai dažnai yra naudojami virtualūs privatūs tinklai leidžiantys realizuoti pigų ir saugų ryšį per viešąjį tinklą. Virtualus privatus tinklas – tai tinklas, kuris naudoja viešojo interneto infrastruktūrą bei leidžia saugiai prijungti unikalius vartotojus prie bendrovės tinklo.

4)Programinės įrangos lygmuo;

Autentifikavimas ir slaptažodžių apsauga; apsaugos politika, kuri reikalauja iš vartotojo pasirinkti sudėtingus ir sunkiai atspėjamus slaptažodžius, laikyti juos paslaptyje bei reguliariai atnaujinti. Būtina naudoti skirtingus slaptažodžius pradedant nuo darbastalio rakinimo iki individualios programinės įrangos ir duomenų bazių. Autentifikavimas – tai procesas, kurio funkcija yra tapatybės nustatymas, t.y. nustatyti, kad vartotojas, programinė įranga arba kompiuteris yra iš tikrųjų tas kuo jis save pristato.

Operacinės sistemos apsauga. Informacinės sistemos apsaugos iš vidaus būdas yra nuolatinis operacinės sistemos atnaujinimų diegimas. Dažniausiai atnaujinimai yra išleidžiami saugumo spragoms ištaisyti. Atnaujinimo procesas yra vartotojo arba administratoriaus atsakomybė.

Taip pat operacinės sistemos nenaudojamų servisų atjungimas leidžia padidinti sistemos saugumą ir atsparumą atakoms;

Apsauga nuo kenksmingo kodo programų. Dažniausias ginklas prieš kompiuterinius virusus yra antivirusinės programos, kurios atlieka sistemos skanavimą ieškant virusų duomenų bylose arba elektroniniuose laiškuose;

Tinklo auditas ir pažeidimų fiksavimas, aktyvavimas. Tinklo auditas – tai procesas fiksuojantis kuris kompiuteris prieina prie tinklo ir kokius resursus naudoja. Informacija yra fiksuojama. Turint ilgalaikę įrašų istoriją galima aptikti įtartiną veiklą tinkle. Tokia informacija leidžia pamatyti kas bandė įsilaužti į tinklą ir imtis atitinkamų veiksmų.

Akivaizdu, jog kibernetinio saugumo samprata yra kompleksinis, daugianaris reiškinys. Jis turi apimti saugų tinklų, kompiuterių, programų veikimą. Kibernetinis saugumas apima techninės ir programinės įrangos infrastruktūrą, kuri taip pat yra labai įtakojama nacionalinės ir tarptautinių strategijų. Atlikus mokslinės literatūros analizę galima teigti, kad visgi termino *kibernetinis saugumas* apibrėžtis yra gana plati ir susidedanti iš daugelio įvairių elementų. Bendrai vertinant kibernetinį saugumą, konstatuotina, jog tai **– tam tikrų įrankių visuma, apimanti politikos, saugumo užtikrinimo gaires, rizikos valdymo metodus, veiksmus, mokymus, technologijas kurios gali būti naudojamos siekiant apsaugoti kibernetinę aplinką jos organizavimą ir vartojimo informaciją**. Terminas „kibernetinis saugumas“ yra palyginti nauja samprata, kuri iš esmės pakeitė kompiuterinio bei informacijos saugumo sampratas. Kibernetinis saugumas dažnai painiojamas su informacijos užtikrinimo ir informacijos saugumo sąvokomis. Šios aplinkybės neretai sudaro sąlygas atsirasti dviprasmybėms, nesutarimams, tam tikriems probleminiams aspektams atsirasti – išsamiau šie elementai aptariami 1.2. poskyryje.

1.2. KIBERNETINIO SAUGUMO PROBLEMATIKA

Dėl nevienareikšmiško kibernetinio saugumo supratimo ir vertinimo susiduriama su nemenkais taikymo iššūkiais tiek Lietuvoje, tiek ES lygmeniu. Pastarieji traktuotini kaip kibernetinio saugumo užtikrinimą ribojančios problemos, kurios nagrinėjamos tiek teoriniu, tiek praktiniu lygmeniu.

Kibernetinis saugumas yra ne tik atvira, saugi ir patikima kibernetinė erdvė, kurios viziją mato daugelis valstybių bet kartu su parengtomis kibernetinės saugos strategijomis apibrėžia, kaip saugiai užtikrinti šią erdvę ir kokių priemonių imtis. ES kibernetinio saugumo strategijoje nurodomi pagrindiniai efektyvų kibernetinį saugumą garantuojantys principai:

3 lentelė Kibernetinio saugumo principai

Principo apibrėžtis	Charakteristika
Pagrindinių žmogaus teisių nuomonės reiškimo laisvės, privatumo ir asmens duomenų apsauga.	Kibernetinis saugumas yra efektyvus tik tada, kai yra paremtas pagrindinių teisių ir laisvių apsauga. Informacijos viešinimas susijęs su kitų asmenų duomenimis galimas tik tuomet, kai laikomasi ES duomenų apsaugos
Prieiga visiems	Ribota prieiga prie interneto sukelia nepatogumus piliečiams Galimybė prieiti prie interneto kartu turi ir užtikrinti saugią prieigą jos vartotojams.
Demokratinis ir efektyvus valdymas	Skaitmeninė erdvė yra valdoma keleto didelių struktūrinių bendrovių. Labai svarbu, kad šios bendrovės suvoktų interneto valdymo svarbą ir išvystytų daugialypį požiūrį į interneto valdymą.
Bendra atsakomybė užtikrinti saugumą	Didėjant priklausomybei nuo interneto, didėja ir komunikacinių technologijų pažeidžiamumas. Svarbu, kad visos įmonės, individualūs vartotojai suprastų įmonės apsaugos nuo kibernetinių atakų svarbą ir panaudotų visus veiksnius, kurie padidintų kibernetinio saugumo užtikrinimą.

(ES kibernetikos saugumo strategijos, 2015)

Pažymėtina, jog „***kibernetinio saugumo principų nesilaikymas sudaro sąlygas neteisingai interpretuoti kibernetinio saugumo priemonių taikymo esmę, jų tinkamumą*“** (LR Vyriausybės nutarimas Nr.716 (2013-07-24)) – tai savo ruožtu sudaro tam tikrų problemų siekiant pritaikyti universalius kibernetinį saugumą užtikrinančius sprendimus. Siekiant ES lygmeniu formuoti vieningą kibernetinio saugumo priemonių taikymo praktiką, kuriamos įvairios kibernetinės strategijos tiek Lietuvos valstybės, tiek ir visos Europos mastu. Šių strategijos kuriamos tam, kad užkirstų kelią kibernetiniams veiklos sutrikdymas bei kitokio pobūdžio atakoms. Šiomis direktyvomis siekiama remti laisvės ir demokratijos vertybes, kurios užtikrintų saugų skaitmeninės ekonomikos augimą, didintų informacinių sistemų atsparumą elektroniniams nusikaltimams, o kartu ir stiprintų ES tarptautinę kibernetinio saugumo politiką. Europos Sąjungos pateikiamoje kibernetinio saugumo strategijoje yra pažymimi tokie pagrindiniai prioritetai:

1) Pasiekti kibernetinį atsparumą;
2) Sumažinti kibernetinių nusikaltimų skaičių;
3) Sukurti kibernetinės gynybos politiką ir pajėgumus, susijusius su bendra saugumo ir gynybos politika;
4) Plėtoti pramonės ir technologinius išteklius kibernetiniam saugumui užtikrinti;
5) Sukurti nuoseklią tarptautinę Europos Sąjungos kibernetinės erdvės politiką ir remti pagrindines ES vertybes.

Pažymėtina, jog minėtais prioritetais vadovaujamasi ir Lietuvos Respublikos mastu nuo 2015 m. įsigaliojusiame LR Kibernetinio saugumo įstatymo (2014 m. gruodžio 11 d. Nr. XII-1428. TAR) 3 str. nurodoma, jog kibernetinis saugumas turi būti grindžiamas kibernetinės erdvės, kibernetinio saugumo proporcingumo, viešojo intereso viršenybės principais, o 2011 m. patvirtintoje „Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 m. programoje“ (LR Vyriausybės nutarimas Nr. 83-4033, 2011-07-09) konstatuojama, jog pagrindiniai kibernetinio saugumo užtikrinimo tikslai Lietuvoje yra pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas, užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą, siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje. Atsižvelgiant į minėtus tikslus bei programos priemones, darytina išvada, jog Lietuvos įmonės turi pakankamai geras sąlygas kibernetiniam saugumui plėtoti ir jo priemonių taikymui.

Kaip jau minėta anksčiau, užtikrinti kompiuterinių sistemų informacinę saugą yra viena iš svarbiausių šių dienų informacinių technologijų problemų. Nepaisant didelio kiekio įvairių skirtingų įmonių dirbančių šioje srityje, tačiau problema yra gana opi ir vis dar neišspręsta. Siekiant tinkamai įvertinti probleminius kibernetinio saugumo priemonių taikymo aspektus, tikslinga tinkamai įvertinti patį saugumo objektą – t.y. duomenis, informaciją. Pažymėtina, jog duomenų rinkimas ir apdorojimas nėra paprastas procesas. Labai svarbu, kad informacija pasižymėtų tam tikromis savybėmis:

1) *Patikimumu* informacija turi būti kaupiama, pasižymėti pakankamumu ir būti nuolatos atnaujinama;

2) *Tikrumu* informacija turi būti išsami ir argumentuota;

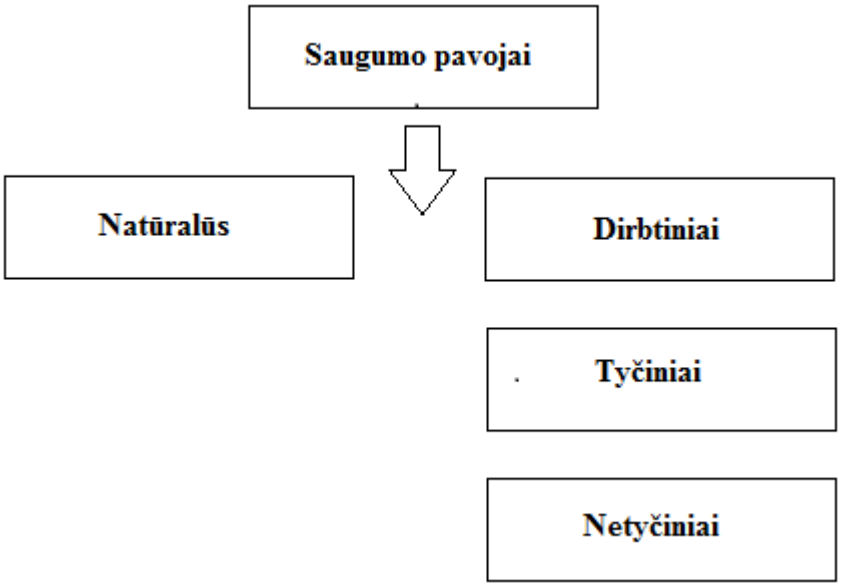
3) *Operatyvumu* informacijai turi būti būdingas konkretumas ir kokybiškumas, kurie leidžia laiku priimti tinkamus sprendimus;

4) *Sistemiškumu*. Informacijos atranka turi būti nuolatos bei sistemiškai vykdoma;

5) *Kompleksiškumu.* Informacija turi padėti suvokti aplinką ir perteikti informaciją susijusią su aplinka

Kaip pažymi E.Kazanavičius ir J.Žilinskas, „*bet kokia technologinė naujovė gali išspręsti tam tikros rūšies problemas ir skatina jos plėtojimąsi bei vystymąsi, tačiau šalia to gali būti sukeliamos naujos, visai kitokio pobūdžio problemų sukėlimo šaltiniu*“ (Kazanavičius, Žilinskas, 2002). Šiuo atveju, kalbant apie naujųjų technologijų poveikį visuomenei, padariniai taip pat gali būti neigiami, jei „*nebus imamasi tinkamo saugumo užtikrinimo*“ (LR Vyriausybės nutarimas Nr. 83-4033, 2011-07-09).

Žinoma, kad **nelegalus informacijos naudojimas, klastojimas, viešinimas ar iškraipymas sukelia akivaizdžius moralinius ir materialinius nuostolius visiems dalyviams, kurie naudojasi kompiuterizuotais informacijos sąveikos procesais** (pavyzdžiui, valstybei, juridiniams ir fiziniams asmenims). SAANS instituto ekspertai grėsmę supranta kaip *„tam tikras įmanomas įvykis, kuris gali padaryti žalos kurių nors subjektų atžvilgiu*“ (SAANS institute, 2015). Informacinės grėsmės, kaip ir daugelis kitų grėsmių pagal jų prigimtį gali būti skirstomas į dvi grupes: natūraliosios ir dirbtinės grėsmės.



3 pav. Grėsmių skirstymas pagal jų prigimtį (sudaryta darbo autoriaus)

Natūralios grėsmės gali būti suprantamos, kaip tokios informacijos saugumo grėsmės, suteiktos pagrindiniams informacijos elementams, pavyzdžiui kompiuterinėms sistemoms dėl natūralių gamtinių reiškinių (pavyzdžiui, stichinės nelaimės), kurios nepriklauso nuo žmogaus veiklos.

Dirbtinės grėsmės, tai grėsmės kompiuterinėms technologijoms ir jų elementams, kurios yra sukeliamos žmogaus veiklos padarinių. Dirbtinės grėsmės dar gali būti skaidomos į netyčines ir tyčines. *Netyčinės* grėsmės atsiranda tuomet, kai įveliamos tam tikros projektavimo, programinės įrangos klaidos ar klaidos, kurios įveliamos dėl personalo veiklos. *Tyčinės* grėsmės yra „*sukeliamos dėl savanaudiškų žmonių paskatų ir siekių*“ (Kazanavičius, 2002).

Svarbi informacijos apdorojimo problema **– informacijos pažeidžiamumas.** Egzistuoja daug galimybių pavogti, pažeisti, sunaikinti ir pakeisti duomenis. Beveik visuose informacijos apsaugos žinynuose yra pabrėžiami pagrindiniai bruožai, apibrėžiantys duomenų saugos lygius:

1) *Administracinis – techninis saugumas;* Administracinis – techninis saugumas, laikomas toks techninių priemonių saugumo užtikrinimas, kad kompiuterinėse sistemose (ir ne tik) laikoma informacija būtų saugi. Šiam saugomos informacijos lygmeniui būdingos tam tikros nuostatos, pavyzdžiui saugumo politikos apibrėžtys, kokią informaciją reikia saugoti, o kokios ne. Taip pat yra pateikiama apsaugos lygių samprata. Informacija yra sugrupuojama į tam tikrus „saugumo“ lygius pagal jautrumą.

2) *Fizinis saugumas*; Šiai saugumo rūšiai priskiriamos kompiuterinių techninių ryšių priemonės, kurios apsaugo nuo fizinio išorinių jėgų poveikio. Šiam poveikiui priskirtini kompiuterių gedimai, stichinės nelaimės ir kiti trikdžiai, kurie negrįžtamai sunaikina duomenis kietuosiuose diskuose, saugojimo įrenginiuose.

3) *Teisinis reglamentavimas*; Toks informacijos saugojimo būdas, kuris apibrėžia, kaip organizacijos darbuotojai turėtų elgtis su svarbia informacija ir duomenimis, kurie apibūdina įmonės komercines paslaptis ir savitumus. Taisyklėmis nustatoma, kokia informacija yra slapta, ir nepatenka į daugelio asmenų naudojamus informacijos šaltinius, o kokia gali būti plačiai vartojama. Įmonėse egzistuojantys norminiai aktai leidžia darbuotojams prasižengus juos bausti pagal administracinę ar baudžiamąją teisę.

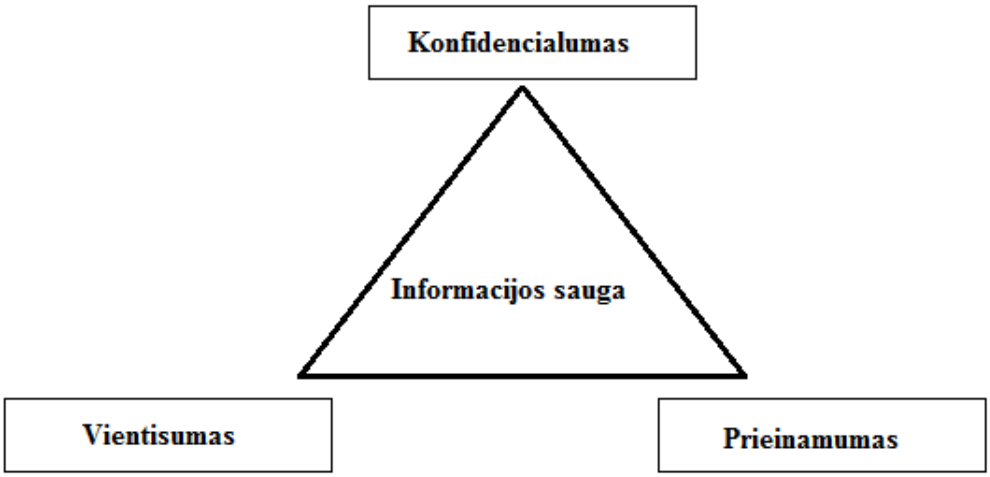
Dauguma kibernetinio saugumo apibrėžimų jau daugiau kaip dvidešimt metų remiasi trimis saugumo tikslais (CIA triada) (Parker, 1981). Pagal CIA triadą įvardijama, kad kibernetinio saugumo tikslas – užtikrinti kibernetinių duomenų konfidencialumą (*confidentiality*), vientisumą (*integrity*) ir prieinamumą (*availability*), kur konfidencialumas suprantamas kaip informacijos slaptumas, t. y. informacija turi būti prieinama tik tiems, kam ji skirta; vientisumas apima pradinės informacijos tikrumą, patikimumą bei autentiškumą, t. y. informacija ir jos šaltinis turi būti apsaugoti nuo bet kokio klaidingo ar nesankcionuoto pakeitimo, visi pakeitimai yra žinomi; prieinamumas – užtikrinta galimybė pasinaudoti informacija, t.y. sankcionuoti vartotojai turi turėti galimybę pasiekti informaciją, kai jos reikia.

Autoriaus S.Jastiugino (2011) teigimu, „*informacijos saugumo tyrimuose analizuotus informacijos saugumo aspektus, galima sugrupuoti ir pateikti, kad informacijos saugumo valdymas apima tris dimensijas*“:

1) strateginę, jungiančią administracinius, organizacinius, valdymo, ekonominius, standartų, teisinius, gerųjų praktikų ir pan. aspektus;

2) žmogiškąją, jungiančią saugumo kultūros etinius, kompetencijų, mokymų, psichologinius ir pan. aspektus;

3) technologinę, jungiančią informacinių technologijų, techninių ir programinių priemonių, matematinius, kriptografinius ir pan.



4 pav. Informacijos saugumas – konfidencialumo, vientisumo ir prieinamumo užtikrinimas

Konfidencialiais duomenimis yra laikoma tokia informacija, su kuria gali dirbti tik tam leidimus turintys asmenys. Jei duomenys pavagiami, atskleidžiami tokia neteisėta veikla jau yra laikoma konfidencialios informacijos saugumo pažeidimu. Konfidenciali informacija yra susijusi su neleistino prisijungimo grėsmėmis, neteisėtu informacijos atskleidimu, sandorių sekimu ir stebėsena, neteisėtu duomenų kopijavimu ir platinimu.

Kiekvienoje įmonėje turėtų egzistuoti tam tikros informacijos saugumo normos, kurios turėtų užtikrinti firmos informacijos saugumą. Egzistuoja tam tikri bruožai, kurie nurodo, jog įmonėje yra gana ryškūs informacijos pažeidimai:

1) Viešose vietose palikti slaptažodžiai, slaptažodžiu naudojasi keli vartotojai;
2) Leidžiamas neribotas bandymų skaičius suvedus netinkamą slaptažodį;
3) Kompiuteriai, iš kurių valdomi serveriai, paliekami be priežiūros;
4) Vartotojui, dirbančiam su nutolusiais serveriais leidžiama į kompiuterį diegti planšetes ir su darbu nesusijusias programas;

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

1) Lygis 0 – informacijos apsaugos organizacijoje nėra;
2) Lygis 1 – informacijos apsauga organizacijoje traktuojama kaip „techninė problema“;
3) Lygis 2 – informacijos apsauga - tai organizacinių ir techninių priemonių kompleksas;

4) Lygis 3 – informacijos apsauga yra organizacijos kultūros dalis.

Kibernetinio saugumo atžvilgiu šiuo atveju probleminė situacija susidaro dėl to, jog **Lietuvoje dažniausiai sutinkamas 0 ir 1 informacijos apsaugos brandos lygiai**. Organizacijos, kurių informacijos apsaugos brandos lygis yra nulinis, krizių atveju patiria labai didelius nuostolius, o jei yra labiau priklausomos nuo informacinių sistemų ir informacinių technologijų – net ir bankrutuoja.

S.Ali, V. Padmanabhan, J.Dixon (Ali, Padmanabhan, Dixon) pažymi, jog kibernetinio saugumo užtikrinimo problematika išryškėja dėl keleto priežasčių: įmonės perkelia turimą informaciją į privačias ir viešąsias duomenų debesijas. Iki tol įmonių duomenys paprastai buvo kaupiami lokaliame serveryje. Akivaizdu, jog sudėtingėjant duomenų talpinimo ir perdavimo metodams, būtina diegti inovatyvius jų apsaugos elementus pradedant nuo saugumo valdymo individualiame lygmenyje, integruota stebėsena, baigiant hibridinėmis valdymo galimybėmis debesijos aplinkoje. Šiuo atveju konstatuotinas probleminis aspektas grindžiamas nuostata, jog **kibernetinis saugumas tobulėjant duomenų perdavimo metodams privalo nuolat būti peržiūrimas, atnaujinamos diegimo priemonės – tai atliekama ne visose įmonėse vienodai, o kai kuriose jų – išvis neatliekama**. Vienas tokių pavyzdžių – mobiliųjų priemonių naudojimo intensyvumas tarp vadovų ir darbuotojų. Tokiu atveju kibernetinio saugumo priemonės privalo būti taikomos ne tik bendrovei priklausančiuose įrengimuose, tačiau kartu bent minimaliai diegiamas ir privačiuose darbuotojų įrenginiuose. Tarptautinėje erdvėje tokiu būdu naudojami ir prižiūrimi įrenginiai vadinami BYOD (angl. *bring-your-own-device*) įrenginiais – pastaraisiais metais atlikti tyrimai parodė, jog artimiausiu metu iki 66 proc. įmonių yra linkę laikytis BYOD politikos – tai savo ruožtu didina kibernetinio saugumo užtikrinimo riziką.

Tarptautinėje praktikoje neretai susiduriama su kibernetinio saugumo priemonių diegimo kliuviniais. Svarbiausias jų – **sutartiniai įsipareigojimai**, kuriems užtikrinti būtinas pakankamai aukštas investicijų atnaujinimo lygis. Tarptautinių prekybos rūmų specialistai (ICC cyber security guide for business, 2015) akcentuoja, jog nepaisant kibernetinio saugumo svarbos augimo, probleminiai šios srities aspektai iki šiol sprendžiami gana sudėtingai – būtina užtikrinti nuolatinį saugumo priemonių valdymą įvertinant galimų inovatyvių išpuolių tikimybes bei būtinybę komunikuoti kuo intensyviau ir labiau.

Apibendrinant poskyrį, galima teigti, kad internetas tapo pasauliniu reiškiniu, tačiau padaugėjo nusikaltimų, kurie yra vykdomi per interneto prieigas. Kibernetinis saugumas privalo garantuoti asmenims saugų interneto naudojimą. Kibernetinio saugumo samprata yra kompleksinis, daugianaris reiškinys. Jis turi apimti saugų tinklų, kompiuterių, programų veikimą. Kibernetinis

saugumas apima techninės ir programinės įrangos infrastruktūrą, kuri taip pat yra labai įtakojama nacionalinės ir tarptautinių strategijų. Atlikus mokslinės literatūros analizę galima teigti, kad visgi termino *kibernetinis saugumas* apibrėžtis yra gana plati ir susidedanti iš daugelio įvairių elementų. Bendrai vertinant kibernetinį saugumą, konstatuotina, jog tai **– tam tikrų įrankių visuma, apimanti politikos, saugumo užtikrinimo gaires, rizikos valdymo metodus, veiksmus, mokymus, technologijas kurios gali būti naudojamos siekiant apsaugoti kibernetinę aplinką jos organizavimą ir vartojimo informaciją**. Terminas „kibernetinis saugumas“ yra palyginti nauja samprata, kuri iš esmės pakeitė kompiuterinio bei informacijos saugumo sampratas. Kibernetinis saugumas dažnai painiojamas su informacijos užtikrinimo ir informacijos saugumo sąvokomis. Kibernetinis saugumas yra naudojamas apibūdinti priemones, kurių imamasi siekiant apsaugoti elektronines informacines sistemas nuo neteisėtų prieigų ir atakų. Tuo tarpu informacijos saugumo užtikrinimas turėtų būti suprantamas kaip užtikrinimas, kuomet informacinėse sistemose tvarkoma informacija bus apsaugota ir, kad „*valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti – šiuo atveju garantuojamas tinkamas konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygis*“. O informacijos saugumas apima visus apsaugojimo aspektus dirbant kompiuteriu, t.y. apsaugą nuo virusų ir įsilaužėlių, teisingą slaptažodžių ir registravimosi vardų politiką bei reikalavimą pastoviai daryti svarbios informacijos kopijas.

2. VERSLO PROCESŲ IR KIBERNETINIO SAUGUMO SĄSAJOS

Šiame skyriuje įvertinamos verslo procesų ir kibernetinio saugumo sąsajos, išgryninama verslo procesų samprata, identifikuojami verslo procesų valdymo etapai, pagrindžiama informacijos saugumo svarba verslo procesuose.

2.1 VERSLO PROCESŲ SAMPRATA

Autoriaus V.Viliūno teigimu, *procesą* galima įvardinti kaip „*tam tikrą apibrėžtą veiklą, kuria siekiama sukurti numatytą išeigą*“ (2011). Proceso vyksmo metu dažniausiai dalyvauja keli asmenys. Jų veikla apibrėžiama kaip komandinę veiklą, kuria siekiama gauti konkrečius rezultatus. Kitų autorių darbuose D.Klimas ir J.Ruževičius procesu įvardija „*tarpusavyje susijusius ir sąveikaujantys organizacijos veiksmus, kuriuose gaviniai yra paverčiami numatytais produktais*“ (Klimas, Ruževičius, 2006). Organizacijų veikloje procesas apibrėžiamas kaip tam veiksmų seka (apibrėžti žingsniai darbo rezultatui pasiekti) kuri turi aiškiai numatytą pradžią ir pabaiga.

