www.mruni.eu

Aurimas ŠIDLAUSKAS

DAKTARO DISERTACIJA

ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE SISTEMOS MODELIS

SOCIALINIAI MOKSLAI,
VADYBA (S 003)
VILNIUS, 2024

M R U
Mykolo Romerio
universitetas

MYKOLO ROMERIO UNIVERSITETAS

Aurimas Šidlauskas

ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE SISTEMOS MODELIS

Mokslo daktaro disertacija
Socialiniai mokslai, vadyba (S 003)

Vilnius, 2024

Mokslo daktaro disertacija rengta 2019–2023 metais Mykolo Romerio universitete pagal Vytauto Didžiojo universitetui su Klaipėdos universitetu, Mykolo Romerio universitetu ir Vilniaus universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 suteiktą doktorantūros teisę.

Mokslinis vadovas:
prof. dr. Tadas Limba (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija ginama Vytauto Didžiojo universiteto, Klaipėdos universiteto, Mykolo Romerio universiteto ir Vilniaus universiteto Šiaulių akademijos vadybos mokslo krypties taryboje:

Pirmininkas:
prof. dr. Andrius Stasiukynas (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Nariai:
prof. dr. Vida Davidavičienė (Vilniaus Gedimino technikos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Fernando Galindo (Saragosos universitetas, Ispanijos Karalystė, socialiniai mokslai, teisė, S 001);
prof. dr. Ligita Šimanskienė (Klaipėdos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Jan Žukovskis (Vytauto Didžiojo universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija bus ginama viešame Vadybos mokslo krypties tarybos posėdyje 2024 m. gegužės 10 d. 9.00 val. Mykolo Romerio universitete, I-414 auditorijoje.
Adresas: Ateities g. 20, Vilnius.

TURINYS

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

PRIEDŲ SĄRAŠAS

PAGRINDINĖS SĄVOKOS

Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (Bendrasis asmens duomenų apsaugos reglamentas, 2014).

Duomenų apsaugos pareigūnas – tai darbuotojas ar išorės ekspertas (paslaugos teikėjas), kuris prižiūri duomenų valdytojo ar duomenų tvarkytojo atitiktį Reglamentui ir padeda ją užtikrinti (Zaleskis, 2017).

Duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas (Bendrasis asmens duomenų apsaugos reglamentas, 2014).

Duomenų tvarkytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis (Bendrasis asmens duomenų apsaugos reglamentas, 2014).

Duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri viena ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones, kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti ES arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise (Bendrasis asmens duomenų apsaugos reglamentas, 2014).

Informacijos saugos įgaliotinis – strateginio lygio pareigybė, atsakinga už tai, kad informacinis turtas ir IT sistemos būtų apsaugoti ir saugūs ir kad tokia apsauga atitiktų organizacijos strateginę kryptį (Hooper ir McKissack, 2016).

Kibernetinė erdvė – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Kibernetinio saugumo subjektas – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Kibernetinis incidentas – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Valstybės informaciniai ištekliai – informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma (Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011).

SANTRUMPOS

BDAR – Bendrasis duomenų apsaugos reglamentas.
EK – Europos Komisija.
ES – Europos Sąjunga.
IRT – Informacinės ir ryšio technologijos.
IS – Informacinė sistema.
YSII – Ypatingos svarbos informacinės infrastruktūra.
IT – Informacinės technologijos.
JAV – Jungtinės Valstijos.
JK – Jungtinė Karalystė.
KAM – Lietuvos Respublikos krašto apsaugos ministerija.
KSĮ – Lietuvos kibernetinio saugumo įstatymas.
LR – Lietuvos Respublika.
NKSC – Nacionalinis kibernetinio saugumo centras.
RIS – Ryšių ir informacinės sistema.
Standartas ISO 27001 – Lietuvos standartas LST EN ISO/IEC 27001:2017 „*Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai*“.
Standartas ISO 27002 – Lietuvos standartas LST EN ISO/IEC 27002:2017 „*Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai*“.
VDAI – Valstybinė duomenų apsaugos inspekcija.
VK – Lietuvos Respublikos valstybės kontrolė.