Atlikus mokslinės literatūros analizę, pastebėta, kad pateikiamas verslo procesų skirtingas ir nepakankamai aiškus apibrėžimas. Siekiant tiksliau suvokti, kas yra *verslo procesas*, svarbu ir naudinga pateikti skirtingų autorių šios sąvokos apibrėžimus. Svarbu pastebėti, jog dalis autorių verslo procesus nagrinėja kaip *procesų vadybą*. Minėtos dvi sąvokos galėtų reikšti tą patį, nes procesų valdymas pirmiausia suprantamas kaip verslo procesų valdymas.

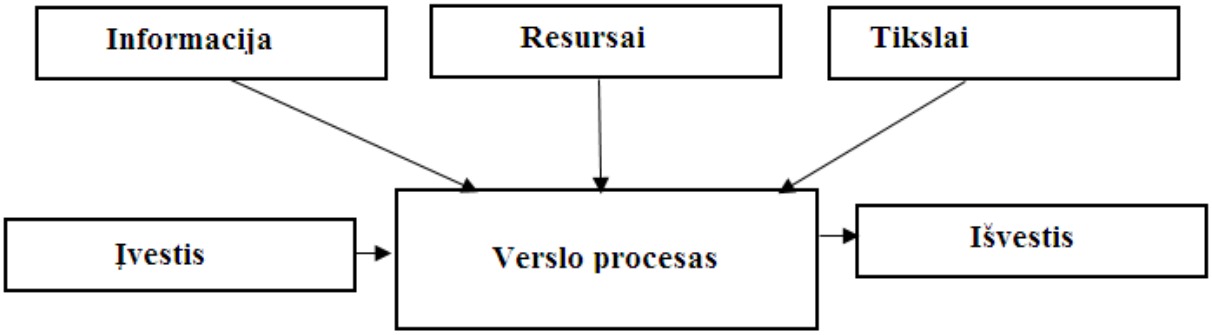
Panašiai verslo procesus apibrėžia ir tyrėjas B.Hommes (2000). Šio autoriaus teigimu *„verslo procesus ir elementarius procesus iš dalies galima laikyti sinonimais*“ (. Jo nuomone, verslo procesas yra „*tam tikrų veiklų rinkinys, kuriam būdinga turėti tam tikras įėjimo ir išėjimo rūšis, kurio svarbiausias tikslas yra kliento poreikių tenkinimas*“. Šiuo atveju verslo procesas yra labai stipriai orientuotas į verslą, tai tarsi apibrėžtis, kaip tam tikrais metodais pasiekti verslo tikslus.

Autoriai De Toro ir McCabe pabrėžia, kad „*verslo procesas gali būti suprantamas kaip tam tikra samprata, kuri nusako labai išsamius verslo procesų gerinimo būdus o tai padeda įmonėms patirti neigiamus padarinius*“ (De Toro, McCabe, 2007). Verslo procesai apima aiškiai apibrėžtą verslo procesų analizavimą, jų kontroliavimą, tobulinimą ir valdymą. Tai užtikrina, kad įmonėje produktai ir su kokybe susijusios paslaugos yra optimizuojamos o su tuo susiję kaštai gali būti ženkliai sumažinti.

Tyrėjo J.Mikulio teigimu, *„bet koks procesas gali būti smulkinamas iki tam tikro detalaus lygio*“ (Mikulis, 2007). Smulkinant ir skaidant procesus svarbu, kad būtų išlaikomas balansas. Jei verslo procesai yra per daug smulkiai suskaidomi, prarandama bendra proceso esmė, tikslas.

Priešingu atveju – „*per daug bendras procesų skaidymas į abstrakčius procesus neduoda teigiamų ir laukiamų rezultatų, nes remiamasi ne konkrečia ir informatyvia informacija*“.

E.Bagdono, I. Patašienės, M.Patašiaus, V.Skvernio (2007) teigimu, „*verslo procesai gali būti apibrėžiami kaip tam tikros struktūrizuotos veiklos aibę, kuri yra kuriama tam tikrai produkcijai ar konkrečiai rinkai, klientūrai*“. Procesų apibrėžtis yra labai panaši: procesai – tai ryšiai (sąryšiai) tarp įėjimų ir išėjimų, kai įėjimai yra transformuojami į išėjimus naudojant tam tikrą veiklos scenarijų, kai reikšmė suteikiama įėjimo pradžioje.



5 pav. Verslo proceso sampratos apibūdinimas

Beveik visi organizacijose vykstantys procesai yra dirbtiniai, sukurti žmogaus ir žmogaus veikla yra priemonė atsirasti ir vykti dirbtiniems procesams. Procesus galima valdyti, kurti, tobulinti, pradėti, kontroliuoti, derinti, nukreipti, užbaigti ir t.t., ir žmogus visa tai gali daryti per veiklą, jos tipą, pobūdį, intensyvumą, greitį, kompleksiškumą ir pan. Tą patį procesą galima pradėti skirtingomis veiklomis. Procesai yra abstraktūs fenomenai ir juos galima vaizduoti schematiškai ar dar kitaip, galima išmatuoti vienus lengviau, kitus - sunkiau. Procesus apibūdinti *„galima ir pagal pėdsakus, taip pat pagal tai juos galima atsekti firmoje*“ (Zacharevičius, 2004).

Manoma, kad rinkos sąlygomis organizacijos išgyvenimui ir vystymuisi reikalingi devyni procesai:

1)Rezultatyvumo (produkavimo);

2) Funkcionavimo;

3) Reprodukcijos;

4) Organizavimo;

5) Vadovavimo;

6) Valdymo;

7) Kūrybos (inovacijų);

8) Naikinimo (marinimo);

9) Vystymosi.

Rezultatyvumo procesas, tai procesas, skirtas sudaryti organizacijoje rezultatą (paprastai tai arba produktas, arba paslauga), kurį galima būtų pateikti rinkai, ir tai vienintelis iš visų procesų, kurio rezultatai skirti rinkai, už ką siekiama gauti finansinę naudą. Šis procesas gali būti laikomas baziniu. Įmonei reikalingas šio proceso metu gautas rezultatas, o kiti procesai organizacijoje laikomi aptarnaujančiais. Nors ir antrarūšiai ar pagalbiniai šie procesai reikalingi tam, kad rezultatyvumo procesas būtų optimalus, efektyvius ir produktyvus.

Funkcionavimo procesas organizacijoje apima visa tai, kas reikalinga, kad organizacija galėtų funkcionuoti. Svarbiausia, kad būtų vykdomas organizacijoje pagrindinis rezultatyvumo procesas. Funkcionavimą sudaro reikalingų žaliavų pirkimas ir jų pristatymas, atlyginimų mokėjimas, buhalterinės apskaitos, darbuotojai ir jų atlikimo funkcijos, įvairūs pataisymai, produktų realizavimas, jų apiforminimas ir pristatymas.

Reprodukcijos procesas tai procesas, kurio metu atnaujinami arba papildomi įvairius įmonėje suvartojami ištekliai, kurie yra svarbūs organizacijos veiklai ir yra iki galo suvartojami. Reprodukcijai svarbūs medžiagų ištekliai, kurie gali būti panaudojami gamybos apimtyse, energetiniuose ištekliuose, įvairius žmogiškuosius išteklius, dažniausiai susiję su jų kvalifikacija. Funkcionavimo procesas įtakoja, jog vyktų gamybinis procesas, kuris tęsiasi trumpą laiko tarpą, o reprodukcijos procesas nulemia tai, kad funkcionavimo procesas tęstųsi daug ilgesnį laiko tarpą. Tai gali siekti dešimtmečius ar metus.

Organizavimo, vadovavimo ir valdymo procesai, yra apjungiami į vieną bendrą visumą, kurią sudaro šie trys procesai, kurie apibrėžiami kaip vadybos procesas. Įvardijant įmonės valdymą reikia apibrėžti dvi skirtingas sąvokas: turto valdymą ir veiklų valdymą. Tai yra dvi skirtingos sąvokos. Turto valdymo metu už turtą atsakingi yra jo savininkai ir bendrasavininkiai. Jie rūpinasi, ką veikti su turtu. Turtas priklauso jų savininkams. Veiklų valdymas yra sutelktas įmonės darbuotojų ir specialistų rankose. Jie vykdo darbo procesus, valdo juos ir siekia, kad viskas vyktų sklandžiai.

Kūrybos ir naikinimo procesas Kūrybos proceso esmė yra žmogus (individas), kuris generuoja įvairias mintis. Žmogus yra mąstanti ir kurianti būtybė. Jo galvoje gimsta įvairios idėjos ir sprendimai. Šio proceso metu žmogus operuoja kokia nors pradine informacija, kurią asmuo turi sukaupęs per savo patyrimą ar kur nors gavęs: perskaitęs, sužinojęs. Asmuo gali priimti inovatyvius sprendimus, kultūrines normas. Tokie procesai įmanomi tik susisteminant esamą dabartį ir praeitį bei numatant ateities perspektyvas. Naikinimo proceso metu sukuriama tuščia erdvės niša. Joje yra organizuojami, pradedami ir realizuojami kūrybiniai procesai ar jo rezultatai. Naikinimo procesas

yra pagrįstas analize ir pažinimu per analizės objektą. Jeigu įmonėje tinkamai neįgyvendintas naikinimo procesas, tuomet negali tinkamai vykti ir kūrybinis procesas.

Vystymosi procesas. Pagrindiniai vystymosi požymiai, tai tam tikri pokyčiai įmonėje, kuriais remiantis įmonėje vyksta įvairių procesų vystymasis, arba įtakoja jų degradavimą, arba išlieka neutraliais jų vystymosi atžvilgiu. Tačiau stabilumas yra gana retai pasitaikantis procesas. Įmonėje procesai visada evoliucionuoja arba tobulėja, o kartais ir nunyksta. Pokyčiai įmonėje yra siejami su jos tobulėjimu. Įmonės vystymosi proceso poreikio reikalingumas siejamas su įmonės išgyvenimu ir poreikių didėjimu. Įmonėje svarbu didinti galimybes užsibrėžiant įvairius siekius arba restruktūrizuoti esamus, nes tai svarbi įmonės vystymosi sąlyga. Vystymasis organizacijoje sietinas su aukštesnių tikslų siekimu ir didesnių galimybių realizavimu.

V.Viliūnas (Viliūnas, 2011) visus verslo procesus skirsto į tris grupes: valdymo, pagrindinius ir pagalbinius verslo procesus. Detali šių procesų klasifikacija pateikiama 4 lentelėje.

4 lentelė Verslo procesų grupavimas

Procesas	Procesų rūšys
Valdymo procesas	Vadovavimo procesas; Organizavimo procesas; Projektų valdymo procesas; Verslo rinkos valdymas; Išorinių organizacijos santykių valdymas; Pokyčių valdymas; Žinių valdymas; Organizacijos vizijos ir strategijos kūrimas ir vystymas; Personalo ir finansinių išteklių valdymas.
Pagrindiniai procesai	Pirkimo procesas; Tiekimo procesas; Produkto ir paslaugos pristatymo procesas; Pardavimo procesas; Užsakymo išpildymo procesas; Gamybos procesas; Išorinių projektų įgyvendinimo procesas.
Pagalbiniai procesai	Rinkodaros procesas; Produktų ir paslaugų vystymo procesas; Kokybės užtikrinimo procesas; Atitikties užtikrinimo procesas; Audito procesas; Informacinių technologijų išteklių valdymas; Nuosavybės valdymo procesas; Vidinių projektų įgyvendinimo procesas.

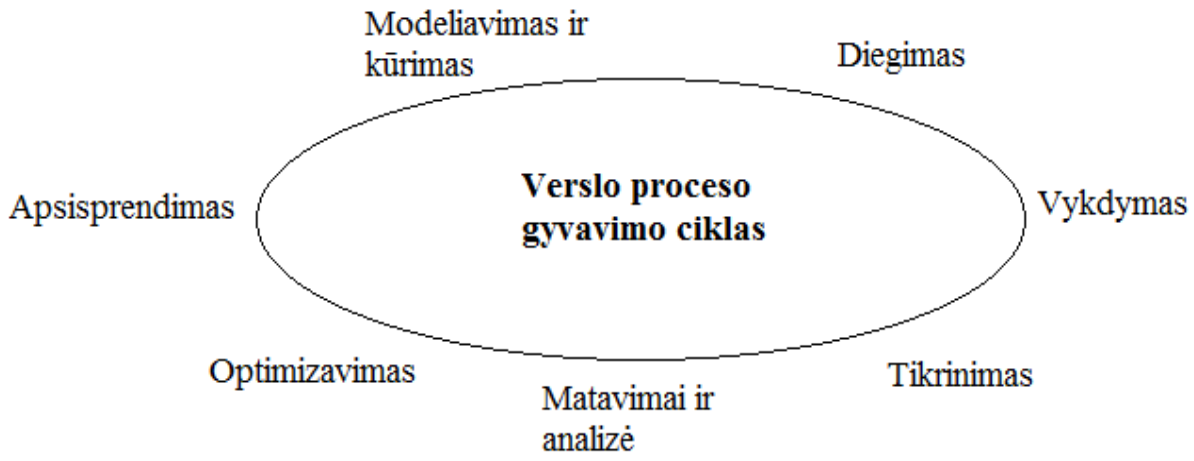
(Viliūnas, 2011)

Autorius Macintoch (1993) savo darbuose išskiria penkis pagrindinius galimus proceso brandos atitikmenis:

1) Pradinė iniciatyva (*initial*) – pradinis procesų sudarymas;

2) Pakartotinis (*repeatable*) – sudaromi pakartotini procesai;
3) Apibūdinamasis (*defined*) – tai procesas, kurio metu apibūdinami įmonėje vykstantys procesai įvairiais atžvilgiais;
4) Naudojimo ir valdymo (*measured*) – tai tiksliai ir kruopščiai kontroliuojami procesai;
5) Optimizuoti (*optimising*) – šiame etape siekiama procesą gerinti ir tobulinti.

Verslo procesai gali būti pateikiami tam tikro ciklo gyvavimo išraiškoje. Šiame cikle pateikiami etapai, kuriuos turi praeiti individualus procesas. Jei procesas yra veikiantis ir naudojamas įmonėje, egzistuoja veiksmų seka, kuri susijusi su šio proceso ciklo gyvavimu. Bendras verslo procesų ciklas pateikiamas 6 paveiksle. Iš pateiktos schemos matyti, kad verslo proceso gyvavimo ciklas susideda iš: atradimų ir dokumentacijos, planavimo, įgyvendinimo, diegimo etapo ir valdymo ir optimizavimo.



6 pav. Verslo proceso gyvavimo ciklas (sudaryta darbo autoriaus)

V.Adomėno teigimu, „*verslo procesai gali būti tobulinami ir gerinami*“. Pasak autoriaus, „*įmonės vadovai turi domėtis ir siekti, kaip pagerinti įmonėje vykstančius verslo ir kitokius procesus, kad jie taptų efektyvesni ir rezultatyvesni*“ (Adomėnas, 2011). Tyrėjas išskiria ir akcentuoja pagrindinius procesų gerinimo veiksnius:

1) Gerinimo priežasčių identifikavimas;
2) Esamos situacijos analizė;
3) Nustatytų problemų analizė;
4) Galimų sprendimų identifikavimas;
5) Poveikio įvertinimas;
6) Naujo sprendimo įgyvendinimas ir įforminimas;

7) Naujo proceso rezultatyvumo ir efektyvumo įvertinimas.

Apibendrinant poskyrį galima teigti, kad mokslinėje literatūroje autoriai pateikia gana plačius verslo procesų apibrėžimus ir sampratas. Pagrindinė to priežastis yra tai, jog procesų vadybos teorija laikoma nevisiškai susiformavusiu mokslu iki galo. Visi tyrėjai ir mokslininkai akcentuoja, kad įmonė, kuri analizuoja, detalizuoja, gerina ir analizuoja įmonės verslo procesus tampa labiau konkurencinga ir turi daugiau galimybių prisitaikyti prie konkurencingos rinkos, nes tokiu būdu atrandamos silpnosios vietos proceso gamyboje.

2.2 VERSLO PROCESŲ VALDYMAS

Verslo procesų valdymas (*BMP* (*Business Process Management*)) yra svarbi sąvoka įmonėms ir organizacijoms, kurios turi sukūrusios verslą ir įvairiomis priemonėmis siekia pagerinti esamus verslo procesus bei naujus pakeitimus. Verslo procesų valdymas yra apibrėžta metodika, kuri padeda pasiekti įmonėje keliamus tikslus procesams ir naujovėms kartu didindamas ir jų kokybiškumą, gaunamas pajamas ir gerina vartotojų poreikius.

Tyrėjas T.[Davenport] pabrėžia, kad *„daugelis asmenų maišo verslo procesų valdymo sąvoką siejama su (Business Process Management) su verslo procesų tobulinimo veiklos apibrėžimu (Business Process Improvement*)“ (Davenport, 1990). Verslo procesų tobulinimas siejamas su projektų arba tam tikrais vienkartinių veiksnių tobulinimu. Jo metu gali būti pakeičiamas vykdomų procesų dizainas ar procesai yra iš esmės kitaip pertvarkomi. Įprastai verslo procesai yra tobulinami taikant techniką, kuri vadinama- šešios sigmos. Ji apimą lanksčią gamybą, visuotinės kokybės valdymą ir procesų *reinžinieringumą*. Kita sąvoka − verslo procesų valdymas. Ji labiau siejama su įmonės veiklos tikslų pasiekimu, kai yra valdomi jos procesai. Šios veiklos metu apimamas nenutrūkstamas grįžtamasis ryšys, kuris užtikrina, kad įmonėje verslo procesai atitiktų jos strategijas ir lūkesčius. Įmonėje, kurioje valdomi procesai, gali būti taikomi verslo tobulinimo metodais, kurių pagalba būtų įgyvendinti specifiniai patobulinimai. Tačiau, verslo tobulinimo metodų panaudojimas įmonėje neužtikrina, kad įmonėje patikimai valdo procesus.

Verslo procesų valdymo sąvoka susiformavo pereito šimtmečio pabaigoje. Ši sąvoka tapo kaip tam tikru standartu, kuris apibrėžia, kaip valdyti tam tikras verslo procedūras, kaip jas struktūriškai organizuoti, skaidriai ir standartizuotai valdyti. Įmonės savo veikloje taiko įvairius procesus norėdamos pertvarkyti esamą padėtį, diegia naujas technologijas, siekia optimizuoti valdymo procesus bei juos pagerinti. Organizacijos paprastai atlieka periodiškus proceso tobulinimus, kurie yra orientuoti į konkrečius verslo procesus. Norint įtvirtinti visus verslo procesų valdymo pakeitimus reikalingos visos organizacijos bendros pastangos, kuriomis siekiama įvertinti

gautus rezultatus susijusius su verslo procesų valdymu ir toliau sėkmingai tobulinti ir diegti šiuos pokyčius savo įmonėje.

Kai kurie tyrėjai ir autoriai pabrėžia verslo procesų valdymo svarbą ir naudingumą įmonėms. Tyrėjai J.Bae, J.Caverlee, L.Liu, ir W.B.Rouse (2007) akcentuoja, kad įmonė gali pasiekti naudingumą, jei valdytų savo procesus remdamasi šiais tikslais:

1) Procesų valdymas įmonėje sukuria aiškią verslo sampratą, o tai padeda atpažinti silpnąsias verslo procesų vietas;

2) Diegiamas procesų valdymas užtikrina geresnius ir kokybiškesnius rezultatus, nes tai užtikrina pastovią ir nuoseklią informacijos valdymą;

3) Procesų valdymas gali tapti automatizuotu. Tai gali būti atliekama ir taikoma mažiau svarbiems valdymo darbams (darbo grafikų sudarymas), o tai lemia jog organizacija gali dėmesį ir veiklą nukreipti į svarbesnius darbus.

Daugelis tyrėjų pabrėžia, kad verslo procesai bei jų modeliai gali būti naudojami įmonėse siekiant priimti tam tikrus sprendimus. L.Paškevičiūtės, A.Čaplinsko teigimu, „*labai svarbu įmonėse išanalizuoti vykstančius verslo procesus, įvertinti esamą padėtį ir įmonės tikslus*“ (Paškevičiūtė, Čaplinskas, 2007). Atsižvelgiant į įmonės informacinių technologijų padėtį galima išskirti šešias verslo procesų fazes:

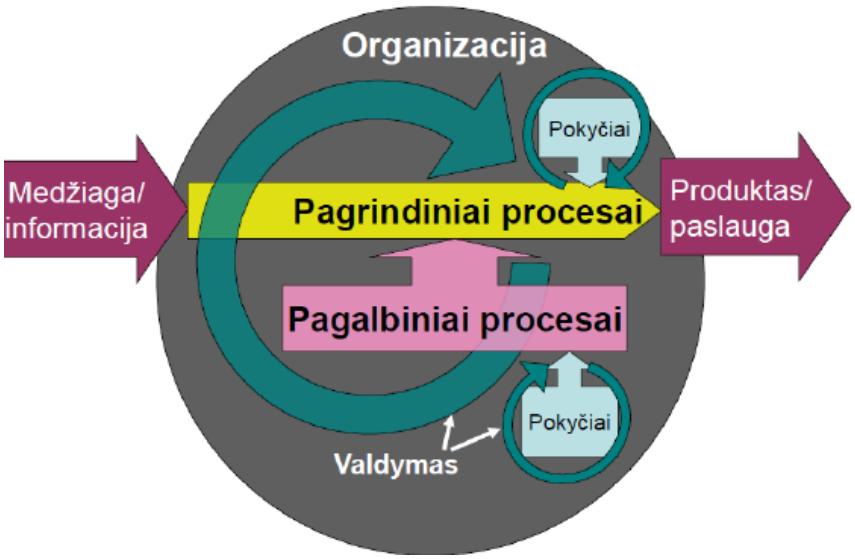
1) Funkcinę hierarchiją;
2) Funkcinė hierarchija su automatine funkcija;
3) Funkcinė hierarchija su duomenų bazės dalimi programiniame įrankių komplekte;
4) Procesas orientuotas į verslą;
5) Tiekimo grandinė orientuota į verslą;
6) Informacinių technologijų ir interneto naudojimas pagyvina verslą.

Verslo procesų valdymas apima ne tik metodus ir procedūras, metodus ir įrankius, kaip pasiekti ar užtikrinti tam tikrą procesą. Kartu *„valdymas apima ir įmonės gebėjimą vertinti ir tobulinti esamus procesus*“ (Niehaves, 2014). Verslo procesų vertinimui ir tobulinimui yra naudojami brandos modeliai. Šiuose brandos modeliuose pateikiama tam tikra įmonės procesų augimo ir vystymosi eiliškumas, kuris reikalingas tikslams pasiekti.

Tyrėjas G.M.Giaglis (1997) siūlo verslo procesus grupuoti atsižvelgiant į jų valdymo požymius. Todėl iš esmės verslo procesai gali būti modeliuojami pagal tokius reikalavimus:

1) Techniniai reikalavimai, kurie apima formalųjį modeliavimą, kiekybinį modeliavimą, modeliavimo dokumentaciją, modelio tinkamumą;

2) Politiniai/socialiniai reikalavimai, tokie reikalavimai, kurie apima alternatyvius projektavimus ir ryšius tarp modelių ir vartotojų.



7 pav. Verslo procesų valdymo modelis (Viliūnas V., 2011)

Pagal įvairių autorių pateiktus verslo proceso ir verslo proceso valdymo apibrėžimus galima teigti, kad verslo proceso valdymo metu proceso planavimas, valdymas ir kontrolė yra sujungiami į bendrą visumą. Vadinasi verslo procesų valdymo modelis apima ir pagrindinius ir pagalbinius procesus. Bendras procesų valdymo modelis pateiktas 7 paveiksle.

Mokslininkų D.J.Elzinga ir kt. (2007) teigimu, verslo procesų metodologiją galima išskirti į tam tikrus esminius etapus:

1) Pasiruošimas (*Preparation*). Įmonės verslo sėkmė priklauso nuo tam tikrų vystomų bruožų ir savybių. Labai svarbu numatyti tikslus įmonėje, jiems sukurti vystymosi struktūrą.

2) Procesų parinkimas (*Process selection*). Šio etapo metu įvardijami procesai, kuriems svarbu pateikti išsamią analizę ir galimybes, kaip jie turėtų būti gerinami.

3) Apibūdinimas (*Description*). Įvertinamas ir apibūdinamas procesas, kaip jis vystosi.

4) Kiekybinis įvertinimas (*Qualification*). Tokiame etape įvertinama kiek reikės investicijų, darbo sąnaudų ir laiko įgyvendinti tam tikram pasirinktam procesui;

5) Gerinimo galimybių parinkimas (*Selecting improvement opportunities*). Šiame žingsnyje naudojamos jau sukauptos žinios, kurias naudojant parenkami svarbiausi faktoriai ir bruožai, kurie turi lemiamą įtaką verslo procesams ir įmonės tikslams pasiekti.

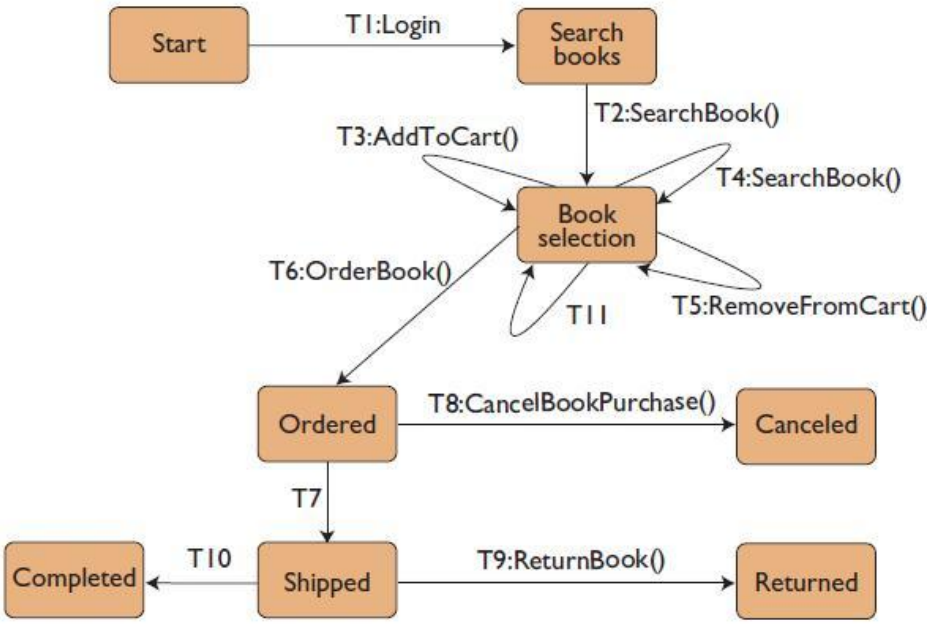
6) Pasirinktų pagerinimų įgyvendinimas (*Implementing improvements*). Šiame etape siekiama įgyvendinti pagerinimus, kurie buvo priimti vieno ar kito proceso tobulinimui. Taip pat ieškoma ir tolimesnių būdų, kaip pagerinti verslo procesus.

Mokslinėje literatūroje pateikiama daug įvairių verslo procesų valdymo tikslų. Tyrėjai A.Juodis ir P.Oržekauskas išskiria ir pateikia du verslo valdymo procesų tikslus:

1) Verslo procesų valdymo tikslas yra atlikti darbą, kurį užsako/ prašo įvykdyti klientas;

2) Verslo proceso valdymo tikslas yra skirti visą dėmesį į kliento pateiktą užsakymą, ji vykdymą ir įmonės tikslą, panaudojant įmonėje turimą įrangą šiam tikslui pasiekti (Juodis, Oržekauskas, 2008).

Įmonėje diegiami ne tik verslo procesai, bet ir tam tikros verslo sistemos. Šios verslo valdymo sistemos apima skirtingus įmonės padalinius į bendrą visumą, kuri tvarko kiekvieno skyriaus individualias veiklas. Suburti atskirus procesus į bendrą darinį (sistemą) yra gana sudėtingas uždavinys. Dažniausiai tam naudojamos bendros programinės įrangos, kurios padeda realizuoti finansines, gamybines, sandėliavimo ar kitas žmogiškųjų išteklių procedūras ir funkcionalumą. Šie atskiri padaliniai naudoja tam tikras savo kompiuterines programas ar jų darbui pritaikytas sistemas. Verslo valdymo sistemos tikslas yra sujungti atskirus įmonės padalinius į bendrą visumą – prie bendros duomenų bazės. Taip užtikrinama, kad informacija visiems padaliniams yra bendra ir jie ja laisvai gali naudotis. Tokios sistemos naudojamos ne tik įprastose įmonėse ir organizacijose, bet ir elektronine komercija užsiimančiose įmonėse. Paprastas pavyzdys internetinio portalo amazon.com verslo portalo schema, kuri pateikta 8 paveiksle.



8 pav. Įmonės veikiančios internetiniame portale verslo procesų principinė schema

Verslo procesų aplinka yra labai dinamiškas reiškinys. Norint, kad įmonė klestėtų ir turėtų savo rinką, reikia gerinti verslo procesus. Verslo procesų kokybės gerinimas siejamas su klientų

poreikių tenkinimu. Procesams gerinti reikia didesnių kaštų, o tai sukelia kapitalo padidėjimo poreikį. Dažnu atveju įmonės mažai suvokia apie verslo procesų pergrupavimą ir jų efektyviai nevykdo, o tai yra klaidingas sprendimas. Patobulinti verslo procesai padidina įmonės pajamas bei vertę. Verslo procesus labiausiai įtakoja:

1) Organizacijos strateginiai tikslai;
2) Valdymo stilius;
3) Turimas kapitalas;
4) Išoriniai veiksniai (įstatymai, konkurencija, rinkos situacija).

Esminės klaidos, kurios susijusios su verslo procesais ir pasitaiko daugelyje įmonių yra susijusios su tuo, kad daugelio organizacijų vadovai siekia ženklaus ir ryškaus verslo procesų pagerėjimo, tačiau neįdeda tinkamų pastangų. Labiausiai nesėkmes įtakoja tai, kad „*vadovybė nesuvokia verslo proceso tobulinimo esmės ir tikslų*“ (Repin, 2004).

Apibendrinant verslo procesų valdymą galima teigti, kad autoriai verslo procesų valdymą, kaip ir verslo procesus suvokia gana skirtingai. Išanalizavus mokslinę literatūrą galima teigti, kad verslo procesų valdymas susideda iš procesų žingsnių planavimo, valdymo (organizavimo) ir kontrolės. Verslo procesų valdymo tyrimų objektas apima pagrindinius ir pagalbinius procesus.

2.3 KIBERNETINIO SAUGUMO SVARBA VERSLO PROCESUOSE

Šiuolaikinėje globalioje erdvėje įmonės yra įtakojamos daugelio sparčiai vykstančių pokyčių, prie kurių turi prisitaikyti. Informacinėje aplinkoje atsiduria ne tik įvairūs duomenys, kurie susiję su įmonės vykdoma veikla, bet ir informacija iš kitokių vidinių ir išorinių šaltinių. Kompiuterinėse sistemose dalyvauja ne tik įmonės, kurios keičiasi informacija, bet ir daugeli kitų dalyvių. Atsiranda „*bendras vystymasis kartu su išorine aplinka, o tai įtakoja organizacijas rūpintis informacijos saugumu, taikymu ir dalijimusi* (Polley, 2007).

Informacija šiomis dienomis yra apibrėžiama kaip vienas iš svarbiausių ir vertingiausių išteklių. Tinkamai suprantama ir valdoma informacija turi daug įtakos verslui ir jo procesams. Informacija nuosekliai naudojama versle, nes kiekvieno proceso metu gaunama ar naudojama įvairaus tipo informacija. Informacija yra „*svarbi efektyviam verslo struktūrizavimui, derinimui ir platinimui*“ (Weesing, 2015).

Labai svarbu, kad informacija būtų ne tik kokybiška, bet ir saugi. Ar informacija kokybiška ir vertinga dažniausiai sprendžia jos vartotojas, o „*informacijos specialistas turi įvertinti informacijos atitikties šaltinį ir būdą, kuriuo yra perduodama informaciją*“ (Atkočiūnienė, 1998).

Kokybiška ir saugi informacija – tai visuma informacijos savybių ir jos rodiklių, kurie atitinka informacijos vartotojų lūkesčius ir keliamus reikalavimus. Informacijos kokybei yra būdingos charakteristikos, kurias galima ištirti ir išmatuoti. Svarbiausi informacijos vertės rodikliai yra grupuojami į tokias kategorijas: esminė informacijos kokybė (tikslumas ir objektyvumas, patikimumas); prieinamumo kokybė (saugumas) bei informacijos reprezentatyvumas. Analizuodami šiuos informacijos kriterijus mokslininkai akcentuoja, kad „*labai svarbu kad informacija naudojama versle būtų kokybiška ir tiksli. Jei įmonė naudoja nekokybišką informaciją, tai ji negali veiksmingai valdyti savo verslo*“ (Ruževičius, Gediminaitė, 2007).

Informacija yra kaupiama ir disponuojama daugelyje įmonių. Kai kurios jų yra svarbios komerciniu atžvilgiu, todėl jos informaciją turi ypatingai saugoti. Gali būti išskiriami kriterijai, kurie apibrėžia, ar informacija yra konfidenciali ir svarbi komerciniu atžvilgiu:

1) Tokios informacijos saugojimui pasitelkiamos išskirtinės apsaugos priemonės;
2) Dėl informacijos praradimo, paviešinimo įmonė gali patirti žalą;
3) Prie tokio pobūdžio informacijos gali prieiti tik ribotas kiekis žmonių;
4) Dėl komercinių tikslų tokio pobūdžio informacija turi būti saugojama;
5) Už informacijos paviešinimą numatomos baudos.

Informacinėms sistemoms yra labai svarbūs kompiuteriniai tinklai. Elektroninių ryšių tinklai padeda šiuolaikinėse įmonėse perduoti ir apdoroti didžiąją dalį komercinės informacijos. Šiomis dienomis įmonėse sparčiai mažėja dokumentų popieriniame pavidale, viskas perkeliama į kompiuterines laikmenas. Kompiuteriuose laikoma svarbi informacija. Dėl to informacijos apsaugos problema tampa dar svarbesnė. Žinoma, kad daugelis informacijos, laikomos kompiuteriuose yra slapta arba ribojamo naudojimo.

Įvairaus pobūdžio organizacijose informacija yra labai svarbi ir vertinga. Informaciją įmonėse gali apimti žinias apie nebrangius tiekėjus ir pasiturinčius klientus, įvairias komercines paslaptis ir operatyvinę informaciją, kuri leidžia įmonei būti tinkamai kontroliuojamai ir besivaržančiai nuolat vystančioje verslo aplinkoje. Informacija labai įtakoja tai, kaip įmonė gali kovoti su konkurencija. Turima informacija tampa svarbi ne tik organizacijos valdžiai ir jos atstovams bet ir konkurentams.

Didelėse įmonėse dažnai egzistuoja sukurti informacijos saugumo skyriai, kurie apima įmonės teritorijos fizinį saugumą, filtruoja svetaines, kuriose gali lankytis tos įmonės darbuotojai, archyvuoja ir saugo konfidencialią įmonės informaciją. Taip pat šiems skyriams priskiriamos ir konkurentų stebėjimo ir analizės funkcijos.

Labai daug verslo procesų yra atliekami naudojant kompiuterinę įrangą, o tai yra labai svarbu šios įrangos eksploatavimui, priežiūrai, taisymui bei atnaujinimui. Kiekviena įmonė siekia patikimų veiklos pasiekimų naudojant šiuolaikinį ir skaitmeninį informacijos perpildytą verslo pasaulį. Organizacijoms svarbu turėti naujas informacines technologijas, kurios leistų optimizuoti ir pagreitinti verslo procesą. Jei procesas yra automatizuojamas jis gali pagerinti rizikų valdymą, atlikti mažiau klaidų, kurios yra siejamos su žmogiškojo faktoriaus klaidomis. Automatiniame procese taip pat gali būti matuojami verslo procesai, renkami ir analizuojami duomenys, o tai tampa labai svarbiu informacinių technologijų įrankiu, kuris leidžia būti konkurencingu verslo sektoriuje. Organizacijos konkurencingumui ir kultūriniam klimatui palaikyti yra svarbus informacinių technologijų įrangą ir nuolatinis verslo procesų ciklinis vykdymas, prižiūra, tvarkymas ir palaikymas.

Informacijos saugumui versle yra keliami specialūs reikalavimai. Pagrindiniai reikalavimai keliami saugiai informacijai yra apibrėžiami tokiais aspektais:

1) Slaptumas. Keičiantis informacija, tikimasi kad išsiųstus dokumentus naudos ir gaus gavėjai. Tai aktualu, jei keičiamasi svarbiais duomenimis: kreditinės kortelės numeris, gyvenamosios vietos adresas;
2) Autentiškumas turi garantuoti, jog gaunami autentiški dokumentai, kuriuos gauna gavėjas, kontaktavęs su siuntėju;
3) Efektyvumas turi užtikrinti, kad informacijos saugumas užtikrintų našią veiklą įmonėje, ir kad jis nesumažėtų.

Autoriai išskiria tam tikrus netinkamai valdomų, neefektyvių informacinių sistemų valdymo problemas įmonėje.

5 lentelė Informacijos valdymo problemos versle

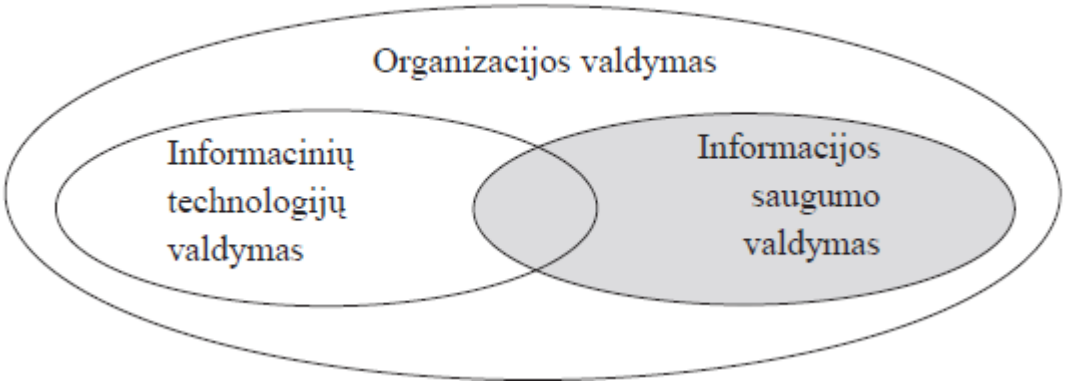
Problema	Charakteristika
Trūksta automatizacijos	Trūksta automatinių verslo procesų valdymo, kuris padėtų sutrumpinti laiko sąnaudas, tobulintų kokybę ir leistų geriau patenkinti klientų poreikius. Įmonės darbuotojai skiria daug laiko duomenų ieškojimui ir įvedimui, jos perdavimui, operacijų tikrinimui.
Klaidingai priimami sprendimai	Nemažai įmonių priima klaidingus sprendimus, nes neturi priėjimų prie tinkamų duomenų ir analitinės informacijos.
IT neatitinka vykdomos veiklos	Verslas ir jo procesai kartais keičiasi labai greitai, o specialistai nespėja atnaujinti sistemas, kurios naudojamos darbui atlikti.
Nekokybiški veiklos sprendimai	Automatizuoti veiklos procesai sugeneruoja didelius

	duomenų kiekius, todėl trūksta laiko teisingam sprendimui priimti.
Sudėtinga veikla	Reikalavimai, kurie nuolat didėja verslo sektoriuje keičia iš dalies ir jo pobūdį (priklausomybė nuo įvairių veiksnių); dideli duomenų srautai kuriuos reikia apdirbti ir priimti sprendimus.

(Kalibaitė, 2011)

Informacijos saugumas labai svarbus įmonės informaciniam turtui. Informacinis turtas pažeidžiamas įmonėje, jei nepakanka saugos priemonių įmonėje, arba jos yra visiškai netaikomos. Informacija gali būti pažeidžiama skirtingai visose įmonėse. Šių pažeidimų lygis yra įtakojamas tokių veiksnių:

1) Informacijos jautrumas;
2) Darbuotojų sugebėjimas reaguoti į informacijos saugumo pažeidimo incidentus;
3) Institucijos ir įstaigos galimybė aptikti pažeidimus;
4) Darbuotojų moralė;
5) Darbuotojų išprusimas informacijos saugos srityje;
6) Esamos informacijos saugos procedūros.



9 pav. Įmonės valdymo sąsajos su informacijos saugumu ir technologijomis

Lietuvių mokslininkas S.Jastiuginas (2009) savo darbuose bandė akcentuoti ir pabrėžti informacijos saugumo svarbą verslo įmonėse. Mokslinėje literatūroje akcentuojama, kad informacijos saugumo valdymo sampratoje informacijos saugumas ir jo taikymas visoje įmonėje sugretintas su informacijos technologijų valdymu yra sudėtinė visos įmonės valdymo dalis. Bendras tarpusavio ryšys tarp informacinių technologijų, informacijos saugumo ir įmonės valdymo yra pateikiamas 9 paveiksle.

Norint užtikrinti verslo informacijos saugumą, galima naudoti tokias technines informacijos saugos priemones:

1) Įdiegti ir palaikyti ugniasienę. Organizacijų kompiuteriniuose tinkluose yra daug vertingos ir svarbios informacijos, kuri gali būti lengvai pasiekiama kitų asmenų. Labai svarbu kad būtų numatomos lėšos geros ugniasienės palaikymui įmonėje;

2) Apsaugoti verslą nuo kompiuterinių virusų. Sumažinama rizika apkrėsti virusais įmonės kompiuterius. Labai svarbu atnaujinti šias programas. Organizacijos darbuotojai turėtų mokėti dirbti su jomis ir jas atnaujinti;

3) Diegti modernias dokumentų kopijų sudarymo sistemas. Jei įmonėje padaromos svarbių dokumentų kopijos, nutikus kokiam nors informacijos incidentui, turint informacine prasme svarbias kopijas galima lengviau grįžti į darbo vėžes ir panaikinti dėl to atsiradusias pasekmes;

4) Siekti, kad darbuotojai būtų sąžiningi. Tai svarbu tam, kad jeigu informacija patenka į nesąžiningo darbuotojo rankas, tai gali sukelti neigiamų padarinių įmonėje. Tokiu atveju, kai kuriose įmonėse gali būti diegiama dokumentų naudojimo sekimo programa, kuri stebi, kaip kontroliuojami informacijos srautai įmonėje, kokie dokumentai naudojami.

Kai kuriose įmonėse vadovai nelinkę per daug investuoti į įmonių informacinį saugumą. Tai reiškia, kad labai pasitikima esama situacija o kartu ir kompiuteriniais tinklais, informacinėmis technologijomis. Pervertinamos galimybės kartais neduoda teigiamų rezultatų.

Kartais įmonėse pasitaiko, kad prie kompiuterinių tinklų ir informacijos jungiamasi ne organizacijos viduje, bet per atstumą. Kartais tuo naudojasi ir kompanijų klientai ar verslo partneriai. Tokiu atveju svarbu, kad būtų atsižvelgiama į tokias charakteristikas:

1) *Vartotojų atpažinimą.* Jos metu vartotojai lengviausiai atpažįstami taikant vienkartinių slaptažodžių atpažinimo sistemą;

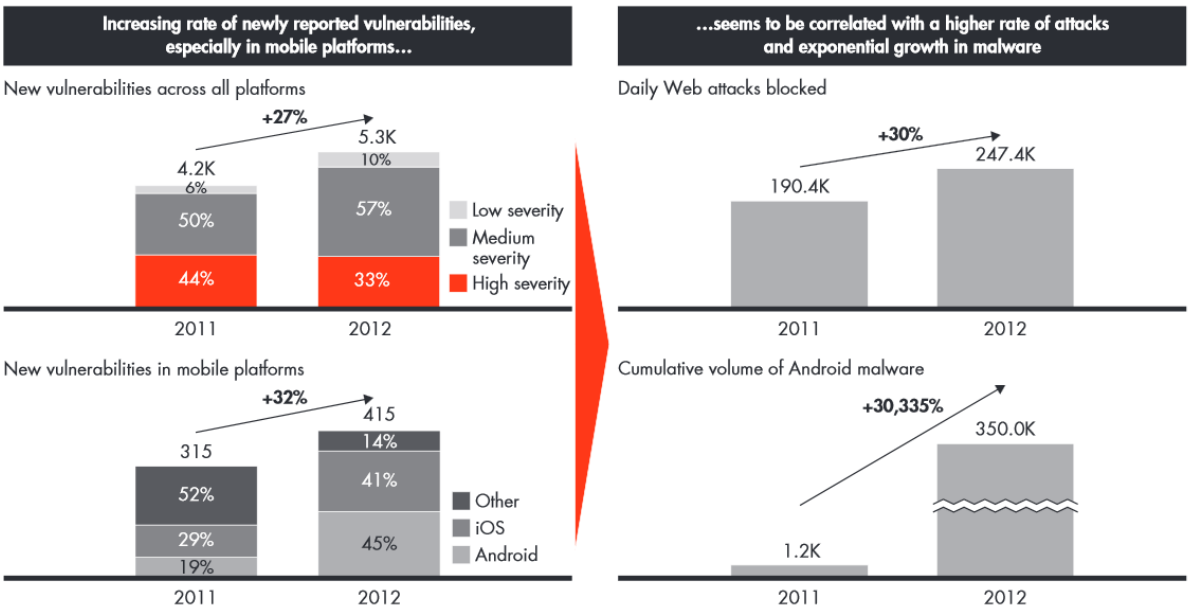
2) *Apsauga nuo įrenginio iš kurio jungiamasi*. Proceso metu siekiama užtikrinti, kad įrenginys iš kurio jungiamasi būtų saugus ir kad nėra paliekama jokia šalutinė informacija, kuri gali trikdyti įmonės veiklą vėlesnėje ateityje.

3) *Duomenų apsauga juo perduodant*. Tokiam užtikrinimui dažnai naudojamas privatus virtualus tinklus (VPN).

4) *Tinklo prieigos ribojimas*. Naudojamos priemonės, kurių pagalba ribojami priėjimai prie tinklo, o tai apsaugo informaciją ir duomenis.

5) *Vartotojų teisių ir nuolatinės prieigos valdymas.* Čia siekiama kontroliuoti, kokia informacija prisijungęs vartotojas gali naudotis, o kokia ne. Kartais nutinka taip, kad vartotojai yra linkę prisijungti prie neleistinos informacijos. Tokios problemos sprendimas – valdyti vartotojų teises.

Pažymėtina, jog kibernetinio saugumo vertinimas ir poreikio būtinybė valdant verslo procesus grindžiama pastarojo dešimtmečio metu išaugusių atakų, sukčiavimo atvejų skaičiumi. Praktikoje pastaruoju metu esmine nuostata, kurios laikomasi kibernetinio saugumo diegimo metu, tampa betarpiškas kibernetinį saugumą užtikrinančių priemonių taikymo užtikrinimas (angl. *security by design)* – tai itin aktualu kuriant ir diegiant naujus produktus, atnaujinimus. Kiekvienas neteisėtas duomenų panaudojimas įmonėms kainuoja realias išlaidas. 10 pav. pateikiama dar 2011-2012 m. registruotų atakų, įsilaužimų statistika (duomenis registruoja ir renka MITRE CVE; Symantec; Trend Micro; Bain kompanijos).



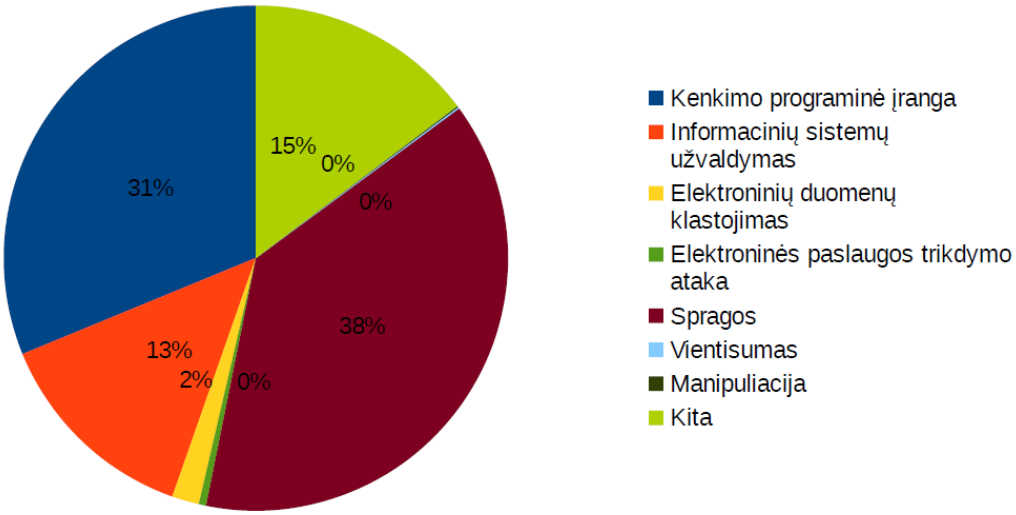
10 pav. Kibernetinio saugumo iššūkiai: atakų ir įsilaužimų dinamika 2011-2012 m.

Vertinant Lietuvos Respublikos mastu, pažymima, jog Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) 2014 m. ištyrė 36136 incidentus pagal pranešimus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų. Palyginti su 2013 m. (25 337 pranešimai), pranešimų buvo gauta 43 proc. daugiau. 6 lentelėje ir 11 pav. pateikiamos nagrinėtų pranešimų pagal tipus suvestinės.

6 lentelė. Nagrinėti pranešimai pagal jų tipus

Pranešimų pobūdis	2014 metų laikotarpis				
	I ketv.	II ketv.	III ketv.	IV ketv.	iš viso
Apie kenkimo programinę įrangą	2 820	2 412	2 807	3 237	11 276
Apie informacinių sistemų užvaldymą	1836	526	1 122	1 369	4 853
Apie elektroninės paslaugos trikdymo atakas	43	35	45	42	165
Apie elektroninių duomenų klastojimą	121	81	220	208	630
Apie vientisumo pažeidimus	19	11	5	0	35
Apie įrenginių saugumo spragas	1 673	3 310	3 647	5 197	13 827
Apie manipuliaciją elektroniniais duomenimis	13	5	8	6	32
Kita	850	993	1 712	1 763	5 318

(CERT-LT, 2014)

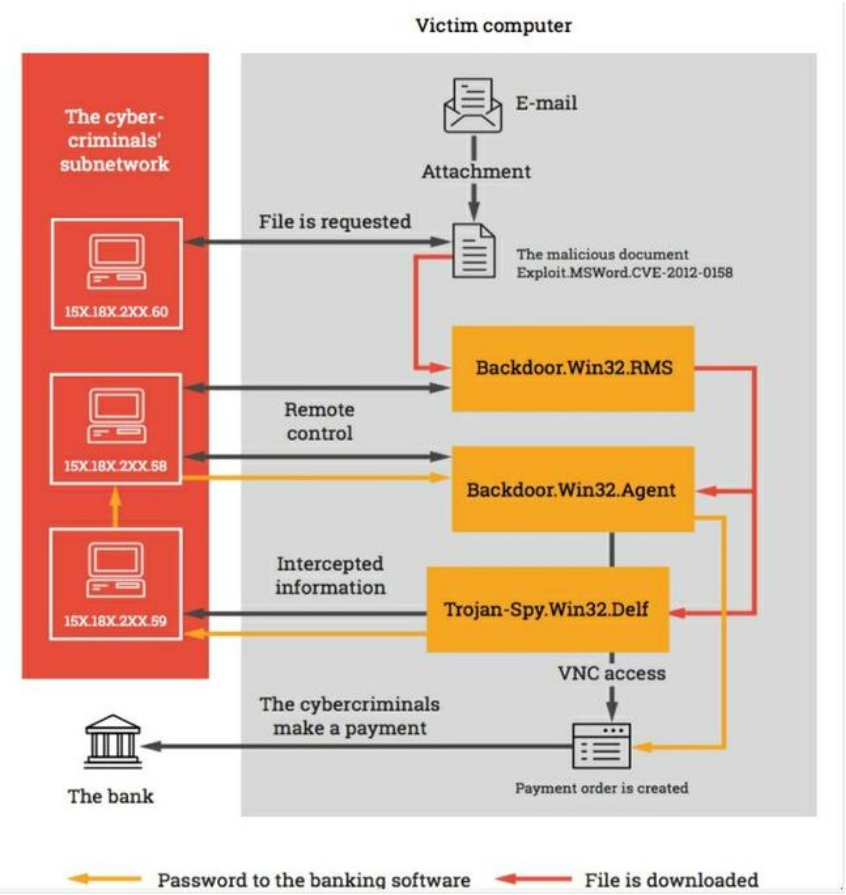


11 pav. CERT-LT 2014 m. gautų ir siųstų pranešimų tipai (Saugumo incidentų tyrimo skyriaus (CERT-LT) 2014 metų veiklos ataskaita' [2015])

Akcentuotina, jog kibernetinio saugumo svarba verslo procesuose turėtų būti grindžiama vien tik galima potencialių nuostolių žala – įmonės turėtų įvertinti maksimalius nuostolius ir atkreipti dėmesį į prevencines priemones.

Statistika grindžiama konkrečiais pavyzdžiais – dažniausiai tiek fizinių, tiek juridinių asmenų veikloje susiduriama su nuotolinio bankinio aptarnavimo sistemų (NBA) atakomis. Paprastai bankų IT infrastruktūra gerai apsaugota, todėl kibernetiniai nusikaltėliai stengiasi užvaldyti NBA sistemą iš kliento pusės, o jų pagrindiniu tikslu tampa buhalteriai, turintys reikalingus duomenis ir prieigos prie NBA sistemos teises. Sėkmės atveju apgavikai gauna galimybę valdyti visas bendrovės lėšas. Paprastai aukos apie įvykdytą ataką sužino paskutinės – apie lėšų nurašymą nuo bendrovės sąskaitos. Vis dėlto, šiuo metu daugelis įmonių yra įsitikinę, jog

tokių incidentų mažėja – tinkamai taikant specialą įrangą, reikalaujančią slaptažodžio ir specialaus rakto prie NBA sistemos prieigos, o mokėjimo siuntėjo IP adresas buvo tikrinamas banko. Vis dėlto, praktika liudija, jog minėtos priemonės nebėra patikimos, o kibernetiniai incidentai vis labiau agresyvėja ir tampa labiau išmanūs. Vienas iš tokių atvejų – „Kaspersky Lab“ specialistams ištyrus nukentėjusios bendrovės buhalterio kompiuteryje aptiko teisėtą programą „Remote Manipulator System“ (Prokhorenko, 2015). Aptikta programos versija modifikuota – ji leido apgavikams ne tik valdyti kompiuterį nuotoliniu būdu, bet ir parsiųsti į jį kitą kenkėjišką programinę įrangą (kibernetinio incidento schema pateikiama 12 pav.).



12 pav. Kibernetinio incidento nuotolinio bankinio aptarnavimo sistemose mechanizmas

Paaiškėjo, kad apgavikai taikė socialinės inžinerijos metodus. Buhalterijai tariamai mokesčių inspekcijos vardu siųstame laiške buvo raginama skubiai apdoroti pranešimą, o paleidus laiškė buvusią programą, iškart užkrečiamas kompiuteris. Gavę pilną ir nepastebimą buhalterio kompiuterio kontrolę, nusikaltėliai papildomai įdiegdavo klaviatūros paspaudimų registravimo programą (angl. *Keylogger*), kad sužinotų prieigos prie NBA sistemos slaptažodį. Tada apgavikams teliko suformuoti ir per sistemą įvykdyti mokėjimo pranešimą buhalterio vardu – raktas ir siuntėjo IP adresas buvo teisėti.

Kitas verslo procesuose pasireiškiančių kibernetinių grėsmių pavyzdys – DDoS (angl. *Distributed Denial of Service* – paskirstytas atsisakymas aptarnauti) – tai atakų prieš kompiuterines sistemas būdas („LMA Technikos mokslų skyrius surengė diskusiją „Kibernetinis saugumas“, 2015). Jo tikslas – sukurti tokias sąlygas, kad teisėtiems sistemos naudotojams jos ištekliai taptų neprieinami ar gaunami apsunkintai. Dažnai naudojamas kompiuterių–zombių tinklas (angl. *botnet*) – grupė tinkle esančių kompiuterių, užkrėstu specialiu kodu (botu), suteikiančiu galimybę nuotoliniu būdu juos valdyti. Paprastai naudojami DDoS atakų rengimui arba brukalams siųsti.

Pažymėtina, jog tokių atakų atsako valdymas verslo procesuose turėtų būti vykdomas, o verslo procesai analizuojami keliamų rizikų kontekste, nustatant prioritetines sritis, kurių apsauga yra svarbiausia.

Maža to, kibernetinio saugumo priemonių diegimui ir tobulinimui būtinas lyderystės elementas organizacijoje – turi būti paskirtas atsakingas asmuo, kuris inicijuotų naujausių gerosios praktikos priemonių diegimą ir adaptaciją. Vertinant verslo procesus kaip visumą organizacijos lygmenyje, būtina būti nuolat pasirengus iššūkiams bei reaguoti į juos viduje ir išorėje, t.y. imantis vidinių atsakomųjų priemonių bei inicijuojant institucinius pakeitimus.

3.KIBERNETINIO SAUGUMO UŽTIKRINIMO ĮTAKA VERSLO PROCESAMS

Šiame skyriuje nagrinėjami pagrindiniai kibernetinio saugumo užtikrinimo įtaką verlo procesuose lemiantys veiksniai bei detalizuojami kibernetinio saugumo valdymo metodai verslo procesuose.

3.1 PAGRINDINIAI VEIKSNIAI LEMIANTYS INFORMACIJOS IR KIBERNETINĮ SAUGUMĄ VERSLO PROCESUOSE

Informacija yra turtas, turintis konkrečią, aktualią vertę, kuri smarkiai įtakoja organizacijos veiklos efektyvumą. „*Egzistuojančios įvairios technologijos padeda kaupti, dalinis, parduoti ir keistis informaciją“ (*Varney, 1996). Labai svarbu užtikrinti informacijos saugumą, nes ji tampa kasdien organizacijoje naudojamu įrankiu. Įmonės turi apibrėžti grėsmes ir pažeidimus, kurie įtakoja verslo procesus.

A.S.Y.Cheung teigia, kad nors internetas daugeliui žmonių sudarė iki tol neturėtas prieinamumo, betarpiškumo, anonimiškumo galimybes, bet kartu tapo iššūkiu žmogaus teisėms, asmens ir visuomenės saugumui (Cheung, 2009). Elektroninių nusikaltimų ypač sparčiai pradėjo gausėti nuo pasaulinės finansų krizės pradžios, kai nemažai IT profesionalų neteko darbo. 2011 m. atliktų tyrimų rezultatai rodo, kad dėl kibernetinio nusikalstamumo pasaulyje kasmet prarandama apie 388 mlrd. JAV dolerių (Norton Cybercrime Report 2011, 2015). Elektroniniai nusikaltimai virtualiai daro poveikį beveik visiems šalies gyventojams ir beveik visoms įmonėms ir organizacijoms. Ekonominiai ir kiti kibernetiniai nusikaltimai jau kuris laikas kelia rimtą grėsmę tiek viešajam saugumui, tiek nacionaliniam saugumui, tiek globaliam saugumui elektroninėje erdvėje. Šioje situacijoje jau nepakanka, kad valstybė dalyvautų kibernetinės erdvės saugumo užtikrinime vien kurdama ir/ar tobulindama teisinę bazę. Neišvengiamas jos dalyvavimas ir ekonomine prasme - kuriant viešąsias gėrybes, kurios ne rinkos sąlygomis kuriamos efektyviau nei rinkos.

B.H.Kobayashi teigia, kad „*kibernetinės erdvės saugumas yra kompleksinė ekonominė realybė, kurios rinkos pusiausvyra ekonomiškai pagrįstais kaštais ir optimaliomis investicijomis pasiekiama tik tada, kai gerai sukoordinuota ir subalansuota viešosios ir privačios gėrybės gamyba. Jos apimtys priklauso nuo kibernetinių atakų skaičiaus“* (Kobayashi, 2006). Priešingu atveju ekonominiai kaštai ir investicijų dydis nėra optimalūs, ir juntama perteklinės produkcijos tendencija.

R.Von Solms pabrėžia, kad „*informacijos saugumas įmonėse vystėsi per tris etapus: pirmasis etapas prasidėjo 1960-aisiais, informacijos saugumas labiausiai rūpinosi užtikrinti ir*

kontroliuoti fizinį saugumą įmonės patalpose; antrajame etape nuo 1970 – ųjų informacinis saugumas taikėsi prie konkrečių atskirų organizacijų poreikių; trečiojo etapo metu, organizacijos turi susieti naudojamas informacines technologijas ir pereiti iš uždarų aplinkų organizacijoje į sudėtingesnes ir platesnes tinklų aplinkas." (Von Solms, 1996). Naudojant kompiuterines technologijas ir tinklus įmonių veikloje bei vykdomuose verslo procesuose, būtina naudoti saugos priemones, kurios užtikrina ir palaiko informacijai keliamus reikalavimus. Informacijos saugumas turi užtikrinti žmonių ir su verslo informacija susijusį konfidencialumą ir apsaugą, nuo įvairių vagysčių ar dokumentų paviešinimo.

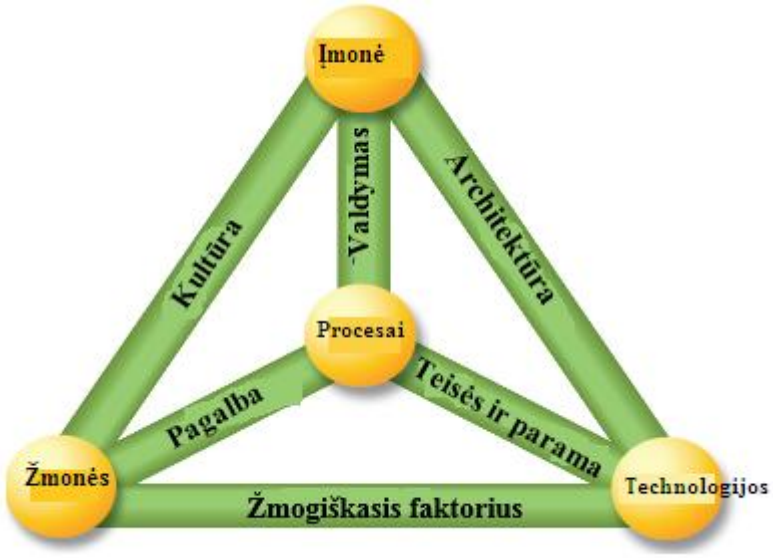
Įmonėje vystant verslo procesus turi būti laikomasi tam tikrų saugumo standartų, informacijos saugumo priemonės turi būti nuolat atnaujinamos ir tobulinamos, nes gali atsirasti informacijos pažeidžiamumo rizika. Europos Sąjungos priimtos direktyvos ir reglamentai apibrėžia informacijos saugumo kriterijus ir standartus. Šie dokumentai yra svarbūs ne tik Europos Sąjungos narėms, bet ir individualioms įmonėms, nes jais besiremdamos įmonės privalo savo viduje diegti informacijos saugumo technologijas ir standartus (European Commission: 2009). Šiuo metu naujausios išleistos Europos Sąjungos institucijų saugumo direktyvos yra šios:

- ✓ 9.1 Regulation (EC) 300/2008 – Europos Parlamento ir Tarybos reglamentas dėl pagrindinių taisyklių civilinės aviacijos saugumo sferoje.
- ✓ 9.2 Direktyva 95/46/EC – Individų saugumas apdorojant jų asmeninius duomenis ir jų laisvame judėjime.
- ✓ 9.3 Direktyva 2002/58/EC – Asmeninių duomenų apdorojimas ir privatumo apsauga elektroninėje komunikacijos sferoje. (Privatumo ir elektroninio komunikavimo direktyva).
- ✓ 9.4 COM(2007) 251: Privatumą apsaugančių technologijų duomenų apsaugos populiarinimas (PETs).

Tyrinėdamas informacinius saugos auditus, autorius A.Januta (2015) pabrėžia, kad informacijos saugos užtikrinimo procesą versle galima išskirti į tam tikras kelias dalis:

- ✓ Objektų, galinčių sulaukti pavojų nustatymas;
- ✓ Esančių ir galimų pavojų išaiškinimas;
- ✓ Galimų pavojaus šaltinių nustatymas;
- ✓ Rizikos analizė;
- ✓ Neigiamo poveikio šaltinio suradimo metodai ir priemonės;
- ✓ Apsaugos nuo žinomų pavojų metodai ir priemonės;
- ✓ Reagavimo į incidentus metodai ir priemonės.

Tyrėjas L.Kiely (2006) sukūrė ir aprašė verslą ir verslo procesus įtakojantį informacijos saugumo modelį. Šis modelis padeda įtvirtinti įvairias tiek informacijos saugumo, tiek kibernetinio saugumo koncepcijas visame pasaulyje. Nagrinėjamame modelyje pateikiamas į verslą orientuotas požiūris susijęs su informacijos saugumo užtikrinimu ir valdymu. Išvystytas holistinis ir dinamiškas požiūris į informacijos saugumą verslo kontekste parodė, kad informacijos saugumas gali būti nuspėjamas ir valdomas. Su verslu susijęs kibernetinio saugumo modelis gali būti taikomas įvairiose įmonėse nepriklausomai nuo jos dydžio ar saugumo. Taikomo kibernetinio saugumo modelio verslo procesuose bendroji schema pateikiama 11 paveiksle.



11 pav. Informacijos saugumo modelis verslo įmonėje

Pateikiamas informacijos saugumo modelis gali būti apibūdinamas kaip trijų dimensijų, turintis piramidės formos struktūrą, sudarytą iš šešių tarpusavyje susijusių elementų. Visi modelį sudarantys elementai sąveikauja tarpusavyje. Jei bent vienas modelio narys yra pakeičiamas ar valdomas netinkamai, modelio pusiausvyrai gresia pavojus. Šios gana dinamiškos jungtys labai jautriai reaguoja į pokyčius įmonėje, todėl modelis turi sparčiai prisitaikyti.

Esminiai keturi elementai, kurie sudaro modelį yra organizacija (įmonė), žmonės, procesai, technologijos.

Organizacija suburia žmones, kurie turi dirbti įmonės naudai siekiant bendrų tikslų. Įmonės strategija apibrėžia, kokie jos verslo tikslai ir uždaviniai turi būti pasiekti. Žmogiškasis elementas apibrėžia žmogiškuosius išteklių ir saugumo klausimus ir kas vyksta aplink juos. *Žmogiškajam* elementui labai svarbu apibrėžti elgesio vertybes ir galimus žalingus nukrypimus. *Procesai* apima formalius ir neformalius mechanizmus, kurie turi užtikrinti gyvybiškai svarbų ryšį su visomis

dinaminėmis jungtimis. Procesai kyla iš įmonės strategijos ir įgyvendina dalį įmonės veiklos elementų. Technologijos elementas apima visus įrankius, taikomąsias programas ir infrastruktūrą, kurie skatina efektyviai veikti procesus. Procesų elementai ypač sparčiai vystosi, dėl to įmonės yra labai priklausomos nuo technologijų, nes jos yra svarbi verslo procesų dalis.

Autoriai savo darbe išskiria veiksnius, kurie jų manymu yra svarbūs norint pagerinti kibernetinį saugumą versle:

1) Informavimas ir mokymas;
2) Valdymo pagalba;
3) Biudžetas;
4) Informacijos saugumo politikos įgyvendinimas ir pritaikymas;
5) Įmonės vizija.

Informavimas ir mokymas. Visose įmonėse yra siekiama apsaugoti informacija kuri įvairiais aspektais siejasi su verslu. Organizacijos vadovai teigia, kad informacijos saugumas gali būti pasiektas padidinus įmonės darbuotojų informuotumą ir rengiant mokymus. Tyrėjas J.A.Kemmerrer (2003) savo darbe akcentuoja, kad organizacijos turi nuolat vykdyti švietimo ir mokymo programas, kurios padėtų pasiekti ir įgyvendinti informacijos saugumo politikas. Darbuotojų informavimo stoka gali susilpninti net stipriausias saugumo priemones.

Valdymo pagalba. Daugelyje organizacijų suvokiama ir laikoma, kad informacijos skyrius ar su informacija dirbantis asmuo yra atsakingas už jos saugumą. Tai patvirtina ir autoriaus P.Fung keliamas mintis, kad *„paprastai įmonės valdžia nesikiša į informacijos saugumo užtikrinimo procesus, nes mano, jog tuo turi rūpintis informacinių technologijų skyrius, kuris turi parinkti tinkamas technologijas, instaliuoti reikalingą įrangą, kuri išlaikytų organizacijos informacijos saugumą*“ (Fung, 2002). Laikomasi nuomonės, kad elgesys ir požiūris į saugumo užtikrinimą bus labiau išreikštas, jei aukščiausioji organizacijos vadovybė parodys susirūpinimą informacijos saugumu. Valdžia nerems informacijos saugumo iki kol neįsitikins, kad informacinis saugumas smarkiai įtakoja ir teigiamai veikia pagrindines verslo funkcijas.

Biudžetas. Kai kurie tyrėjai akcentuoja, kad įmonės turimas biudžetas yra labai svarbus aspektas, siekiant įgyvendinti informacijos saugumą organizacijoje. Nesant tinkamo biudžeto, organizacija negali būti aprūpinama pakankamais ištekliais, kurie užtikrintų informacijos saugumą. Tyrėjas F.Bjorck apibūdina biudžetą, kaip *„finansinį įrenginį, kuris racionaliai įvertina išlaidas ir įvertina galimybę, kuri yra reikalinga ištelkiamas, norint sėkmingai įgyvendinti informacijos saugumą organizacijoje*“ (Bjorck, 2002).

Informacijos saugumo politikos įgyvendinimas ir pritaikymas. Informacijos saugumo politika yra planas, identifikuojantis organizacijai labai svarbų turtą − informaciją. Ši politika taip pat pateikia paaiškinimus, kas yra ar būtų priimtina, nepriimtina ir kaip turėtų elgtis darbuotojas, kad būtų siekiama užtikrinti informacijos saugumą organizacijoje. Informacijos saugumo politika yra esminis faktorius, kuris užtikrina informacijos saugumo valdymą įmonėje. Informacijos saugumo politikos priėmimas įmonėje yra pradinė priemonė, kurios pagalba siekiama sumažinti informacijos saugumo grėsmes iki minimumo. Pati įmonė saugumo užtikrinti negali. Tai yra „*būtina, bet nepakankama sąlyga organizacijų verslo procesams užtikrinti"* (Hone, Eloff, 2002).

Įmonės vizija. M.Karjalainen, M.Siponen (2014) teigimu, „*pabrėžiant įmonių saugumą (informacinį), įmonės paprastai nieko nedaro iki kol neatsitinka kas nors blogo*". Tuomet įmonė atkreipia dėmesį ir teikia daug pastangų, siekiant atsigauti nuo patirtų nuostolių, nors kartais atsigavimas yra ir visiškai neįmanomas. Kai kurie tyrėjai nurodo, jog aiškūs įmonės tikslai ir uždaviniai yra pasiekiami, jei organizacijoje yra taikoma informacijos saugumo politika bei organizacijoje egzistuoja išvystyta informacijos kultūra, tai įtakoja įmonės verslą ir jo procesų sėkmę. Autoriaus J.A.Lewis teigimu, *„jei organizacijos misija nėra išskirta, tuomet ir toliau vyks kova, kurios metu bus siekiama apsaugoti informaciją, o darbuotojai vengs atsakomybės dėl informacijos saugumo*" (Lewis, 2006).

Mokslinėje literatūroje greta kibernetinio saugumo mikrolygmens elementų vertinami ir makrolygmens veiksniai, kurie funkcionuoja nacionaliniu ir tarptautiniu mastu. Natūralu, jog įmonės, kad ir kaip sėkmingai valdydamos kibernetinio saugumo priemones vidiniuose procesuose, privalo atsižvelgti ir į valstybiniu mastu egzistuojančias tendencijas bei įgyvendinamas priemones.

Reikėtų akcentuoti šias šiuolaikinio pasaulio tendencijas, kurios turėtų padėti suprasti tiek kibernetinio saugumo problemų veikimą, tiek praverstų ieškant adekvataus jų sprendimo:

- didėjantis bendradarbiavimas tarp viešojo ir privataus sektorių paslaugų sektoriuje;
- didėjantis civilinės ir karinės sričių persidengimas;
- politiniai valstybės interesai ir padėtis tarptautiniu mastu.

Šiuo atveju itin daug dėmesio skiriama politiniams veiksniams, viešojo ir privataus sektoriaus bendradarbiavimui. M.Dunn (2009) teigimu, siekiant įvertinti, kuri iš daugybės kibernetinio saugumo užtikrinimu suinteresuotų politinių grupių konkrečiu atveju iškils kaip „laimėtoja", tikslinga atsižvelgti į keletą esminių faktorių:

- platesnį saugumo aplinkos, kurioje formuojasi grėsmės samprata, bruožų, įskaitant technologinį išsivystymą;

- institucinę sąrangą, ypač taisykles, normas, įpročius ir kultūrą;
- platesnį politinį kontekstą, jam priklausančių veikėjų bruožus, įskaitant jų įsitikinimus ir turimus išteklius;
- diskursyvų problemos formulavimo pobūdį.

Politinėje darbotvarkėje, kad ir kokie reikšmingi būtų, saugumo klausimai neatsiduria savaime ir yra priklausomi nuo juos ten įtraukiančių ar pašalinančių veikėjų. Praktiškai tai yra valstybės ir visuomenės elito – politikų, biurokratų, ekspertų, žiniasklaidos, akademikų ir interesų grupių – įtakos rezultatas. Dominuojanti pozicija neabejotinai tenka valdžios elitui: *„saugumo sritis yra ypač smarkiai institucionalizuota, privilegijuojant vyriausybę ir tokias specialiąsias saugumo institucijas kaip žvalgybą ir kariuomenę.“ (Eriksson, Giampiero, 2009).* Įvertinant politinį kontekstą, į kurį patenka su kibernetiniu saugumu susijusi problema, svarbu atsižvelgti, kokios politinės jėgos dominuoja įstatymų leidžiamojoje valdžioje, aljansuose, koalicijose, derybose; kokios preferencijos veda ir kokiomis ideologijomis vadovaujamasi ir pan.

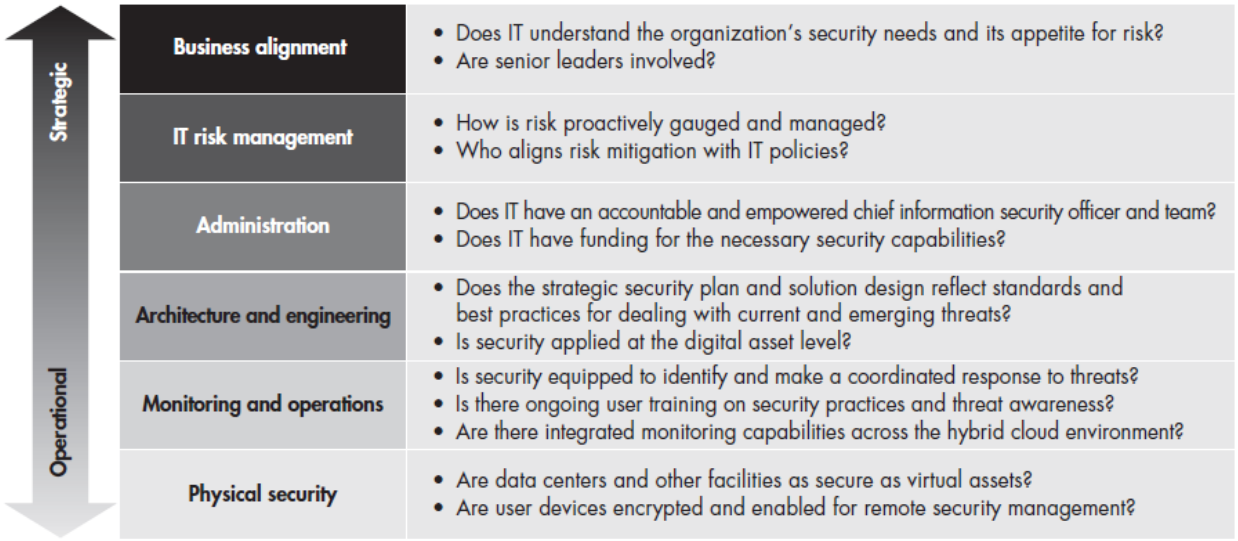
Antrojo operatyvinių tarnybų departamento prie LR Krašto apsaugos ministerijos specialistų teigimu, Lietuvoje artimiausiu metu nesitikima kibernetinių incidentų skaičiaus mažėjimo, o „*pati kibernetinė erdvė išliks viena pagrindinių veiklos erdvių vykdant tiek šnipinėjimą, tiek kitaip veikiant svarbius Lietuvos nacionaliniam saugumui, šalies gynybinei galiai kritinės infrastruktūros objektus*“ (Antrojo operatyvinių tarnybų departamento prie LR Krašto apsaugos ministerijos, 2015). Kibernetinėje erdvėje agresyviai veikiantys subjektai stengsis pasinaudoti valstybės institucijų eksploatuojamų ADA sistemų ir tinklų pažeidžiamumu ir toliau rinksis taikinius, neturinčius tinkamų kibernetinių įrankių / ginklų, išankstinio perspėjimo, aptikimo sistemų, leidžiančių nuolat ir kryptingai užtikrinti kibernetinę gynybą ir jos strategiją, taip pat gebančių laiku nustatyti kibernetinio saugumo efektyvumą bei pašalinti nustatytus trūkumus ir pažeidžiamumą.

Bendrai vertinant veiksnius, garantuojančius kibernetinio saugumo užtikrinimą verslo procesuose verta akcentuoti mikro ir makro lygmenį, nuo kurių atitinkamai priklauso ir taikomų priemonių ypatumai. Makrolygmeniu kibernetinio saugumo užtikrinimą verslo procesuose lemia valstybės dalyvavimo intensyvumas formuojant kibernetinio saugumo politiką, ES priimtos direktyvos ir reglamentai. Šiuo atveju verta akcentuoti didėjantį bendradarbiavimą tarp viešojo ir privataus sektorių paslaugų sektoriuje, didėjantį civilinės ir karinės sričių persidengimą bei politinius valstybės interesus bei padėtį tarptautiniu mastu. Tuo tarpu mikrolygmeniu akcentuotina, jog kibernetinis ir informacijos saugumas gali būti lengvai nuspėjamas ir valdomas. Mikrolygmeniu svarbu tinkamai nustatyti objektus, galinčius sulaukti pavojų, išsiaiškinti esančius ir galimus

pavojus bei jų šaltinius, atlikti giluminę rizikos analizę, nustatyti neigiamo poveikio suradimo metodus bei priemones bei tinkamai raguoti į incidentus. Pažymėtina, jog mikrolygmeniu kibernetinis saugumas užtikrinamas didinant darbuotojų informatyvumą bei rengiant mokymus įvertinant tai, jog darbuotojų informavimo stoka gali susilpninti net ir stipriausias saugumo priemones. Maža to, nesant tinkamo biudžeto, organizacija negali būti aprūpinama pakankamais ištekliais, kurie užtikrintų informacijos saugumą. Informacijos saugumo politikos priėmimas įmonėje yra pradinė priemonė, kurios pagalba siekiama sumažinti informacijos saugumo grėsmes iki minimumo.

3.2. KIBERNETINIO SAUGUMO VALDYMAS VERSLO PROCESUOSE

Kaip jau minėta ankstesniuose skyriuose, tinkamas verslo procesų valdymas užtikrinamas planuojant, valdant, organizuojant bei kontroliuojant. Visų etapų eiga užtikrinama įgyvendinant strateginius ir operatyvinius tikslus. S.Ali, V.Padmanabhan, J.Dixon (2014) strateginius įmonių tikslus, susijusius su kibernetinio saugumo užtikrinimu, siūlo formuoti pagal tam tikrus uždavinius (12 pav.).



12 pav. Kibernetinio saugumo užtikrinimas: strateginiai ir operatyviniai tikslai verslo procesų kontekste. Šaltinis: S.Ali, V.Padmanabhan, J.Dixon. „Why cybersecurity is a strategic issue?“, 2014.

Verslo „vienijimas“ – esminė strateginių tikslų įgyvendinimo priemonė: aktualu, jog IT skyriaus darbuotojai būtų informuojami apie strateginius įmonės tikslus, dalyvautų aptariant juos. Savo ruožtu IT ekspertų nuomonė apie strateginius sprendimus kibernetinio saugumo kontekste turėtų būti itin vertinama įmonės lygmeniu. IT rizikos valdymas organizacijoje turėtų būti

vertinamas itin rimtai, o su kibernetiniu saugumu susijusios rizikos – kaip vienos prioritetinių. Administravimo strateginių sprendimų kontekste būtina suvokti, jog siekiant tinkamo kibernetinio saugumo užtikrinimo įgyvendinimo, IT skyriaus vadovas turi pasižymėti aukštomis kompetencijomis, orientacija bei aukštais įgaliojimais. Tuo tarpu IT komanda organizacijoje turi gauti pakankamą finansavimą ir sulaukti aukšto pasitikėjimo lygio. Kita vertus, operatyviniai tikslai orientuojami į labiau kasdien aktualias sritis. Šiuo atveju ne ką mažiau svarbūs technologiniai sprendimai – svarbu įvertinti, ar turimi technologiniai pajėgumai bei taikomi algoritmai atspindi organizacijos kibernetinio saugumo poreikius, ar taikomos naujausios gerosios praktikos atvejai. Atliekant su kibernetiniu saugumu susijusias operacijas, būtina žinoti, kaip efektyviai atliekama kasdienė stebėsena ir integruotas mišrių duomenų debesijų monitoringas, ar šias operacijas atliekančių darbuotojų kompetencijos ugdomos nuolat. Fiziniai kibernetinį saugumą padedantys užtikrinti atributai taip pat privalo būti įvertinti – būtina įvertinti, kaip apsaugoti techniniai duomenų centrai, kokio šifravimo lygio apsauga yra taikoma darbuotojų kompiuteriuose.

Esminiai kibernetinio saugumo valdymo verslo procesuose etapai, pasak S.Ali, V.Padmanabhan, J.Dixon (2014), turėtų būti koncentruoti į organizacijos pagrindinių procesų nustatymą bei su jais susijusios rizikos tikimybę ir įvertinimą. Įvertinus rizikingumo lygį, tikslinga nustatyti saugumo užtikrinimo spragas. Abiejų elementų įgyvendinimas leistų organizacijai padėti tinkamus pamatus efektyviai kibernetinio saugumo strategijai, kurią privalo pripažinti tiek įmonės vadovybė, tiek darbuotojai. Strategijos efektyvus įgyvendinimas gali būti pasiektas pasitelkiant pripažintus specialistus.

Tuo tarpu McAfee specialistai („White PaperMcAfee Guide to Implementing the 10 Steps to Cyber Security“, 2015) kibernetinio saugumo įgyvendinimą verslo procesų valdyme siūlo įgyvendinti keletu būdu – koreguojant jau priimtą strategiją pritaikius tam tikras korekcijas arba iš naujo formuojant naują strategiją. Pirmuoju atveju siūloma sukurti informacijos saugumo ir rizikos valdymo programą (režimą). Antruoju atveju – kurti verslo valdymo strategiją, kuri būtų paremta visos verslo procesų valdymo sistemos nauja konfigūracija, kuri būtų orientuota į kibernetinį saugumą.

Bendrai vertinant kibernetinio saugumo valdymo nuoseklumą verslo procesuose pažymėtina, jog tokiu atveju garantuojančių veiksnių nepakanka - būtina išgryninti kibernetinio saugumo valdymo modelį konkrečioje įmonėje. Pažymėtina, jog kibernetinio saugumo valdymo modelis grindžiamas keletu esminių nuolat atliekamų tarpusavyje sąveikaujančių veiklų. Verslo vienijimo veikla apima strateginių įmonės tikslų įgyevndinimą įtraukiant visus darbuotojus. Maža to, su kibernetiniu saugumus susijusios rizikos turi būti išskiriamos kaip prioritetinės rizikos

vertinime. Šiuo atveju būtinas suvokimas, jog siekiant tinkamo kibernetinio saugumo užtikrinimo įgyvendinimo, IT skyriaus vadovas privalo pasižymėti aukštomis kompetencijomis, orientacija bei aukštais įgaliojimais. Kasdienė stebėsena ir integruotas mišrių duomenų debesijų monitoringas privalo vykti lygiagrečiai anksčiau paminėtiems procesams. Visi išvardinti procesai garantuoja sėkmingą kibernetinio saugumo užtikrinimą įmonės verslo procesuose.

4. DUOMENŲ IR INFORMACIJOS SAUGUMO ORAGANIZACIJOSE ANALIZĖ

Įvertinus kibernetinio saugumo užtikrinimo verslo procesuose problematiką teoriniu lygmeniu, aktualu nustatyti, kokia kibernetinio saugumo užtikrinimo praktika vyrauja Lietuvos įmonėse. Šiuo tikslu šiame skyriuje atliekamas Lietuvos vidutinių ir mažų įmonių kibernetinio saugumo užtikrinimo situacijos vertinimas, kuris grindžiamas empirinio tyrimo (anketinės apklausos) rezultatais.

4.1.TYRIMO METODOLOGIJA

Šiame baigiamajame darbe nagrinėjama svarbi kibernetinio saugumo įtakos verslo procesams problematika įvairiose įmonėse. Buvo mėginama apžvelgti kibernetinio saugumo problemas privačiose mažose ir didelėse įvairaus pobūdžio įmonėse. Darbe siekiama ištirti, kokiais būdais yra užtikrinamas kibernetinis saugumas, ar taikomi informacijos saugumo lygiai. Kibernetinio saugumo problema yra aktuali įmonėms, nes didelėse įmonėse informacijos saugumas yra sietinas ir su konkurencinga verslo aplinka. Nutekinus informaciją, neapsisaugojant nuo kibernetinių atakų, gali stipriai nukentėti įmonės konkurencingumas.

Darbe atlikta mokslinės literatūros analizė informacijos ir kibernetinio saugumo sampratos tematika, analizuoti ne tik pagrindinės informacijos ir kibernetinio saugumo bruožai ir principai, bet ir problemos, galimos priežastys, dėl ko kyla kibernetinio saugumo incidentai ir kaip juos valdyti.

Šiame skyriuje pateikiama atlikto kiekybinio tyrimo kibernetinio saugumo užtikrinimo lygių analizė. Darbo metu buvo apklausiami įvairiose įmonėse dirbantys asmenys, kurie atsakingi už kibernetinį saugumą. Atliekama šių duomenų analizė ir pateikiami susisteminti duomenys.

Analizės metodui buvo naudojamas kiekybinis tyrimas – elektroninė anketinė apklausa, kurioje dalyvavo skirtingo dydžio įmonėse dirbantys informacinių technologijų specialistai. Kiekybinis tyrimas buvo atliekamas norint nustatyti ir įvertinti informacijos saugumo lygius įmonėse ir juos palyginti tarpusavyje.

Tyrimo problema: sparčiai vystantis informacinėms technologijoms, didėjant informacijos perduodamų duomenų srautams, įvairiose įmonėse susiduriama su informacijos saugos ir kibernetinio saugumo problemomis. Neretai kibernetinio saugumo priemonių taikymas tapatinamas su elektroninių duomenų, informacijos sauga, todėl iki šiol Lietuvos įmonėse pakankamai sudėtinga nustatyti kibernetinio saugumo priemonių taikymo intensyvumą ir paplitimą. Tai savo ruožtu apsunkina verslo procesų saugą kibernetinio saugumo prasme: nepakankamai įvertinamos galimos grėsmės, galimi incidentai bei jų pasekmės tiek įmonės, tiek valstybiniu mastu. Svarbu išanalizuoti ir įvardinti svarbiausias kibernetinio saugumo užtikrinimo grėsmes, su kuriomis susiduriama. Pagal tai galima parengti tam tikras rekomendacijas ir siūlymus kaip reiktų adaptuoti efektyvias kibernetinį saugumą užtikrinančias priemones, įgyvendinti LR Kibernetinio saugumo įstatyme (LR Kibernetinio saugumo įstatymas. 2014 m. gruodžio 11 d. Nr.) numatytas nuostatas, ir kaip galima būtų gerinti informacijos saugojimą įmonėse.

Tyrimo tikslas: įvertinti kibernetinio saugumo užtikrinimo poveikį verslo procesams, saugumo užtikrinimo problemas bei esamą padėtį mažose ir didelėse įvairaus pobūdžio įmonėse.

Uždaviniai:

1) Nustatyti, su kokiais kibernetinio saugumo incidentais susiduriama smulkiose ir vidutinėse įmonėse;
2) Nustatyti, kokiomis priemonėmis bandoma užtikrinti kibernetinį saugumą įmonėse;
3) Nustatyti, kokios fizinės ir elektroninės priemonės taikomos kibernetiniam saugumui užtikrinti;
4) Įvertinti ar įmonėje taikoma informacijos saugumo bei kibernetinio saugumo politika, kokius sprendimus ji apima;
5) Išskirti pagrindines priežastis, kurios sunkina kibernetinio saugumo užtikrinimo problemas;
6) Išanalizuoti, kaip kibernetinio saugumo sistemos veikia verslo procesus įmonėje, kaip kibernetinio saugumo poveikį ir rezultatus yra linkę vertinti įmonių vadovai ir darbuotojai;
7) Nustatyti, ar įmonėse už kibernetinį saugumą yra atsakingas konkretus asmuo ir kokias atsakomybes jis prisiima.

Tyrimo metodai: darbo metu buvo naudojama anketinė apklausa, kuri buvo išsiuntinėta elektroniniu paštu. Tyrimo anketa sudaryta iš uždarų klausimų. Anketinė apklausa analizuojama ir pateikiami bendrieji gautų rezultatų pasiskirstymai;

Duomenų rinkimas: tyrimui atlikti buvo naudojama elektroninė apklausa. Šiam metodui tinkamai įvykdyti svarbu nustatyti reikiamą apklausti dalyvių skaičių. Duomenims rinkti dėl nedidelių kaštų ir patogumo buvo pasirinktas informacijos rinkimo būdas elektroniniu paštu.

Tyrimo objekto elementas (imties vienetas): mažos ir didelės įvairaus pobūdžio įmonės, kurios savo veikloje naudoja elektroninių tinklų, interneto, informacinių technologijų paslaugas.

Tyrimo imties dydis: siekiant išsiaiškinti, kiek įmonių vadovų reikia apklausti, buvo taikoma matematinė analizė. Pagal I.Paniott formulę apskaičiuota respondentų imtis. Pagal Lietuvos Statistikos departamento duomenis Vilniaus mieste 2014 metais buvo įregistruota 6205 mažų ir vidutinių įmonių.

Respondentų imtis apskaičiuojama pagal V. I. Paniotto formulę (Kardelis, 2002):

$$n = \frac{1}{\Delta^2 + \frac{1}{N}} \quad (1)$$

Čia: $n-$ imties dydis (reikalingas apklausti mažų ir vidutinių įmonių vadovų skaičius)

$\Delta-$ leidžiamas paklaidos dydis (moksliniuose tyrimuose standartine paklaida laikoma 5 proc. , kuri gaunama su 0,95 tikimybe);

$N-$ tiriamos visumos dydis (mažų ir vidutinių įmonių skaičius).

Reikalingas apklausti klientų skaičius:

1/(0,05x0,05 + 1/6205)=384 (įmonių vadovai)

Kadangi tyrimą atliko vienas asmuo, apklausta 100 klientų iš Vilniaus mažų ir vidutinių įmonių pasirinktinai.

Anketos charakteristika: anketa buvo sudaryta iš dvidešimt klausimų. Buvo siekiama, kad klausimai būtų pakankamai tikslūs ir perteiktų reikiamą informaciją. Anketa pateikiama 1 priede.

Tyrimo proceso aprašymas: pagrindinis tyrimo instrumentas – anketos – platintas elektroniniu paštu 2015 m. spalio – lapkričio mėn. Organizuojant tyrimą laikytasi tyrimo etikos principų: savanoriškumo ir geranoriškumo, privatumo ir pagarbos, teisingumo, anonimiškumo (Tidikis, 2003). Dalyviams buvo suteikta galimybė atsisakyti dalyvauti tyrime, informacija apie tyrimo tikslą ir svarbą buvo pateikiama išsamiai ir tiksliai, bendraujama dalykiniu stiliumi. Savo ruožtu tyrimo duomenys buvo koduojami ir apsaugomi. Esant susidomėjimui ir poreikiui, tyrimo dalyviams pažadėta leisti susipažinti su tyrimo rezultatais ir išvadomis.

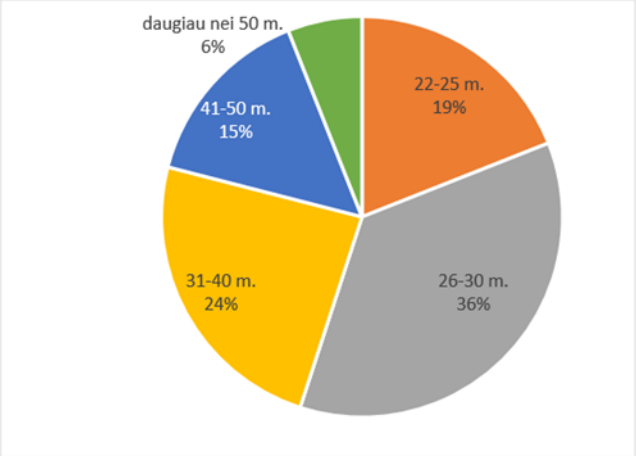
Gauti anketų atsakymai apdoroti laikantis klausimyne nustatytų kriterijų – kai kuriais atvejais atsakymai „reitinguojami“, kai kuriais atvejais pasirenkama procentinė išraiška. Suvestinės

lygmeniu pateikiamas kiekvieną klausimą apibendrinančių atsakymų teiginys, kurio pagrindu konstruojamos tyrimo išvados.

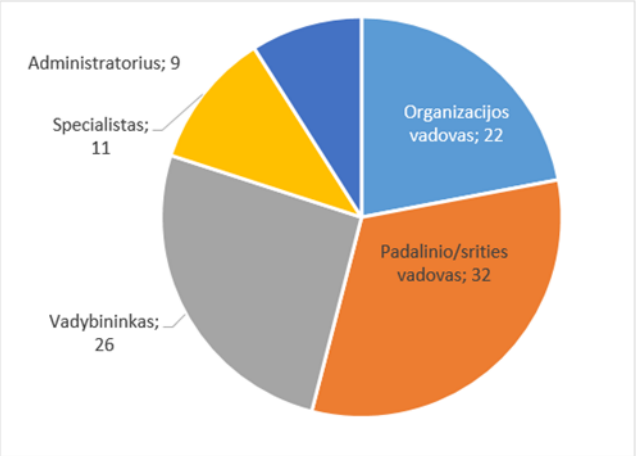
4.2. TYRIMO REZULTATAI

Tyrimas pradedamas nuo demografinės statistikos apžvalgos. Šie kriterijai temos atžvilgiu reikšmingi, nes padeda įvertinti tyrime analizuojamos atsakymų grupės atsakymų charakteristikas, identifikuoti dalyvių patirtį atsižvelgiant į jų amžių bei užimamas pareigas įmonėse.

13-14 pav. pateikiama šių dviejų charakteristikų vizualizacija. Kaip galima spręsti pagal 13 pav., tyrimo atsakymai ir išvados atspindi jaunų – vidutinio amžiaus atatsovų nuomonę (t.y. net 60 proc. dalyvių amžius yra 26-40 m.). Tokia charakteristika leidžia konstatuoti, jog tyrime bus apžvelgiama kvalifikuotų savo sroties žinovų nuomonė, kurie dirba su naujausiomis technologijomis, tačiau dalis jų gali paliūdyti apie inovacijų plėtrą ir tobulinimą. Vertinant tyrimo dalyvių pareigas, jog, kaip ir tikėtasi, daugiausiai pavyko gauti vadovaujančias pareigas užimančių darbuotojų atsakymus (54 proc. respondentų yra arba padalinio / srities vadovas, arba įmonės vadovas). Tai leidžia konstatuoti, jog respondentų nuomonė svari ir kompleksinė – neretai įmonių vadovai turi susidarę kompleksinę nuomonę kibernetinio saugumo klausimais,, o savo srities ekspertai (vidutinio lygmens vadovai) gali išreikšti nuomonę būtent kibernetinio saugumo pažeidimo atvejais, kai tuo tarpu kitų pareigų atstovai neretai rodo tik savo srities žinias ir kompetencijas.

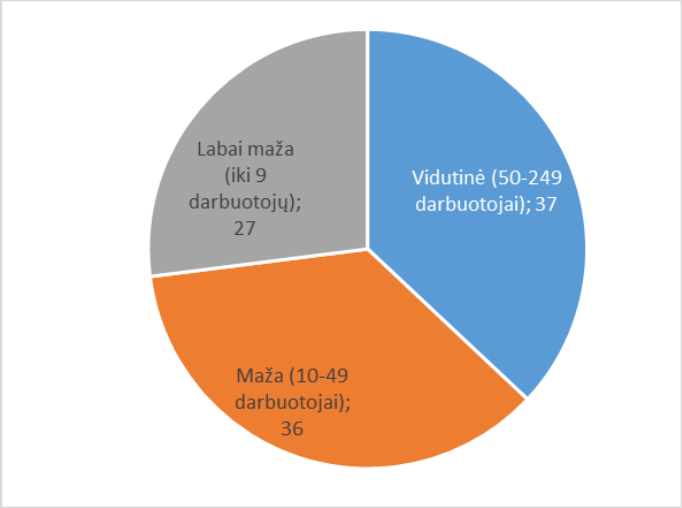


13 pav. Respondentų pasiskirstymas pagal amžių



14 pav. Respondentų pasiskirstymas pagal užimamapareigas

Pažymėtina, jog įmonės dydis kibernetinio saugumo atžvilgiu – taip pat vienas svarbiausių kriterijų – tikėtina, jog kuo didesnė įmonė, tuo didesnė svarba suteikiama kibernetiniam saugumui – kartu auga ir disponuojamos informacijos srautai, kas padidina kibernetinių atakų ar incidentų tikimybę. 15 pav. atsispindi tyrime dalyvavusių įmonių pasiskirstymas pagal dydį – pažymėtina, jog tyrimas iš esmės orientuotas į vidutines ir mažas įmones atsiribojant nuo didelių įmonių – pastarasis atvejis kiek apsunkina analizę dėl įmonių dydžio. Vis dėlto, klausimynas pateiktas neatsižvelgiant į įmonių dydį, tačiau, kaip matyti iš 15 pav., tyrime daugiausiai atspindima mažų ir vidutinių įmonių pozicija (73 įmonės iš 100 patenka į šią kategoriją).

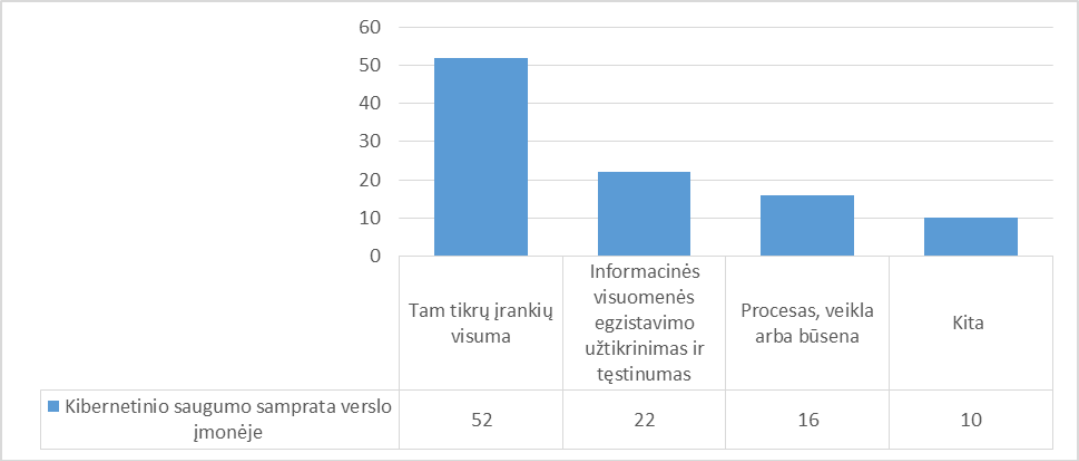


15 pav. Tyrime dalyvavusių įmonių dydis pagal darbuotojų skaičių

Mažų ir vidutinių įmonių nuomonės ir patirties nagrinėjimas pasižymi keletu privalumų – ekspertai konstatuoja, jog būtent mažos ir vidutinės įmonės yra *„pati mobiliausia, nuolat besikeičianti įmonių grupė – geba labai lanksčiai reaguoti į dažnai besikeičiančias paklausos sąlygas, technologinius reikalavimus ir diegti naujoves*“ (Misiūnas, 2008). Maža to, įmonėse, kuriose diegiamos inovacijos, fiksuojamas didesnis produktyvumas – sukuriami geresni produktai bei gamybos metodai. Tai išties lemia kibernetinio saugumo inovacijų panaudojimo būtinybę ir nuolatinius tobulinimo procesus. R..Garuckas ir G.Jatuliavičienė pažymi, jog *„pagrindinis mažų ir vidutinių įmonių privalumas prieš stambias įmones inovacijų diegimo procese yra tai, jog mažų ir vidutinių įmonių struktūra ir valdymo procesai nėra sudėtingi ir tai leidžia greitai ir lanksčiai keistis*“ (Garuckas, Jatuliavičienė, 2005).

Nustačius pagrindines tyrimo dalyvių charakteristikas, aktualias kibernetinio saugumo taikymui verslo procesuose, tyrimo metu buvo tikslinga išgryninti, kaip tyrimo dalyviai yra linkę interpretuoti kibernetinį saugumą jų įmonėse. Iki šiol mokslinėje literatūroje ir praktikoje

pakankamai sudėtingai nustatoma tikroji kibernetinio saugumo samprata, kuri dažnai painiojama su informacijos saugumu ar su elektroninės erdvės saugumu. Kaip galima spręsti pagal 17 pav. pateikiamą informaciją, dauguma tyrimo dalyvių (52 proc.) yra linkę kibernetinį saugumą suprasti kaip tam tikrų įrankių visumą, į kurią būtų įtraukiamos tiek politikos, saugumo užtikrinimo gairės, rizikos valdymo metodai, veiksmai, tiek mokymai, technologijos – šių įrankių pagalba būtų galima apsaugoti kibernetinę aplinką jos organizavimą ir vartojimo informaciją. Pažymėtina, jog tokios nuomonės iš esmės buvo visi vidutinių įmonių atstovai (87 proc. jų atsakymų), kiek kitaip kibernetinį saugumą vertina mažų ir labai mažų įmonių respondentai – dauguma jų (63 proc.) yra linkę manyti, jog kibernetinis saugumas turėtų būti siejamas su visuomenės informavimu iš esmės. Tokia pozicija liudija, jog šiuo atveju siekiama „nusiimti“ kibernetinio saugumo užtikrinimo naštą nuo įmonės pečių – t.y. tikimasi efektyvaus kibernetinio saugumo užtikrinimo mechanizmo nacionaliniu ir globaliu lygmeniu. Tokios nuostatos nėra kritikuotinos – vis dėlto, įmonių atstovai turėtų būti pasiruošę ginti individualius informacijos saugumo poreikius, rūpintis kibernetinio saugumo specifika savo įmonėje atsižvelgiant į tai, jog vykdomos veiklos ypatumus ir jos saugos reikalavimus geriausiai išmano šią veiklą įgyvendinantys atstovai.

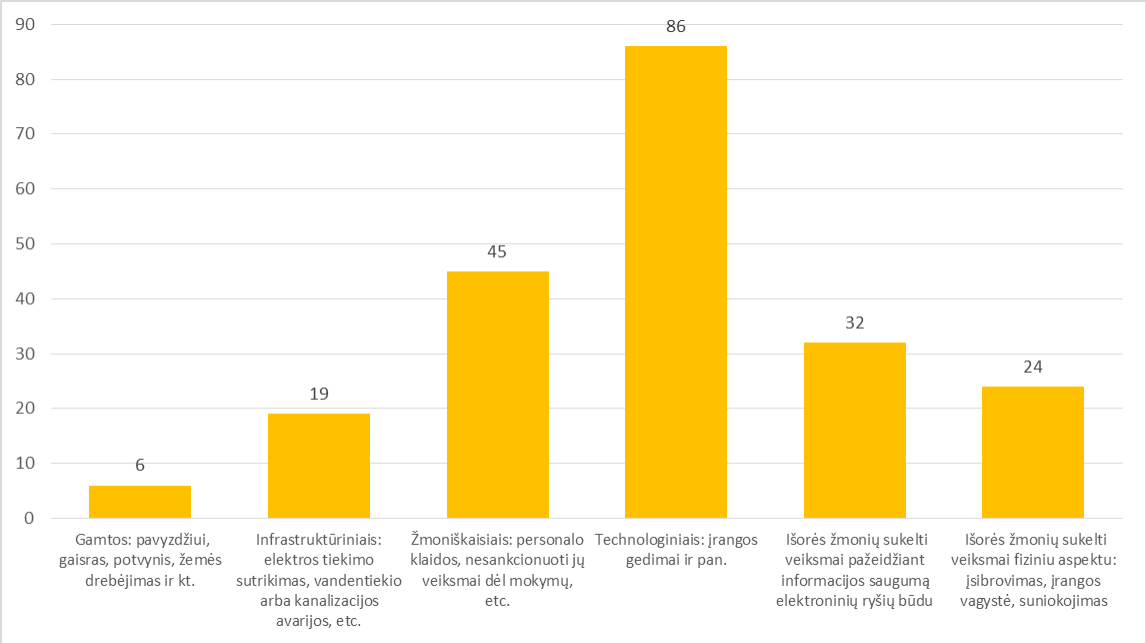


16 pav. Kibernetinio saugumo sąvokos išgryninimas – respondentų nuomonė

Kita vertus, tarp tyrimo dalyvių populiari ir priešinga nuostata – 16 proc. respondentų laikosi nuomonės, jog kibernetinis saugumas išties ribojamas keleto pagrindinių kriterijų ir turėtų būti suprantamas kaip „*procesas, veikla arba būsena pagal kurią informacijos ir ryšių sistemos yra saugomos nuo sugadinimo, neteisėto naudojimo ar modifikuotų pakeitimų*“. Pažymėtina, jog tai nėra pati teisingiausia kibernetinio saugumo supratimo forma – vis dėlto, konkretus apibrėžimas mažoms ir vidutinėms įmonėms padeda aiškiai taikyti kibernetinio saugumo priemones nepainiojant jų su nacionalinėmis reikmėmis. Minėti teiginiai vienokiu ar kitokiu požiūriu liudija tai, jog 90

proc. respondentų susiduria su kibernetiniu saugumu. Blogiausiai šiuo atveju vertintina tai, jog dešimtadalis apklaustųjų paminėjo, jog kibernetinis saugumas jų nuomone yra „Kita“, tačiau prašant apibrėžti šią sąvoką, jokių papildomų atsakymų nebuvo gauta – darytina išvada, jog apie kibernetinį saugumą šiuo atveju nėra nuomonės ar tiesiog neturima žinių.

Nustačius, jog 90 proc. įmonių tikrai suvokia kibernetinio saugumo svarbą įmonėje ir vienokiomis ar kitokiomis priemonėmis bando ją apibūdinti ir taikyti kasdienėje veikloje, tyrimo metu buvo siekiama nustatyti, su kokia kibernetinių incidentų patirtimi ir kiek dažnai susiduria respondentai. 17 pav. pateikiama respondentų nuomonės suvestinės vizualizacija šiuo klausimu.

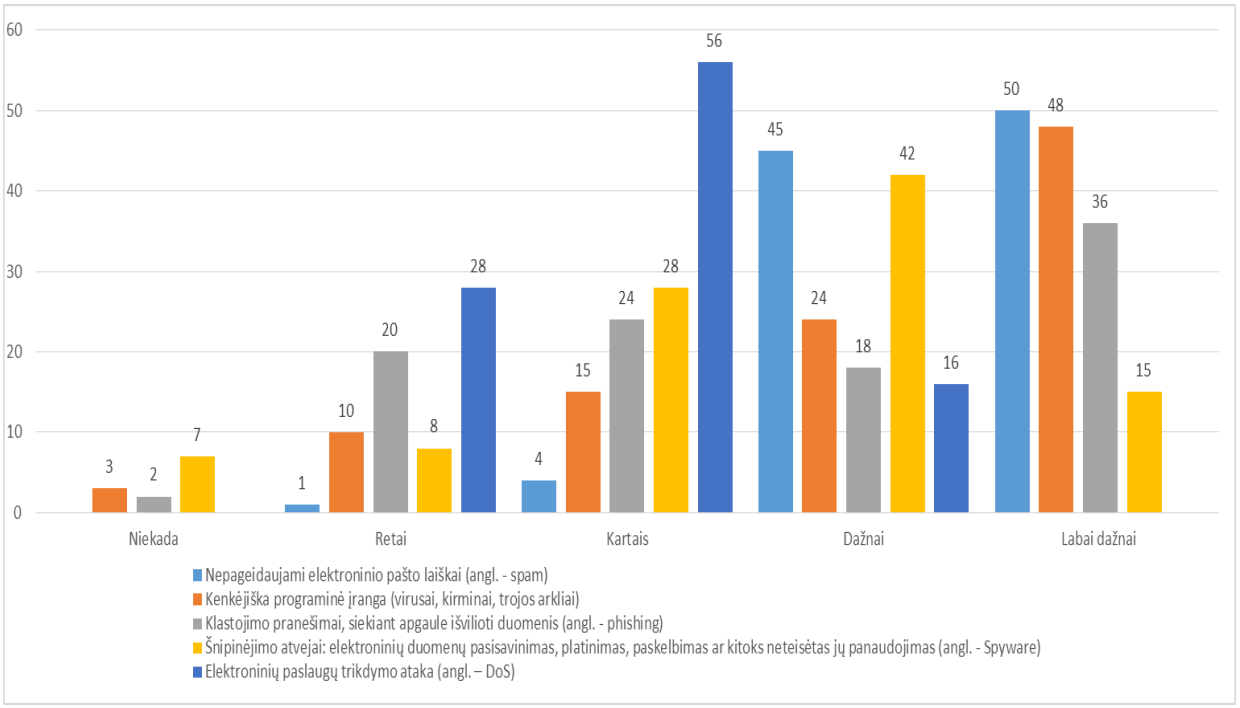


17 pav. Kibernetinių incidentų patirtis tyrime dalyvavusiose įmonėse

Paprašius apibūdinti dažniausias rizikas, su kuriomis susiduria įmonės siekdamos garantuoti kibernetinį saugumą, net 86 proc. respondentų nurodė, jog šiuo metu aktualiausi technologiniai įrangos gedimai. Tokios tendencijos aktualios ir gali būti lengvai išsprendžiamos skiriant papildomo dėmesio formuojant aktyvią apsaugos strategiją bei investuojant į turimas technologijas. Vis dėlto, itin svarbi antroji kibernetinio incidentų šaltinių grupė – net 45 proc. respondentų nurodė, jog incidentus dažniausiai nulemia įmonių darbuotojai, kuriems suteikiamos nepagrįstai didelės prieigos teisės arba nesuteikta prieiga, nevykdoma jų autentifikavimo ir prieigos kontrolė (skirtingas jų neigiamas poveikis ar neveikimo padariniai). Tokiu atveju itin svarbi tampa vidinių įgaliojimų suteikimo politika ir aiški kibernetinio saugumo strategija bei jos efektyvus įgyvendinimas įmonėje. Pasvertas įgaliojimų suteikimas bei darbuotojų teisių ir atsakomybių įteisinimas juridine prasme turėtų būti vieni svarbiausių veiksmų įgyvendinant kibernetinio saugumo užtikrinimo strategiją.

Kibernetinio saugumo užtikrinimas trečiųjų asmenų atžvilgiu – trečioji pagal svarbą kibernetinių incidentų priežastis (beveik ketvirtadalis, t.y. 24 proc., atsakymų). Paminėtina, jog šiuo atveju pasireiškia išoriniai įsilaužėliai į įmonių IT sistemas, turintys skirtingų tikslų (galimas ir skirtingas jų poveikis) ar tretieji asmenys, pagal sutartį vykdantys IT sistemų, įrangos priežiūrą, saugantys jiems perduotus duomenis duomenų saugyklose, centruose ir „debesyse“, užtikrinantys elektros tiekimą, nuomojantys patalpas, vykdantys IT įrangos remontą, apsaugos darbuotojai, teikiantys paslaugas (galimas skirtingas jų poveikis ar neveikimo padariniai). Techniniai trikdžiai, kurių pagrindinis sukėlėjas būna infrastruktūros gedimai ar gamtos išdaigos taip pat pasireiškia beveik ketvirtadalyje įmonių. Bendrai vertinant tyrimo dalyvių patirtį užtikrinant kibernetinį saugumą, konstatuotina, jog dauguma jų susiduria su „šiuolaikiškais“ incidentais, kurių šaltinis – žmogiškieji ištekliai, dirbantys įmonės viduje, ar tretieji asmenys, kurių paslaugomis naudojasi tyrimo dalyviai. Techniniai kliuviniai tyrimo dalyvių patiriami rečiau – tai greičiausiai lemia šiuo metu pakankamai išvystyta apsaugos priemonių visuma tiek nacionaliniu, tiek įmonių lygmeniu bei taikomos apsidraudimo priemonės.

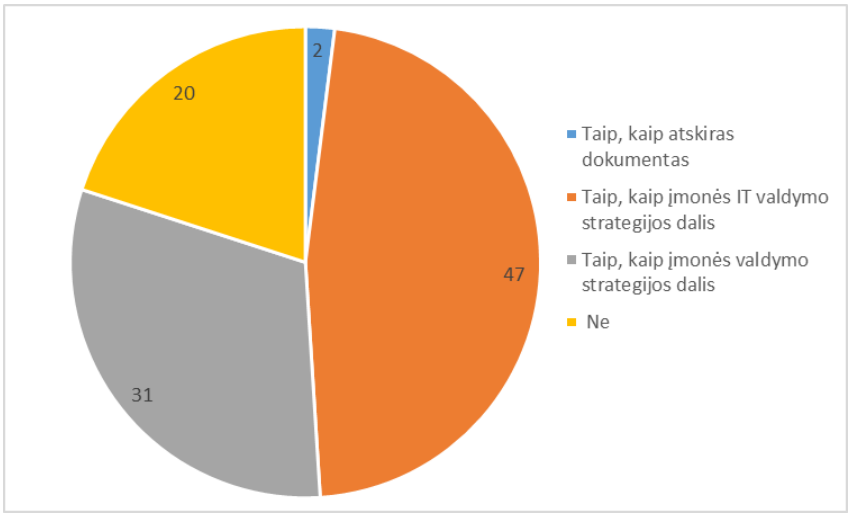
Identifikavus, jog pagrindiniai kibernetinio saugumo užtikrinimo trikdžiai fiksuojami technologinių bei žmogiškųjų išteklių lygmeniu, tyrimo dalyvių buvo prašoma konkretizuoti, su kokiais elektroninės informacijos saugumo incidentais teko susidurti pastaruoju metu. 18 pav. pateikiama tyrimo dalyvių atsakymų suvestinė šiuo klausimu.



18 pav. Elektroninės informacijos saugumo incidentai tyrime dalyvavusiose įmonėse

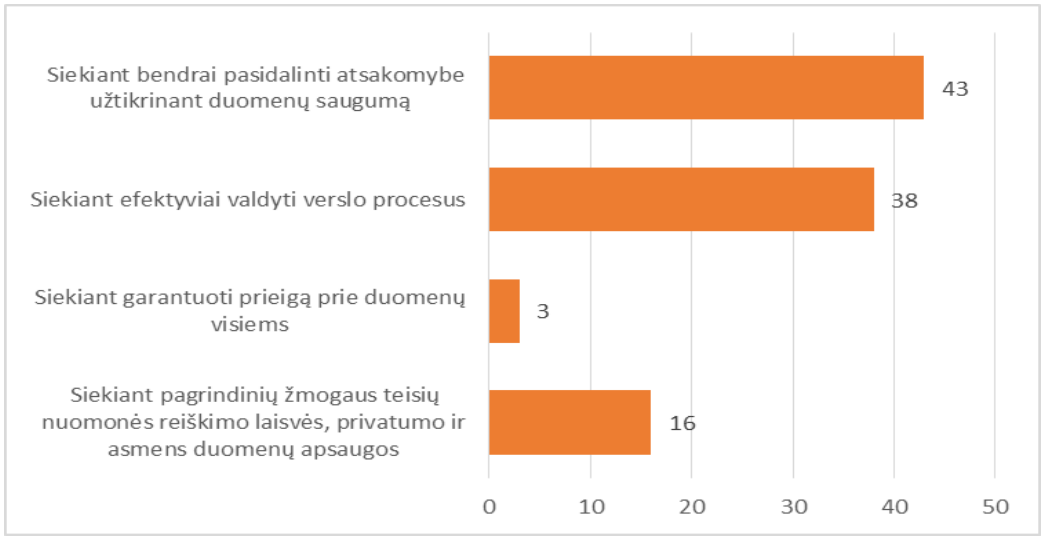
Pažymėtina, jog kiekvieno elektroninės informacijos saugumo incidento atžvilgiu respondentai turėjo ranguoti jo dažnį. Rangas „Labai dažnai“ buvo skirtas praktiškai visų elektroninės informacijos saugumo trikdžių atžvilgiu – vis dėlto, daugiausiai paminėti nepageidaujami elektroninio pašto laiškai (angl. *spam*) – su šiuo trikdžiu labai dažnai susiduria 50 proc. respondentų; saugotis nuo kenkėjiškų programų (virusų, kirminų, trojos arklių) labai dažnai tenka net 48 proc. dalyvių. Paminėtina, jog šie trikdžiai pasireiškia tiek fizinių, tiek juridinių asmenų veikloje. Kiek svarbiau kibernetinio saugumo atžvilgiu vertintina tai, jog labai dažnai mažos ir vidutinės įmonės susiduria su klastojimo pranešimais, siekiant apgaule išvilioti duomenis (angl. *phishing*) ar šnipinėjimo atvejais, kuomet pasisavinami elektroniniai duomenys, jie naudojami neteisėtai, platinami (15 proc. atsakymų).

Nustačius pagrindinius kibernetinį saugumą trikdančius veiksnius įmonėse bei įvertinus tyrimo dalyvių patirtį kovojant su šiais trikdžiais, tyrimo dalyvių teirautasi, ar jie atlieka šių trikdžių valdymą strateginiu lygmeniu, t.y. ar skiria pakankamai dėmesio – klausta, ar įmonėse yra suformuota kibernetinio saugumo užtikrinimo politika ir ją garantuojanti strategija. Visų pirma teirautasi, kiek stipriai yra įgyvendinamos kibernetinio saugumo užtikrinimo politikos priemonės, kiek tvirtai taikoma politika. Nustatyta, jog net 47 proc. visų įmonių kibernetiniam saugumui skiria dalį įmonės valdymo politikoje, 31 proc. numato šias priemones įmonės strateginiu lygmeniu, tačiau vos 2 proc. šiam saugumui yra paskyrę atskirą dokumentą, kai tuo tarpu net penktadalis jų kibernetinio saugumo nereglamentuoja strateginiu lygmeniu. Tokia situacija įvertinant tai, jog labai dažnai susiduriama su didesnio ar mažesnio kenksmingumo kibernetinio saugumo trikdžiais, vertinama itin nepalankiai – nors įmonės susiduria su trikdžių žala, tačiau iki šiol problemos nevertina strateginiu lygmeniu, nesiima strateginių problemų sprendimo būdų.



19 pav. Kibernetinio saugumo užtikrinimo politikos įgyvendinimo lygis tyrime dalyvavusiose įmonėse

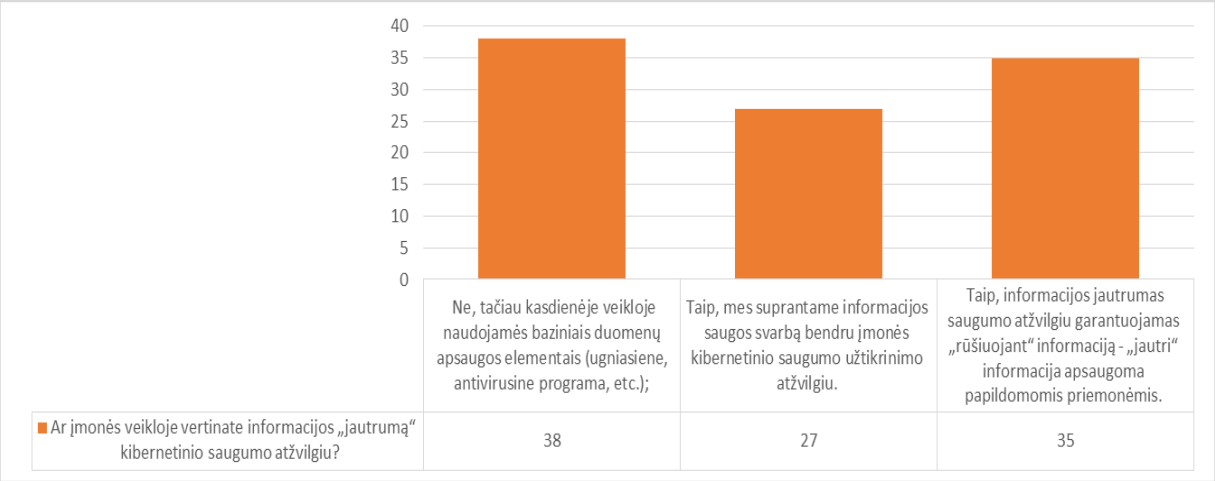
Vis dėlto, politikos priemonių netaikymas nesudaro pagrindo drąsiai konstatuoti, jog kibernetinio saugumo užtikrinimas nėra formuojamas strateginiu lygmeniu. Nors šiuo metu esanti situacija nepalanki, tačiau tyrimo dalyvių buvo klausiama, ką planuojama atlikti ateityje ir kokiu tikslu būtų formuojama įmonės strategija atsižvelgiant į kibernetinį saugumą. Pažymėtina, jog į šį klausimą atsakinėjo visi respondentai, t.y. net ir tie, kurie iki šiol nėra taikę jokių kibernetinio saugumo užtikrinimo politikos priemonių (minėti 20 proc.). Dauguma tyrimo dalyvių kibernetinio saugumo užtikrinimo strategiją formuotų siekiant bendrai pasidalinti atsakomybe užtikrinant duomenų saugumą (43 proc.), kiek mažiau įmonių būtų linkę strategiją įgyvendinti siedami su verslo procesais (38 proc.). Akcentuotina, jog minėti atsakymai iš esmės buvo pateikiami didesniųjų įmonių, kai tuo tarpu labai mažos įmonės linkusios strategijos išvis neformuoti ar pateikti bendras strategines nuostatas, kaip kad „strategija dėl duomenų prieigos garantijos visiems“ ar pagrindinių žmogaus teisių. Pastarieji atsakymai vertinami gana skeptiškai – nors strategija yra labiau koncepcinio pobūdžio planavimo priemonė, tačiau joje numatomi tikslai ir priemonės turi sietis su konkrečiomis įmonės veiklos priemonėmis, o neatspindėti humanistines idėjas. Atsižvelgiant į tai konstatuotina, jog beveik penktadalis (19 proc.) respondentų šiuo metu nėra pasiruošę suformuoti kibernetinio saugumo užtikrinimo strategijos, nesuvokia jos esmės ir nemato jos poreikio.



20 pav. Kibernetinio saugumo užtikrinimo strategijos pagrindinis tikslas - respondentų nuomonė

Nustačius santykinai prastą pasiruošimą formuoti kibernetinio saugumo užtikrinimo strategiją bei įgyvendinamas politikos priemones, tyrimo dalyvių teirautasi apie taktiniame bei operatyviniame lygmenyse taikomą įmonių informacijos „jautrumo“ vertinimą galimiems kibernetinio saugumo užtikrinimo trikdžiams. 21 pav. pateikiama informacija apie įmonių

supratimą, kiek stipriai jautri jų verslo procesuose naudojama informacija galimiems kibernetiniams incidentams.

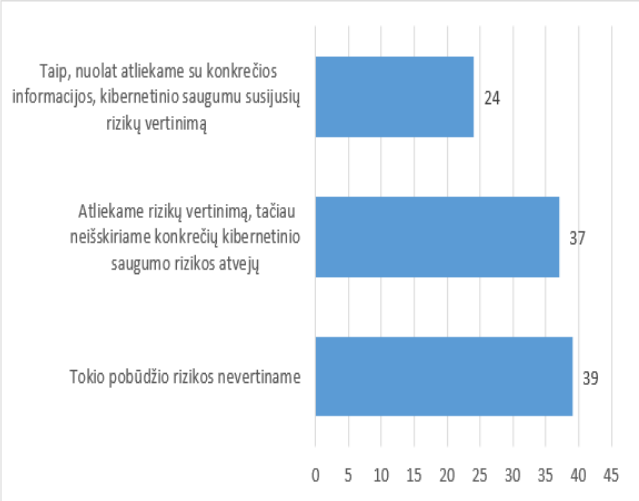


21 pav. Kibernetinio saugumo užtikrinimo priemonės – informacijos „jautrumo" nustatymas tyrime dalyvavusiose įmonėse

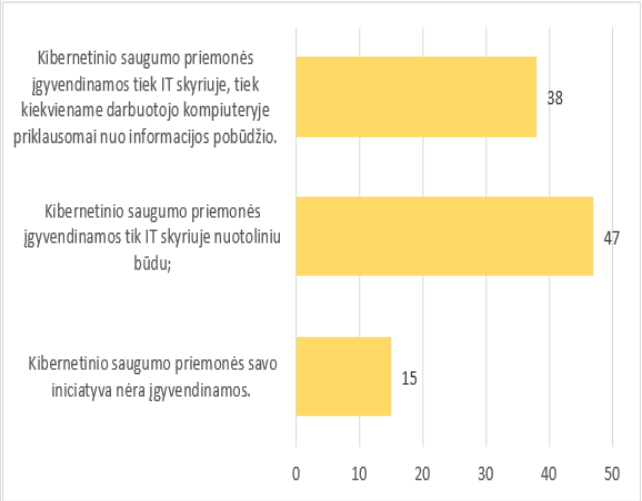
Pagal pateiktus duomenis galima spręsti, jog dauguma įmonių (38 proc.) informacijos saugumui nėra linkę kreipti papildomo dėmesio – nors kasdienėje veikloje taikomi baziniai duomenų apsaugos elementai (ugniasienė, antivirusinė programa, etc.), tačiau „jautrumas" papildomiems, agresyvesniems trikdžiams nėra testuojamas, juolab vertinamas ir lyginamas. Tuo tarpu kiek mažiau (35 proc.) respondentų laikosi priešingos pozicijos – informacija rūšiuojama pagal „jautrumą", taikomos papildomos priemonės. Palankiai vertinama tai, jog beveik trečdalis įmonių (dauguma jų – labai mažos ar mažos) tiesiogiai nurodo, jog supranta informacijos „jautrumo" svarbą kibernetinių atakų atžvilgiu (27 proc.). Bendrai vertinant įmonių veiksmus vertinant informacijos saugojimo svarbą, konstatuotina, jog dauguma įmonių (2/3) yra linkę diferencijuoti disponuojamą informaciją pagal jos svarbą ir saugumo būtinybę, tačiau kiek daugiau nei trečdalis taiko tik bazines saugumo priemones ir neskiria tam papildomo dėmesio.

Informacijos jautrumo nustatymas ir jos apsauga turi būti užtikrinama skirtingomis priemonėmis – tiek fizinėmis, tiek elektroninėmis. Informacijos panaudojimo bei sklaidos rizikos lygio nustatymas būtų vienas esminių žingsnių, lemsiančių sėkmingą kibernetinį saugumą užtikrinančios strategiją. Atsižvelgiant į tai, tyrimo dalyvių buvo klausiama, ar atliekamas su kibernetiniu saugumu susijusių rizikų vertinimas – bendrai vertinant, net 61 proc. įmonių yra linkę į tai atsižvelgti, tačiau net 39 proc. iki šiol tokios rizikos nevertina. Tokie rezultatai gana prieštaringai

apibūdina ankstesnius įmonių atsakymus – nors dauguma paminėjo, jog taiko ir formuoja strateginius sprendimus kibernetiniam saugumui užtikrinti, tačiau kiek mažiau nei pusė net neįvertina kylančių rizikų. Konstatuotina, jog nepaisant minėtų pasisakymų, abejotina, ar galimai formuojama kibernetinį saugumą užtikrinanti strategija būtų net neįvertina kylančių rizikų. Konstatuotina, jog nepaisant minėtų pasisakymų, abejotina, ar galimai formuojama kibernetinį saugumą užtikrinanti strategija būtų sėkminga – ji juk nėra grindžiama šiuo metu esančios situacijos analize, todėl gali būti sunkiai pritaikoma įmonių reikmės ir procesams.

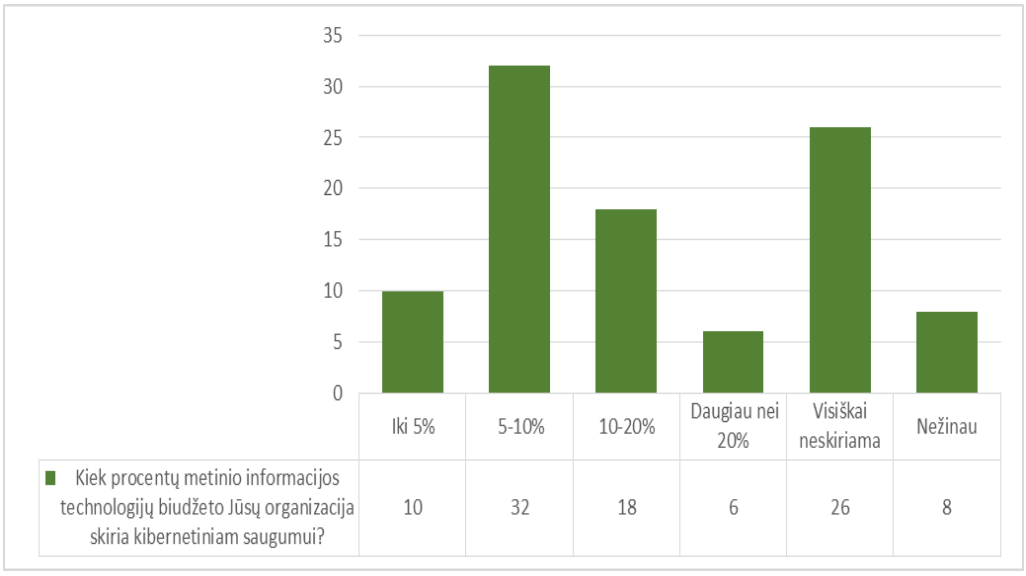


22 pav. Kibernetinio saugumo užtikrinimo priemonės – rizikos lygių vertinimas tyrime dalyvavusiose įmonėse



23 pav. Kibernetinio saugumo priemonių lygio nustatymas tyrime dalyvavusiose įmonėse

Panaši išvada darytina vertinant ir kibernetinio saugumo užtikrinimo priemones bei jų valdymą – nors net 38 proc. įmonių nurodo, jog kibernetinio saugumo priemonės įgyvendinamos tiek IT skyriuje, tiek kiekviename darbuotojo kompiuteryje priklausomai nuo informacijos pobūdžio, tačiau šių veiksmų efektyvumas abejotinas. Neįvertinus informacijos jautrumo ar kylančių rizikų bei taikant unifikuotas apsaugos priemones, jų tinkamumas ir efektyvumas gali labai sumenkti. Bendrą situaciją prastina dar tai, jog 47 proc. įmonių tokias apsaugos priemones taiko tik IT skyriuje, tai atliekama nuotoliniu būdu ar išvis kibernetinio saugumo priemonių valdymas nėra įgyvendinamas (62 proc. įmonių). Akivaizdu, jog detaliau vertinant taikomas priemones, įmonių kibernetinio saugumo situacija gerokai skiriasi nuo anksčiau deklaruotų nuostatų – realybėje situacija žymiai prastesnė nei deklaruojami ketinimai formuoti strateginius sprendimus ar politines priemones.

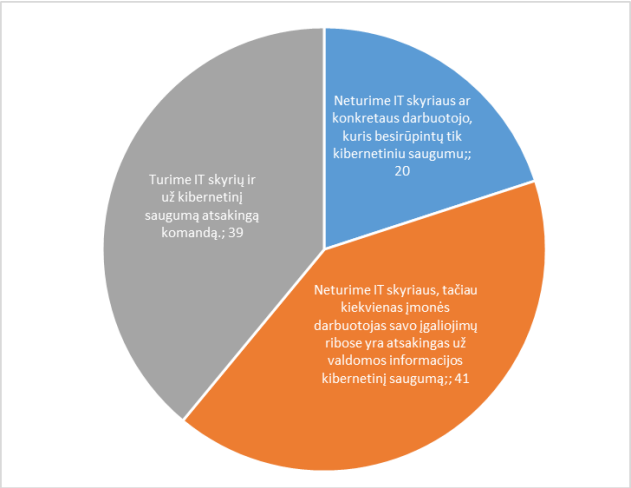


24 pav. Kibernetinio saugumo užtikrinimui skiriamų lėšų dydis tyrime dalyvavusių įmonių biudžetuose

Apie situacijos sudėtingumą byloja ir kibernetiniam saugumui skiriamų lėšų dydis palyginus su įmonių biudžetais – daugumoje įmonių (32 proc.) daugiausiai skiriama iki 10 proc. įmonė s biudžeto šių priemonių įgyvendinimui. Blogiausiai vertintina tai, jog net 26 proc. įmonių išvis nėra linkę skirti lėšų kibernetinio saugumo užtikrinimo priemonėms. Akcentuotina, jog saugumo užtikrinimo priemonių finansavimas ir įmonių dydis susiję tik iš dalies – nors dauguma (46 proc. vidutinių įmonių) yra linkę skirti papildomą finansavimą saugumo užtikrinimui, tačiau šiuo atveju ne ką tenusileidžia ir mažos bei itin mažos įmonės (53 proc.). Tokia situacija gali būti paaiškinama teiginiu, jog įmonės ar disponuojamų lėšų dydis neįtakoja kibernetinio saugumo užtikrinimo

politikos ir prioritetų – sprendimai formuojami atsižvelgiant į vadovybės patirtį nei nuostatas, konservatyvumą, o ne į vien tik verslo dydį.

Siekiant nustatyti, kaip įmonės yra pasiruošę susidoroti su galimomis kibernetinio saugumo atakomis, respondentų buvo klausiama, kiek stipriai išvystyta už saugumą atsakingų IT specialistų funkcija įmonėje (25 pav.).

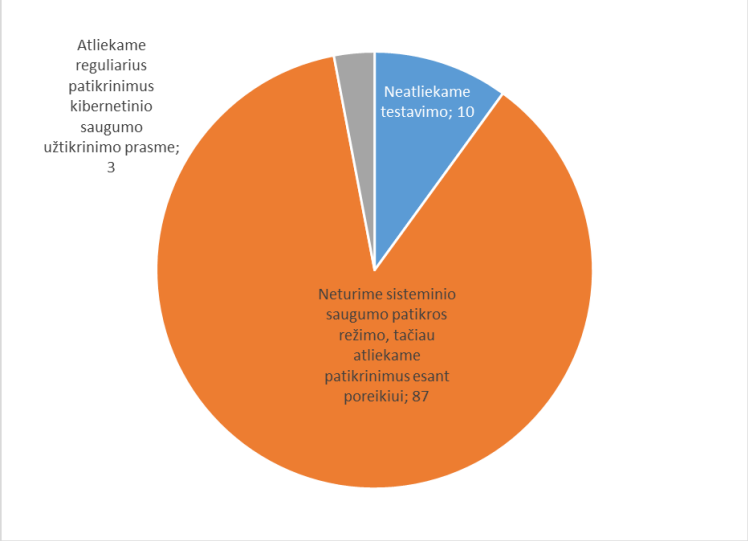


25 pav. Už kibernetinį saugumą atsakingų asmenų funkcijos įmonėse

Nustatyta, jog dauguma vidutinių bei dalis mažų įmonių (bendrai 39 proc. įmonių) turi IT skyrių ar už kibernetinį saugumą atsakingą komandą – tokia situacija leidžia konstatuoti, jog įmonės, strateginiu lygmeniu neinvestuodamos į kibernetinio saugumo priemones, suformuodamos ir išlaikydamos tokius padalinius tikisi, jog tik šios pareigybės ar padaliniai kompleksiškai užkirs sąlygas kibernetinėms atakoms. Tai gana ribotas požiūris – konkrečios pareigybės neformuoja įmonės politikos, todėl jų įgaliojimai riboti, nerodoma iniciatyva, o esanti situacija vertinama gera tokia, kokia yra, t.y. neįžvelgiami ateities pavojai ir grėsmės. Minėtus teiginius patvirtina ir tai, jog 41 proc. įmonių laikosi nuomonės, jog kiekvienas įmonės darbuotojas savo įgaliojimų ribose yra atsakingas už valdomos informacijos kibernetinį saugumą – pernelyg didelis pasitikėjimas įmonės darbuotojais nefiksuojant jų konkrečių atsakomybių dėl turimos konfidencialios informacijos ilgainiui gali padaryti finansinės ir komercinės žalos. Bendrai vertinant, konstatuotina, jog įmonės iki šiol deramai nevaldo ir neišnaudoja IT skyriaus darbuotojų potencialo ar galimybių – vienu atveju visa atsakomybė „numetama“ konkrečiam darbuotojui nepriimant strateginių sprendimų, neskiriant tinkamo finansavimo, kitu atveju suteikiami pernelyg dideli įgaliojimai, nesisaugojama ir neapibrėžiamos dėk darbuotojų elgesio kylančios rizikos.

Siekiant pagrįsti ar paneigti minėtus teiginius, respondentų buvo klausiama apie praktikoje taikomas kibernetinio saugumo priemones ir veiksmus (26 pav.) – tikėtina, jog jas iš esmės atlieka

jau aptartos IT specialisto pareigybės ar skyrius. Konstatuotina, jog periodiniai kibernetinio saugumo patikrinimai įmonėse nėra atliekami – nes „nėra sukurta sisteminio saugumo patikros režimo“, nors tvirtinama, jog esant poreikiui patikrinimai yra atliekami (87 proc.). Vis dėlto, konkretūs poreikiai ir situacijos nebuvo paminėti. Tuo tarpu 10 proc. atsakiusiųjų nurodė, jog tokie patikrinimai įmonėje nebuvo išvis atliekami iki šiol. Tik 3 proc. tyrimo dalyvių (visi jų – vidutinės įmonės) nurodė, jog periodiniai kibernetinio saugumo užtikrinimo priemonių patikrinimai atliekami.



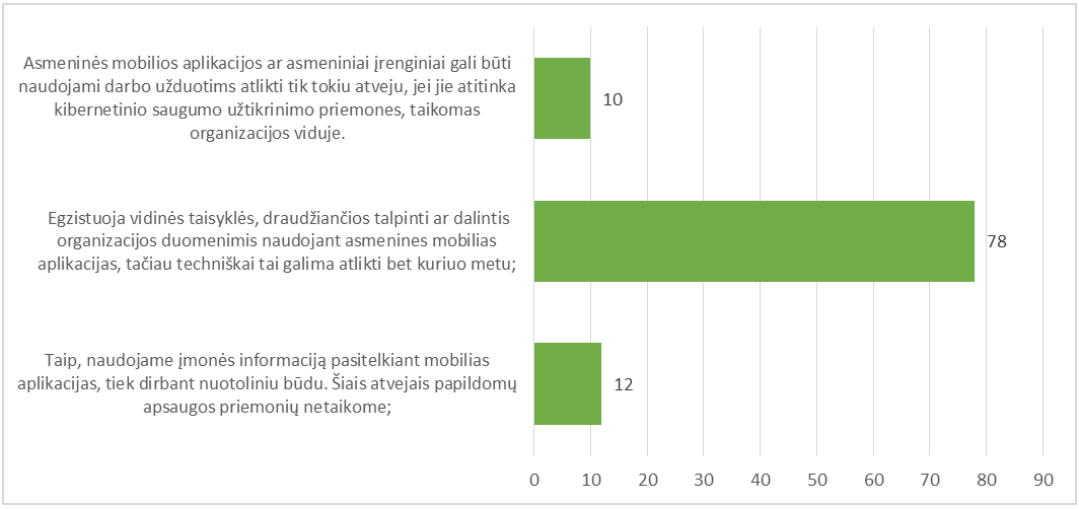
26 pav. Periodinio turimų technologijų ir įrengimų patikrinimo kibernetinio saugumo atžvilgiu dažnis tyrime dalyvavusiose įmonėse

Atsižvelgiant į patikrinimo atvejų situaciją, natūralu, jog saugumo incidentų registravimo procesai įmonėse vyksta taip pat nenuosekliai – net 63 proc. respondentų apie tokius registrus nežinojo, net ketvirtadalis patvirtino, jog tokių registrų įmonėje neturi. 12 įmonių nurodė, jog tokius registrus pildo įvykus kibernetinio saugumo trikdžiams. Tokius registrus pildo tik vidutinės įmonės.

Įvertinus santykinai prastą kibernetinio saugumo taikymo ir suvokimo lygį Lietuvos vidutinėse ir mažose įmonėse, darytina išvada, jog bene geriausia išeitis – nuolatinis įmonių vadovų ir darbuotojų informacinio išprusimo lygio didinimas. Pažymėtina, jog šios srities žinias turėtų kaupti ne tik IT specialistai, tačiau bendrą suvokimą turėtų turėti kiekvienas įmonės darbuotojas, juolab įmonės vadovas. Tokios priemonės padėtų ne tik efektyvinti saugumo užtikrinimą, kartu sudarytų sąlygas formuoti efektyvesnę į kibernetinio saugumo užtikrinimą orientuotą strategiją. Įvertinus minėtus aspektus, tyrimo dalyvių buvo klausiama, kaip intensyviai ir ar išvis yra organizuojami į kibernetinį saugumą orientuoti mokymai siekiant vis labiau įtraukti darbuotojus į kibernetinio saugumo užtikrinimo procesus. Nepaisant kitais atvejais nustatytos nepalankaus

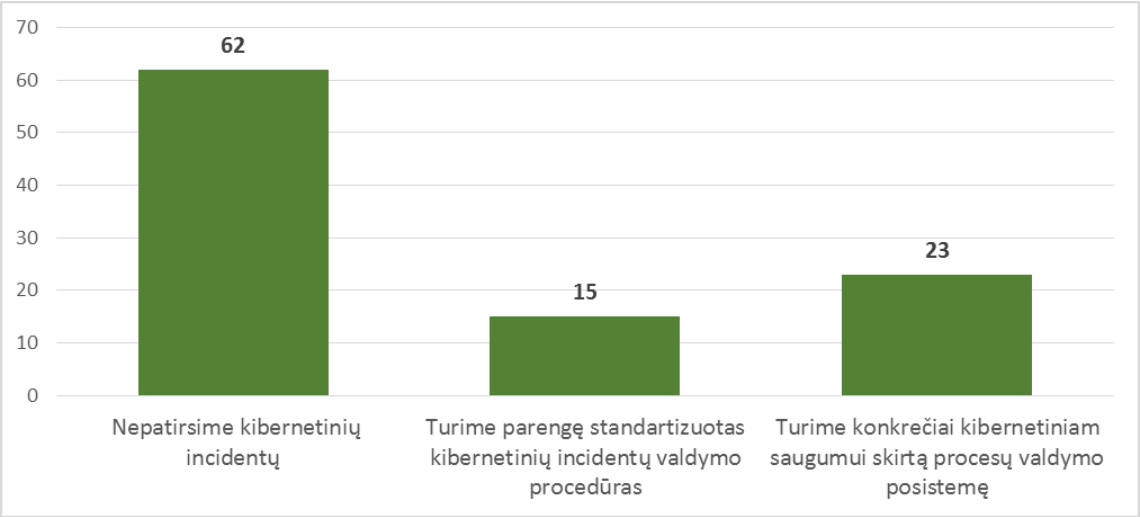
įmonių situacijos vertinimo, net 55 proc. respondentų nurodė, jog šios srities mokymai atliekami ir organizuojami, o juose dalyvauja didžioji dalis įmonių darbuotojų.

Siekiant kompleksiškai įvertinti tyrime dalyvavusių įmonių realius pajėgumus atlaikyti kibernetines atakas bei galimą kibernetinio saugumo užtikrinimo lygį, tyrimo pabaigoje įvertinamas įmonių veiklos rizikingumas atsižvelgiant į leidimą naudoti mobiliąsias aplikacijas kasdienėje veikloje. Natūralu, jog kuo daugiau ir platesniame tinkle naudojamasi įmonės duomenimis, tuo sunkiau užtikrinti saugumo priemones bei atlaikyti galimas atakas. 27 pav. pateikiama informacija leidžia daryti išvadą, jog mobiliosios aplikacijos išties paplitusios vidutinių ir mažų įmonių darbuotojų tarpe – net 78 proc. respondentų nurodė, jog nors egzistuoja vidinės taisyklės, draudžiančios talpinti ar dalintis organizacijos duomenimis naudojant asmenines mobilias aplikacijas, tačiau techniškai tai galima atlikti bet kuriuo metu. Maža to, 12 proc. atsakiusiųjų nurodė, jog nors naudoja įmonės informaciją pasitelkiant mobilias aplikacijas dirbant nuotoliniu būdu, tačiau papildomų apsaugos priemonių netaiko.



27 pav. Tyrime dalyvavusių įmonių patirtis darbuotojams leidžiant naudoti mobiliąsias aplikacijas tiesioginėms darbo užduotims atlikti

Minėti teiginiai patvirtina teiginį, jog įmonės oficialiai deklaruoja kibernetinio saugumo užtikrinimo priemonių taikymą ir jų veiksmingumą, tačiau realybėje tam neretai pritrūksta lėšų, neįvertinamos galimos rizikos, ne iki galo suprantama kibernetinio saugumo svarba įmonių veiklai. 28 pav. pateikiama tyrimo dalyvių nuomonės apie įmonių „atsparumą“ kibernetinėms atakoms vizualizacija.



28 pav. Tyrime dalyvavusių įmonių pasirengimo atlaikyti kibernetinį incidentą lygis (įmonių atstovų nuomonė)

Įmonių kibernetinio saugumo „stiprumo“ lygis išties vertinamas pakankamai prastai – net 62 proc. įmonių yra įsitikinę, jog su turimomis kibernetinio saugumo užtikrinimo priemonėmis jie nesusidurs su kibernetiniais incidentais. Tuo tarpu likę 38 proc. nurodo, jog turi parengę standartizuotas kibernetinių incidentų valdymo procedūras ar posistemę, tačiau praktikoje jų nelabai linkę taikyti.

Bendrai vertinant kibernetinio saugumo užtikrinimo galimybes Lietuvos įmonėse, konstatuotina, jog kibernetinio saugumo sąvoka įmonėse vis dar pakankamai retai naudojama sąvoka – nors dauguma respondentų šiuos procesus suvokia kaip tam tikrų įrankių visumą, į kurią būtų įtraukiamos tiek politikos, saugumo užtikrinimo gairės, rizikos valdymo metodai, veiksmai, tiek mokymai, technologijos. Vis dėlto, mažosios įmonės kibernetinį saugumą sieja su nacionaliniu mastu įgyvendinama politika, perkeliant saugumo užtikrinimo atsakomybę valstybei. Neigiamai vertinama tai, jog net penktadalis įmonių net nežino, kaip veikia kibernetinis saugumas ir kam tai reikalinga. Praktika liudija, jog kibernetinio saugumo poreikis išties egzistuoja – šiuo metu įmonėms aktualiausi technologiniai įrangos gedimai nei incidentai, kuriuos įtakoja įmonių darbuotojai, kuriems suteikiamos nepagrįstai didelės prieigos teisės arba nesuteikta prieiga, nevykdoma jų autentifikavimo ir prieigos kontrolė. Kibernetinį saugumą įtakojantys trikdžiai apima nepageidaujamus elektroninio pašto laiškus, kenkėjiškas programas, klastojimo pranešimus, siekiant apgaule išvilioti duomenis ar šnipinėjimo atvejais. Kibernetinio saugumo užtikrinimo poreikis akivaizdus, tačiau jo valdymas dar nėra pakankamai plėtojamas Lietuvos įmonėse - nors beveik pusė įmonių kibernetiniam saugumui skiria dalį įmonės valdymo politikoje, 31 proc. numato šias priemones įmonės strateginiu lygmeniu, tačiau vos 2 proc. šiam saugumui yra paskyrę atskirą

dokumentą, kai tuo tarpu net penktadalis jų kibernetinio saugumo nereglamentuoja strateginiu lygmeniu. Akivaizdu, jog nors įmonės susiduria su trikdžių žala, tačiau iki šiol problemos nevertina strateginiu lygmeniu, nesiima strateginių problemų sprendimo būdų. Kibernetinio saugumo užtikrinimo galimybių atžvilgiu palankiai vertinama tai, jog dauguma įmonių strategiją formuotų siekiant bendrai pasidalinti atsakomybe užtikrinant duomenų saugumą, kiek mažiau įmonių būtų linkę strategiją įgyvendinti siedami su verslo procesais (38 proc.). Mažos įmonės linkusios strategijos išvis neformuoti ar pateikti bendras strategines nuostatas – nors pažymėtina, jog nors strategija yra labiau koncepcinio pobūdžio planavimo priemonė, tačiau joje numatomi tikslai ir priemonės turi sietis su konkrečiomis įmonės veiklos priemonėmis, o neatspindėti humanistines idėjas. Konstatuotina, jog beveik penktadalis respondentų šiuo metu nėra pasiruošę suformuoti kibernetinio saugumo užtikrinimo strategijos, nesuvokia jos esmės ir nemato jos poreikio. Galimybes taikyti kibernetinio saugumo priemones apsunkina tai, jog dauguma įmonių informacijos saugumui nėra linkę kreipti papildomo dėmesio – nors kasdienėje veikloje taikomi baziniai duomenų apsaugos elementai (ugniasienė, antivirusinė programa, etc.), tačiau „jautrumas“ papildomiems, agresyvesniems trikdžiams nėra testuojamas, juolab vertinamas ir lyginamas, nevertinamas informacijos rizikingumas kibernetinio saugumo trikdžių atžvilgiu. Abejotina, ar galimai formuojama kibernetinį saugumą užtikrinanti strategija būtų sėkminga – ji juk nėra grindžiama šiuo metu esančios situacijos analize, todėl gali būti sunkiai pritaikoma įmonių reikmės ir procesams. Neįvertinus informacijos jautrumo ar kylančių rizikų bei taikant unifikuotas apsaugos priemones, jų tinkamumas ir efektyvumas gali labai sumenkti. Darytina išvada, jog įmonės ar disponuojamų lėšų dydis neįtakoja kibernetinio saugumo užtikrinimo politikos ir prioritetų – sprendimai formuojami atsižvelgiant į vadovybės patirtį nei nuostatas, konservatyvumą, o ne į vien tik verslo dydį. Įmonės iki šiol deramai nevaldo ir neišnaudoja IT skyriaus darbuotojų potencialo ar galimybių – vienu atveju visa atsakomybė „numetama“ konkrečiam darbuotojui nepriimant strateginių sprendimų, neskiriant tinkamo finansavimo, kitu atveju suteikiami pernelyg dideli įgaliojimai, nesisaugojama ir neapibrėžiamos dėk darbuotojų elgesio kylančios rizikos. Saugumo incidentų registravimo procesai įmonėse vyksta taip pat nenuosekliai. Darytina išvada, jog nors Lietuvos įmonės oficialiai deklaruoja kibernetinio saugumo užtikrinimo priemonių taikymą ir jų veiksmingumą, tačiau realybėje tam neretai pritrūksta lėšų, neįvertinamos galimos rizikos, ne iki galo suprantama kibernetinio saugumo svarba įmonių veiklai. Bendrai vertinant įmonių kibernetinio saugumo užtikrinimo galimybes, darytina išvada, jog situacija santykinai prasta – daugiau nei pusė įmonių tiki, jog praktikoje nesusidurs su kibernetiniais incidentais.

IŠVADOS

Bendrai vertinant tyrimo rezultatus, galima konstatuoti, jog kibernetinis saugumas užtikrina teigiamą ir sklandžią verslo procesų veiklą. Tokiu būdu patvirtinama darbe keliama hipotezė – netiesiogiai galima daryti išvadą, jog kuo didesnė įmonė, tuo labiau rūpinamasi kibernetiniu saugumu. Tokią situaciją lemia ne tiek įmonės dydis, kiek verslo procesų kompleksiškumas didesnėse įmonėse – suvokiama, jog verslo procesams sudėtingėjant, būtina labiau investuoti į kibernetinio saugumo priemones strateginiu įmonės lygmeniu.

1. Darytina išvada jog kibernetinis saugumas privalo garantuoti asmenims saugų interneto naudojimą. Kibernetinis saugumas – tam tikrų įrankių visuma, apimanti politikos, saugumo užtikrinimo gaires, rizikos valdymo metodus, veiksmus, mokymus, technologijas, kurios gali būti naudojamos siekiant apsaugoti kibernetinę aplinką jos organizavimą ir vartojimo informaciją. Praktika liudija jok kibernetinis saugumas dažnai painiojamas su informacijos užtikrinimo ir informacijos saugumo sąvokomis.
2. Praktikoje kibernetinio saugumo užtikrinimas susiduria su keletu pagrindinių trikdžių: kibernetinio saugumo principų nesilaikymas sudaro sąlygas neteisingai interpretuoti kibernetinio saugumo priemonių taikymo esmę, jų tinkamumą, o nelegalus informacijos naudojimas, klastojimas, viešinimas ar iškraipymas sukelia akivaizdžius moralinius ir materialinius nuostolius visiems dalyviams, kurie naudojasi kompiuterizuotais informacijos sąveikos procesais bei lemia informacijos pažeidžiamumą (Lietuvoje iki šiol dažniausiai sutinkamas 0 ir 1 informacijos apsaugos brandos lygiai). Akivaizdu, jog kibernetinis saugumas tobulėjant duomenų perdavimo metodams privalo nuolat būti peržiūrimas, atnaujinamos diegimo priemonės – tai atliekama ne visose įmonėse vienodai, o kai kuriose jų – išvis neatliekama.
3. Apžvelgus pagrindines verslo procesų sampratas, darytina išvada, jog mokslinėje literatūroje autoriai pateikia gana plačius verslo procesų apibrėžimus ir sampratas. Pagrindinė to priežastis yra tai, jog procesų vadybos teorija laikoma nevisiškai susiformavusiu mokslu iki galo. Akcentuojama, jog įmonė, kuri analizuoja, detalizuoja, gerina ir analizuoja įmonės verslo procesus tampa labiau konkurencinga ir turi daugiau galimybių prisitaikyti prie konkurencingos rinkos, nes tokiu būdu atrandamos silpnosios vietos proceso gamyboje. Įvertinus verslo procesų asociacijas su kibernetiniu saugumu, darytina išvada, jog iki šiol mokslinėje literatūroje verslo procesų valdymas, kaip ir verslo procesai suvokiami gana skirtingai. Dažniausiai verslo procesų valdymas susideda iš procesų žingsnių planavimo, valdymo ir kontrolės, o verslo procesų valdymo tyrimų objektas apima pagrindinius ir pagalbinius procesus.

4. Kaip labiausiai verslo procesus įtakojantys kibernetinio saugumo kriterijai ir aspektai išskiriami du veiksnių lygiai. Makrolygmeniu kibernetinio saugumo užtikrinimą verslo procesuose lemia valstybės dalyvavimo intensyvumas formuojant kibernetinio saugumo politiką, ES priimtos direktyvos ir reglamentai (didėjantis bendradarbiavimas tarp viešojo ir privataus sektorių paslaugų sektoriuje, augantis civilinės ir karinės sričių persidengimas bei politiniaius valstybės interesai bei padėtis tarptautiniu mastu). Mikrolygmeniu kibernetinis saugumas užtikrinamas didinant darbuotojų informatyvumą bei rengiant mokymus įvertinant tai, jog darbuotojų informavimo stoka gali susilpninti net ir stipriausias saugumo priemones. Maža to, nesant tinkamo biudžeto, organizacija negali būti aprūpinama pakankamais ištekliais, kurie užtikrintų informacijos saugumą. Informacijos saugumo politikos priėmimas įmonėje yra pradinė priemonė, kurios pagalba siekiama sumažinti informacijos saugumo grėsmes iki minimumo.

5. Kibernetinio saugumo valdymo nuoseklumo nustatymui verslo procesuose būtina išgryninti kibernetinio saugumo valdymo modelį konkrečioje įmonėje. Toks modelis grindžiamas keletu esminių nuolat atliekamų tarpusavyje sąveikaujančių veiklų. Verslo vienijimo veikla apima strateginių įmonės tikslų įgyevndinimą įtraukiant visus darbuotojus. Su kibernetiniu saugumu susijusios rizikos turi būti išskiriamos kaip prioritetinės rizikos vertinime. Šiuo atveju būtinas suvokimas, jog siekiant tinkamo kibernetinio saugumo užtikrinimo įgyvendinimo, IT skyriaus vadovas privalo pasižymėti aukštomis kompetencijomis, orientacija bei aukštais įgaliojimais. Kasdienė stebėsena ir integruotas mišrių duomenų debesijų monitoringas privalo vykti lygiagrečiai anksčiau paminėtiems procesams. Visi išvardinti procesai garantuoja sėkmingą kibernetinio saugumo užtikrinimą įmonės verslo procesuose.

6. Atlikus kokybinį kibernetinio saugumo užtikrinimo galimybių tyrimą, darytina išvada, jog kibernetinio saugumo sąvoka įmonėse vis dar pakankamai retai naudojama – nors dauguma respondentų šiuos procesus suvokia kaip tam tikrų įrankių visumą, į kurią būtų įtraukiamos tiek politikos, saugumo užtikrinimo gairės, rizikos valdymo metodai, veiksmai, tiek mokymai, technologijos, mažosios įmonės kibernetinį saugumą sieja su nacionaliniu mastu įgyvendinama politika, perkeliant saugumo užtikrinimo atsakomybę valstybei. Net penktadalis įmonių net nežino, kaip veikia kibernetinis saugumas ir kam tai reikalinga. Kibernetinio saugumo užtikrinimo poreikis akivaizdus, tačiau jo valdymas dar nėra pakankamai plėtojamas Lietuvos įmonėse. Nors įmonės susiduria su trikdžių žala, iki šiol problemos nevertinamos strateginiu lygmeniu, nesiimama strateginių problemų sprendimo būdų.

7. Kokybinio tyrimo rezultatai leidžia konstatuoti, jog kibernetinio saugumo užtikrinimo galimybės apimtų tinkamų strateginių sprendimų priėmimą - dauguma įmonių strategiją formuotų siekiant bendrai pasidalinti atsakomybe užtikrinant duomenų saugumą, kiek mažiau įmonių būtų

linkę strategiją įgyvendinti siedami su verslo procesais. Nepalankiai vertinama tai, jog dalis įmonių linkę strategijos išvis neformuoti, nesuvokiama jos esmė ir poreikis. Tinkamas informacijos „jautrumo“ diferenciavimas – dar viena kibernetinio saugumo užtikrinimo galimybių. Jautrumas agresyvesniems trikdžiams iki šiol įmonėse nėra testuojamas, vertinamas ir lyginamas, nevertinamas informacijos rizikingumas kibernetinio saugumo trikdžių atžvilgiu. Galimybes kibernetinio saugumo užtikrinimui stipriai riboja tai, jog įmonės iki šiol deramai nevaldo ir neišnaudoja IT skyriaus darbuotojų potencialo ar galimybių – visa atsakomybė „numetama“ konkrečiam darbuotojui nepriimant strateginių sprendimų, neskiriant tinkamo finansavimo, kitu atveju suteikiami pernelyg dideli įgaliojimai, nesisaugojama ir neapibrėžiamos dėl darbuotojų elgesio kylančios rizikos. Saugumo incidentų registravimo procesai įmonėse vyksta taip pat nenuosekliai.

8. Darytina išvada, jog nors Lietuvos įmonės oficialiai deklaruoja kibernetinio saugumo užtikrinimo priemonių taikymą ir jų veiksmingumą, tačiau realybėje tam neretai pritrūksta lėšų, neįvertinamos galimos rizikos, ne iki galo suprantama kibernetinio saugumo svarba įmonių veiklai. Bendrai vertinant įmonių kibernetinio saugumo „stiprumo“ lygį, darytina išvada, jog situacija santykinai prasta – daugiau nei pusė įmonių tiki, jog praktikoje nesusidurs su kibernetiniais incidentais.

REKOMENDACIJOS

1. Esminis kibernetinio saugumo užtikrinimą garantuojantis veiksnys – ***kibernetinio saugumo svarbos identifikavimas strateginiu lygmeniu*** - įmonių atstovai turėtų būti pasiruošę ginti individualius informacijos saugumo poreikius, rūpintis kibernetinio saugumo specifika savo įmonėje atsižvelgiant į tai, jog vykdomos veiklos ypatumus ir jos saugos reikalavimus geriausiai išmano šią veiklą įgyvendinantys atstovai. Tinkamama strategijos formavimui labai praverstų tinkamas ***kibernetinio saugumo sąvokos bei šį saugumą apibūdinančių kriterijų išgryninimas įmonės lygmeniu;***

2. ***Būtina aktyvinti informacijos jautrumo vertinimą įmonės lygmeniu*** - informacijos jautrumo nustatymas ir jos apsauga turi būti užtikrinama skirtingomis priemonėmis – tiek fizinėmis, tiek elektroninėmis. Neįvertinus informacijos jautrumo ar kylančių rizikų bei taikant unifikuotas apsaugos priemones, jų tinkamumas ir efektyvumas gali labai sumenkti. Kaip papildoma priemonė, padedanti informacijos jautrumo vertinimui, siūlytina inicijuoti privalomą trikdžių registravimą;

3. Tinkamam kibernetinio saugumo užtikrinimo strategijos įgyvendinimui ***būtinas adekvataus dydžio biudžetas*** personalo kvalifikacijos kėlimui bei technologinių įrengimų atnaujinimui;

4. Gavus pakankamą finansavimą, būtinas įmonių ***IT komandos įgaliojimų stiprinimas ir kompetencijų gilinimas*** – tai leistų išvengti tokių situacijų, kuomet visa atsakomybė „numetama“ konkrečiam darbuotojui nepriimant strateginių sprendimų ar suteikiami pernelyg dideli įgaliojimai, nesisaugojama ir neapibrėžiamos dėl darbuotojų elgesio kylančios rizikos.

5. ***Būtina platesnė informacijos apie kibernetinio saugumo svarbą sklaida įmonės lygmeniu*** - šios srities žinias turėtų kaupti ne tik IT specialistai, bendrą suvokimą turėtų turėti kiekvienas įmonės darbuotojas, juolab įmonės vadovas. Tokios priemonės padėtų ne tik efektyvinti saugumo užtikrinimą, kartu sudarytų sąlygas formuoti efektyvesnę į kibernetinio saugumo užtikrinimą orientuotą strategiją.

Minėtas rekomendacijas siūlytina ***įgyvendinti laikantis ES kibernetinio saugumo strategijoje nurodomų pagrindinių efektyvų kibernetinį saugumą garantuojančių principų*** - garantuojant pagrindinių žmogaus teisių nuomonės reiškimo laisvės, privatumo ir asmens duomenų apsauga, suteikiant prieigą visiems, valdant demokratiškai ir efektyviai bei atsakomybę už kibernetinį saugumą prisiimant bendrai. Svarbu, kad visos įmonės, individualūs vartotojai suprastų įmonės apsaugos nuo kibernetinių atakų svarbą ir panaudotų visus veiksnius, kurie padidintų kibernetinio saugumo užtikrinimą.

LITERATŪROS SĄRAŠAS

1. Adomėnas V. *Standartizuota vadybos sistema: nuo kūrimo iki tobulinimo*. 2011. Kaunas.
2. Amoroso, E. *Cyber Security.* New Jersey: Silicon Press 2006.
3. Antrojo operatyvinių tarnybų departamento prie LR Krašto apsaugos ministerijos. Grėsmių nacionaliniam saugumui vertinimas. Vilnius. 2015. Interaktyvus. Prieiga internete: [http://www.vsd.lt/files/documents/635633000992101250.pdf], žiūrėta 2015-06-24.
4. Atkočiūnienė Z., *Informacijos resursai*. Vilnius, 1998.
5. Bagdonas E., Patašienė I.Patašius M., Skvernys V., „Internetinis verslo procesų imitavimas“. ISSN 1392-0561. Informacijos mokslai. 2007 42–43
6. Bae J., J.Caverlee, L.Liu, ir W.B.Rouse, „Process Mining, Discovery, and Integration using Distance Measures“. 2007. Interaktyvus. Prieiga internete: [https://smartech.gatech.edu/bitstream/handle/1853/14340/GT-CSS-06-06.pdf], žiūrėta 2015-06-03.
7. Buzan B. et al, Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers, Inc., 1997.
8. Bjorck, F., *Implementing Information Security Management Systems* .An Empirical Study of Critical Success Factors, 2002
9. *Canada's Cyber Security Strategy.* Ottawa: Public Safety Canada, Government of Canada. 2010
10. Canongia, C., & Mandarino, R., Cybersecurity: The New Challenge of the Information Society. In *Crisis Management: Concepts, Methodologies, Tools and Applications:* Hershey, PA: IGI Global 2014. 60-80 p.
11. Cavelty M.D "Cyber-Security". 2012. Interaktyvus. Prieiga internete; [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055122], žiūrėta 2015-06-05.
12. Cheung, A. S. Y. A Study of Cyber-Violence and Internet Service Providers' liability: Lessons from China. Pacific Rim Law & Policy Journal. 2009, 18(2): 345
13. Deibert R., Rohozinski R. *Liberation vs. Control: The Future of Cyberspace*. Journal of Democracy, 2010 21(4): 43-57.
14. De Toro I., McCabe T., *How to stay flexible and elude fads.* Quality Progress, 2007, Vol. 30, No. 3.
15. Dhillon, G., Managing and Controlling Computer Misuse. Information Management & Computer Security, 1999, Vol. 7, No. 4.
16. Davenport Th., Short J., „The New Industrial Engineering: Information Technology and Business Process Redesign“.July 15, 1990. Interaktyvus. Prieiga internete:

[http://sloanreview.mit.edu/article/the-new-industrial-engineering-information-technology-and-business-process-redesign/], žiūrėta 2015-06-01.

17. DHS.*A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security*, 2014.

18. Dunn, M. A., "National Security and the Internet: Distributed Security through Distributed Responsibility". International Studies Review, 11, 1, 2009.

19. Elzinga D. J., Horak T., Bruner C., *Business process management: survey and methodology*//IEEE Transactions on Engineering Management, Vol. 42 No 2. P.p. 119-27

20. Eriksson, J. Giampiero. "Conclusion: Digital-age security in theory and practice". Kn. Johan Eriksson and Giampiero Giacomello (sud.), International Relations and Security in the Digital Age. London & New York: Routledge, 2007.

21. Fung, P., Jordan, E., I*mplementation of Information Security: A Knowledge-based Approach*, 2002

22. Giaglis G., *Simulation for intra - and interorganizational business process modelling*, Informatika, 1997, Vol. 21, no 4, 613-620 p.

23. Gibson, W. (November 12, 2008). "Sci-fi special: William Gibson". New Scientist. Interaktyvus. Prieiga internete: [http://www.newscientist.com/article/mg20026821.600-scifi-special-william-gibson.html], žiūrėta 2015-06-23.

24. Goodall J. R., Lutters W. G., Komlodi A., *Developing Expertise for Network Intrusion Detection*. Information Technology & People, 2009 22(2): 92-108.

25. Hone, K. & Eloff, J.H.P, *What makes an Effective Information Security Policy*. Network Security, 2002, Vol. 20, No. 6.

26. Hommes B. ir kt., *Assessing the quality of business process modelling techniques*, 2000 California (USA)

27. ISO 27001. LST ISO/IEC 27001, Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai, Lietuvos standartizacijos departamentas.

28. ITU. *Overview of Cybersecurity. Recommendation ITU-T X.1205*. Geneva: International Telecommunication Union (ITU). 2009. Interaktyvus. Prieiga internete: [], žiūrėta 2015-06-24

29. Januta A., Marozas L., Informacinės saugos audito vykdymas remiantis ISO /IEC 27000 šeimos standartų reikalavimais, 2011, Vilnius

30. Januta A., „Introduction to electronic Identification". Interaktyvus. Prieiga internete: [https://open.dsv.su.se/mod/resource/view.php?id=64], žiūrėta 2015-10-30.

31. Jastiuginas S., *Informacijos saugumo valdymas Lietuvos viešajame sektoriuje*. Informacijos mokslai, 2011, 57, p. 7–25

32. Jouini M., Rabai L., Aissa A., *Classification of security threts in information systems*. Procedia Computer Science, 2014 Vol 32 489-896 p.

33. Juodis A., Oržekauskas P., Verslo procesų valdymo sprendimai, 2008, Kaunas: Technologija

34. Kalibaitė G., *Metažinių svarba įmonių veiklos ir informacijos valdymui*. 2011. KTU

35. Kardelis K. Mokslinių tyrimų metodologija ir metodai. - Kaunas: Judex, 2002. P. 12-23; 389-391.

36. Karjalainen M., Siponen M., „Toward a New Meta Theory for Designing Information Systems (IS) Security Training Approaches“. Journal of the Association for Information Systems. Volume 12, Issue 8, pp. 518-555, August 2011

37. Kazanavičius E., Žilinskas J., *Informacijos apdorojimo sistemos*. Technologija, Kaunas. 2002

38. Kemmerer, R. A., *Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering:* 2003, 705-715

39. Kiely L., Benzel T., „Systemic Security Management: A new conceptual framework for understanding the issues, inviting dialogue and debate, and identifying future research needs“. IEEE, security and privacy magazine. December. 2006

40. Kvedaravičius J., Organizacijų vystymos vadyba. 2006. Kaunas. VDU leidykla.

41. Lewis, J. A., *Cybersecurity and Critical Infrastructure Protection.* Washington, DC: Center for Strategic and International Studies, 2006

42. LR Kibernetinio saugumo įstatymas. 2014 m. gruodžio 11 d. Nr. XII-1428. TAR, 2014-12-23, Nr. 20553

43. LR Vyriausybės nutarimas dėl „Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“, Valstybės žinios, 2011-07-09, Nr. 83-4033.

44. Mackintoch A. L., *The need for enriched knowledge representation for enterprise in Enterprise Modelling*. 1993

45. Mikulis J., *Pažangūs vadybos principai. Visuotinė koybės vadyba*. 2007. Vilnius.

46. Niehaves B., Poeppelbuss J., Plattfaut R., BMP capability development – a matter of contingencies. Business Process Management, 2014 Journal Vol. 20, 90-106p.

47. Parker, B. D. *Computer Security Management. Reston*, VA: Reston Publishing Company Inc. 1981.

48. Paškauskas, Ž. *Elektroninės informacijos saugos tarptautinio teisinio reguliavimo analizė: Lietuvos padėtis.* 2007. Jurisprudencija Nr. 58 (83), p. 82-89.

49. Paškevičiūtė L., Čaplinskas A., „Verslo ir informacinių technologijų darna“. 2007.Information Sciences (Informacijos mokslai), issue: 4243/, pages: 145148

50. Paulauskas N., Garšva E., Skudutis J., *Network Scan Detection Simulation*. Elektra ir Elektronika. 2009. ISSN 1392-1215, 43-46 p

51. Polley V., Smith R., *Measuring KM Activity and Progress*. 2007

52. Repin, D. *Theories of Risk and Decision Making*. 2004

53. Ruževičius J., Kokybės vadybos metodai ir modeliai. Vilniaus Universitetas, 2006, 100-117 p.

54. Ruževičius J., Gediminaitė A., Verslo informacijos kokybės vertinimas. Informacijos mokslai, 2007, t. 40, 47-56 p.

55. Schou C., Hernandez S., *Information Assurance Handbook: Efective computer security and risk management strategies.* McGraw-Hill Osborne Media. 2014

56. Sewdass N., Chen X. H., Snyman M., *Interrelationship between document management, information management and knowledge management*. South Africa Journal of Information Management. 2005 Vol 7(3)

57. Štitilis D., Paškauskas Ž. *Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė*. 2007. Jurisprudencija Nr. 2 (92) 37-45 p.

58. Talabis M., McPherson R., Martin J., *Information Security Analytics*. Syngress, 2014

59. Zacharevičius P., Kvedaravičius J., Augustauskas T., Organizacijų vystymosi paradigma. 2004. Kaunas. VDU leidykla.

60. Varney, C. A., Consumer Privacy in the Information Age: A View from the United. States. Remarks before the Privacy and American Business National Conference, 1996, Washington.

61. Viliūnas, V. Projektų valdymo paskaitų konspektai. 2011.

62. Von Solms, R., Information Security Management: Why Standards are Important. Information Management & Computer Security, 1999, Vol. 7, No. 1, pp. 50-57.

63. Weesing F., Information System Management: Making Data Warehouses Talk Sence. Interaktyvus. Prieiga internete: [http://www.artmis.com/ism.html], žiūrėta 2015-05-26.

Pelenis P. *Kibernetinio saugumo užtikrinimo įtaka verslo procesams* / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas prof. dr. Darius Štitilis – Vilnius: Mykolo Romerio universitetas, Socialinių technologijų fakultetas, 2015. – 81 psl.

SANTRAUKA

Temos aktualumas grindžiamas nuostata, jog taikydama naująsias technologijas įmonė tampa labiau globalesnė, gali supaprastinti verslo procesus, atrasti daugiau nišų savo veiklai internetinėje erdvėje, administruoti savo darbuotojų veiklą. Būtina užtikrinti kibernetinį saugumą įmonėse, nes gali būti prarandama elektroninė informacija. Nacionalinio elektronikos ryšių tinklų ir informacijos saugumo tyrimo padalinio duomenimis 2014 metais kibernetinių nusikaltimų skaičius Lietuvoje siekė virš 36 tūkstančių, o lyginant su ankstesniais metais, išaugo virš 43 proc. Didžiausia kibernetinio saugumo problema ne tik Lietuvoje, bet ir visame pasaulyje yra tai, kad daugybė kibernetinių įrenginių turi saugumo spragų. Lietuvoje svarbu stiprinti ne tik kibernetinio saugumo įstatymus, bet ir aktyvinti privataus ir viešojo sektoriaus iniciatyvas bendradarbiaujant tarpusavyje stiprinti ir užtikrinti kibernetinį saugumą. Įvertinus temos aktualumą, susiduriama su tam tikra darbo problematika – kibernetinio saugumo užtikrinimas yra labai svarbus verslo procesams. Neretai kibernetinio saugumo priemonių taikymas tapatinamas su elektroninių duomenų, informacijos sauga, todėl iki šiol Lietuvos įmonėse pakankamai sudėtinga nustatyti kibernetinio saugumo priemonių taikymo intensyvumą ir paplitimą. Tai savo ruožtu apsunkina verslo procesų saugą kibernetinio saugumo prasme: nepakankamai įvertinamos galimos grėsmės, galimi incidentai bei jų pasekmės tiek įmonės, tiek valstybiniu mastu. Baigiamojo darbo tikslas – įvertinti kibernetinio saugumo užtikrinimo poveikį verslo procesams. Darbe atliekamas tyrimas pritaikant analizės, aprašomąjį, lyginamąjį, istorinį, loginį, lyginamąjį bei sisteminį metodus. uoju, lyginamuoju istoriniu, loginiu, lyginamuoju, sisteminiu metodais. Magistro darbą sudaro įvadas, 4 skyriai, išvados, rekomendacijos, literatūros sąrašas ir santraukos (lietuvių bei anglų kalbomis), priedai. Darbo apimtis 81 psl.

Pelenis P. *The influence ensuring cyber security in business processes* / Cyber security management master thesis. Supervisor prof. dr. Darius Štitilis. – Vilnius: University of Mykolas Romeris, Faculty of Social Technologies, 2015 . - 81 p.

SUMMARY

Relevance of the topic is based on the provision that the application of new technologies the company is becoming more globalized, can streamline business processes, to find more niches for their activities in the Internet space, to manage their workers. It is necessary to ensure cyber security companies, because there may be loss of electronic information. It is necessary to ensure cyber security companies, because there may be loss of electronic information. National electronic communications networks and information security investigation unit data for the year 2014 the number of cyber-crime Lithuania amounted to over 36 thousand, and in comparison with the previous year, increased by over 43 percent. The biggest cyber security problem not only in Lithuania, but also in the world is the fact that many cyber facilities have security vulnerabilities. Lithuania is important not only to enhance the cyber security law, but to activate the private and public sector initiatives to strengthen cooperation with each other to ensure cyber security. The evaluation of the relevance of the subject, there is a certain employment problems - cyber-security is a very important business processes. Often, cyber-security measures to avoid future confusion with electronic data, information security, and so far Lithuanian companies fairly complex set of cyber security measures the intensity and distribution. This in turn complicates the business process safety cybersecurity sense of underestimation of the potential threat of possible incidents and their consequences for both the company and national level. Final goal - to assess the influence ensuring cyber security in business processes. The work carried out by adapting research analysis, descriptive, comparative, historical, logical, comparative and systematic methods. th comparative historical, logical, comparative, systematic methods. The Master's thesis consists of an introduction, 4 chapters, conclusions, recommendations, references and summaries (in Lithuanian and English), accessories. Work volume 81 pages.

PRIEDAI

P1 Anketos pavyzdys

Anketos pavyzdys

Kibernetinio saugumo užtikrinimo įtaka verslo procesams

Šiandien bet kurio pobūdžio verslas iš dalies arba visas grindžiamas technologijomis, besivystančių IT dalis versle nuolat didėja. Taigi svarbia problema tampa informacijos saugumas. Ši apklausa skirta asmenims, dirbantiems Lietuvos verslo organizacijose. Jos tikslas - išanalizuoti Lietuvos verslo organizacijų informacijos saugumo užtikrinimo lygį ir šios srities planavimo organizacijose problemas. Apklausa yra anoniminė, rezultatai bus panaudoti rašant magistro baigiamąjį darbą. Iš anksto dėkui už atsakymus ir sugaištą laiką.
(Šios anketos rezultatai viešai nepublikuojami)

1.Jūsų amžius:
□18-21 m.
□22-25 m.
□26-30 m.
□31-40 m.
□41-50 m.
□daugiau nei 50 m.

2.Jūsų organizacijos dydis pagal darbuotojų skaičių:
□Vidutinė (50-249 darbuotojai)
□Maža (10-49 darbuotojai)
□Labai maža (iki 9 darbuotojų)

3.Jūsų darbo pozicija:
□Organizacijos vadovas
□Padalinio/srities vadovas
□Vadybininkas
□Specialistas
□Administratorius

4. Kaip esate linkę vertinti kibernetinio saugumo sampratą verslo įmonėje? Pasirinkite labiausiai priimtiną variantą.

 tam tikrų įrankių visuma, apimanti politikos, saugumo užtikrinimo gaires, rizikos valdymo metodus, veiksmus, mokymus, technologijas kurios gali būti naudojamos siekiant apsaugoti kibernetinę aplinką jos organizavimą ir vartojimo informaciją;

 informacinės visuomenės egzistavimo užtikrinimas ir tęstinumas, garantuojant ir apsaugojant elektroninę erdvę, jos informaciją, turtą bei ypatingos svarbos infrastruktūrą;

 procesas, veikla arba būsena pagal kurią informacijos ir ryšių sistemos yra saugomos nuo sugadinimo, neteisėto naudojimo ar modifikuotų pakeitimų;

 kita_____.

5. Su kuriais informacijos saugumo veiksniais Jūsų organizacijai teko susidurti per pastaruosius metus?

 Gamtos: pavyzdžiui, gaisras, potvynis, žemės drebėjimas ir kt.

□ Infrastruktūriniais: elektros tiekimo sutrikimas, vandentiekio arba kanalizacijos avarijos, avarinės būklės pastatai, telefoninio arba interneto ryšio sutrikimai, aplinkos užteršimas nuodingomis medžiagomis ir pan.
□ Žmogiškaisiais: personalo klaidos, nesankcionuoti jų veiksmai dėl mokymų, motyvacijos stokos, nepakankamo atsakomybių paskirstymo ir pan.
□ Technologiniais: įrangos gedimai ir pan.
□ Išorės žmonių sukelti veiksmai pažeidžiant informacijos saugumą elektroninių ryšių būdu
□ Išorės žmonių sukelti veiksmai fiziniu aspektu: įsibrovimas, įrangos vagystė, suniokojimas
□ Susidurti neteko

6. Su kuriais elektroninės informacijos saugumo incidentais yra susiduriama Jūsų organizacijoje? (1-niekada, 2-retai, 3-kartais, 4-dažnai, 5-labai dažnai)

	1	2	3	4	5
Nepageidaujami elektroninio pašto laiškai (angl. - spam)	□	□	□	□	□
Kenkėjiška programinė įranga (virusai, kirminai, trojos arkliai)	□	□	□	□	□
Klastojimo pranešimai, siekiant apgaule išvilioti duomenis (angl. - phishing)	□	□	□	□	□
Šnipinėjimo atvejai: elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas (angl. - Spyware)	□	□	□	□	□
Elektroninių paslaugų trikdymo ataka (angl. – DoS)	□	□	□	□	□

7. Ar Jūsų organizacijoje yra vadovybės patvirtinta kibernetinio saugumo politika?
□ Taip, kaip atskiras dokumentas
□ Taip, kaip įmonės IT valdymo strategijos dalis
□ Taip, kaip įmonės valdymo strategijos dalis
□ Ne

8. Kaip manote, kokiu tikslu būtina inicijuoti kibernetinio saugumo užtikrinimo strategiją? (Pažymėkite labiausiai priimtinas ar jau įgyvendinamas nuostatas).
□ Siekiant pagrindinių žmogaus teisių nuomonės reiškimo laisvės, privatumo ir asmens duomenų apsaugos;
□ Siekiant garantuoti prieigą prie duomenų visiems;
□ Siekiant efektyviai valdyti verslo procesus;
□ Siekiant bendrai pasidalinti atsakomybe užtikrinant duomenų saugumą.

9. Ar įmonės veikloje vertinate informacijos „jautrumą“ kibernetinio saugumo atžvilgiu?
□ Ne, tačiau kasdienėje veikloje naudojamės baziniais duomenų apsaugos elementais (ugniasiene, antivirusine programa, etc.);
□ Taip, mes suprantame informacijos saugos svarbą bendru įmonės kibernetinio saugumo užtikrinimo atžvilgiu.
□ Taip, informacijos jautrumas saugumo atžvilgiu garantuojamas „rūšiuojant“ informaciją - „jautri“ informacija apsaugoma papildomomis priemonėmis.

10. Ar atliekate su kibernetiniu saugumu susijusių rizikų vertinimą?
□ Tokio pobūdžio rizikos nevertiname;

 Atliekame rizikų vertinimą, tačiau neišskiriame konkrečių kibernetinio saugumo rizikos atvejų;
 Taip, nuolat atliekame su konkrečios informacijos, kibernetinio saugumu susijusių rizikų vertinimą.

11. Kokiu lygmeniu atliekamas kibernetinio saugumo priemonių valdymas?
 Kibernetinio saugumo priemonės savo iniciatyva nėra įgyvendinamos.
 Kibernetinio saugumo priemonės įgyvendinamos tik IT skyriuje nuotoliniu būdu;
 Kibernetinio saugumo priemonės įgyvendinamos tiek IT skyriuje, tiek kiekviename darbuotojo kompiuteryje priklausomai nuo informacijos pobūdžio.

12. Kiek procentų metinio informacijos technologijų biudžeto Jūsų organizacija skiria kibernetiniam saugumui?
 Iki 5%
 5-10%
 10-20%
 Daugiau nei 20%
 Visiškai neskiriama
 Nežinau

13. Ar savo įmonėje turite IT skyrių ar konkrečius kibernetiniu saugumu besirūpinančius darbuotojus?
 Neturime IT skyriaus ar konkretaus darbuotojo, kuris besirūpintų tik kibernetiniu saugumu;
 Neturime IT skyriaus, tačiau kiekvienas įmonės darbuotojas savo įgaliojimų ribose yra atsakingas už valdomos informacijos kibernetinį saugumą;
 Turime IT skyrių ir už kibernetinį saugumą atsakingą komandą.

16.Ar atliekate periodinį turimų technologijų ir įrengimų patikrinimą kibernetinio saugumo atžvilgiu?
 Neatliekame turimos įrangos, technologijų periodinių patikrinimų ar atsparumo įsiveržimams testavimo;
 Neturime sisteminio saugumo patikros režimo, tačiau atliekame patikrinimus esant poreikiui;
 Atliekame reguliarius turimos įrangos ir technologijų patikrinimus kibernetinio saugumo užtikrinimo prasme.

17.Ar Jūsų organizacijoje sukurtas saugumo incidentų registravimo procesas?
 Taip
 Ne
 Nežinau

18.Ar Jūsų organizacijoje atliekamas darbuotojų švietimas, mokymai kibernetinio saugumo tema?
 Taip
 Ne

19.Ar Jūsų organizacijoje darbuotojai gali naudoti mobilias aplikacijas tiesioginėms darbo užduotims atlikti?
 Taip, naudojame įmonės informaciją pasitelkiant mobilias aplikacijas, tiek dirbant nuotoliniu būdu. Šiais atvejais papildomų apsaugos priemonių netaikome;

 Egzistuoja vidinės taisyklės, draudžiančios talpinti ar dalintis organizacijos duomenimis naudojant asmenines mobilias aplikacijas, tačiau techniškai tai galima atlikti bet kuriuo metu;
 Asmeninės mobilios aplikacijos ar asmeniniai įrenginiai gali būti naudojami darbo užduotims atlikti tik tokiu atveju, jei jie atitinka kibernetinio saugumo užtikrinimo priemones, taikomas organizacijos viduje.

20. Jūsų nuomone, ar Jūsų organizacija yra pasiruošusi atlaikyti kibernetinį incidentą be neigiamų pasekmių?
 Nepatirsime kibernetinių incidentų, darbuotojai yra pakankamai kompetentingi susitvarkyti su iškylančiomis problemomis;
 Turime parengę standartizuotas kibernetinių incidentų valdymo procedūras, tačiau praktikoje jų nelabai esame linkę taikyti;
 Turime konkrečiai kibernetiniam saugumui skirtą procesų valdymo posistemę su reikalingais informacijos valdymo mechanizmais. Kiekvieno incidento atveju stengiamės kuo efektyviau valdyti kylančias grėsmes ir problemas bei tobulinti jau turimą mechanizmą.

Dėkoju už dėmesi