ĮVADAS

Tyrimo aktualumas ir naujumas. Sparti technologinė plėtra dėl skaičiavimo galios progreso, padidėjusių duomenų saugojimo kiekių ir pažangesnio tinklo technologijos leidžia organizacijoms rinkti ir apdoroti vis didesnius duomenų kiekius. Žinių ekonomikoje duomenys tapo svarbia konkurencinio pranašumo kūrimo dalimi. Organizacijos, kurios nesugeba tinkamai apsaugoti asmens duomenų, gali prarasti vartotojų pasitikėjimą, kuris yra būtinas skatinant žmones naudotis naujais gaminiais ir paslaugomis. Asmens duomenų apsauga yra svarbus mokslinių tyrimų objektas, nes egzistuoja platus interpretavimo laukas, kaip ir kokiomis priemonėmis organizacijos turėtų apsaugoti asmens duomenis. Netinkamas asmens duomenų tvarkymas organizacijoms kelia finansinę, teisinę ir reputacijos riziką, todėl organizacijos, tvarkančios ES piliečių asmens duomenis privalo įgyvendinti ir užtikrinti Bendrojo duomenų apsaugos reglamento atitikties reikalavimus.

Šiuolaikinių organizacijų valdymo neįmanoma įsivaizduoti be informacinių technologijų ir informacinių sistemų bei interneto prieigos. Interneto, informacinių technologijų plėtra, informacijos perkėlimas į elektroninę erdvę didina informacinių procesų ir veiklos kokybę. Nors naujos technologijos ir paslaugos yra naudingos tiek verslui, tiek vartotojams, tačiau jos taip pat kelia rimtą pavojų kibernetiniam saugumui. Pasaulyje kiekvienais metais didėjant kibernetinių incidentų skaičiui, kibernetinis saugumo aktualumas didėja. Tai nėra tik technologinė problema, nes didžiąją daugumą kibernetinio saugumo problemų sukuria ne technologijos, o žmonės. Dažnai tai yra tyčiniai, gerai apgalvoti, tikslingai orientuoti į siekiamus tikslus, aukštos kvalifikacijos reikalaujantys veiksmai. Nėra universalaus sprendimo, siekiant užtikrinti kibernetinį saugumą, todėl svarbiomis tampa kompleksinės priemonės, apimančios nacionalinį reguliavimą, organizacijos vidaus politiką ir sėkmingų tarptautinių praktikų atkartojimą. Absoliutaus kibernetinio saugumo pasiekti neįmanoma, bet tinkamai parinktos ir taikomos saugumo priemonės, procedūros ir procesai gali sumažinti rizikos laipsnį ir praradimų mastą.

Organizacijos, norėdamos užtikrinti asmens duomenų apsaugą, yra privestos keisti, tobulinti duomenų tvarkymo procesus ir procedūras bei taikyti kibernetinio saugumo priemones. Bendrajame duomenų apsaugos reglamente nėra įvardyta, kokios kibernetinio saugumo priemonės yra tinkamos. Asmens duomenų apsauga yra aktuali ir svarbi šiandienos problematika, todėl tinkamų kibernetinio saugumo priemonių taikymas svarbus tiek teorine, tiek praktine prasme. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis leistų numatyti ir sumažinti galimas asmens duomenų apsaugos ir kibernetinio saugumo rizikas.

Apibendrinant disertacijoje analizuotus informacijos šaltinius galima teigti, kad mokslinėje literatūroje tyrėjai atkreipia dėmesį į tokias asmens duomenų apsaugos ir kibernetinio saugumo sąveikos reiškinio problematikas: kokie pagrindiniai asmens duomenų apsaugos ir kibernetinio saugumo reikalavimai; kokios pagrindinės asmens duomenų apsaugos ir kibernetinio saugumo užtikrinimo interpretacijos; koks duomenų apsaugos pareigūno vaidmuo organizacijoje; kaip valdyti asmens duomenų

saugumo pažeidimą ir kibernetinį incidentą; kaip asmens duomenų saugaus valdymo elektroninėje erdvėje priemonės gali sumažinti asmens duomenų pažeidimo ir kibernetinio incidento rizikas; ir kt. Verta pastebėti, kad asmens duomenų apsaugos ir kibernetinio saugumo užtikrinimo organizacijose vertinimo tyrimai nėra išplėtoti. Taigi asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio priemonės vertinimo aspektu yra aktualus tyrimų objektas tiek teoriniu, tiek ir praktiniu požiūriais, jo platesniam pažinimui ir skiriamas šis disertacinis darbas.

Temos ištirtumo lygis. Pasaulio ir Lietuvos mokslininkai, tarptautinės ir Lietuvos organizacijos kibernetinį saugumą ir asmens duomenų apsaugą nagrinėja įvairiais aspektais.

Asmens duomenų apsaugą, kaip reiškinį, nagrinėjo: Tikkinen-Piri, 2018; Cortez, 2021; Voigt, Von dem Bussche, 2017; Kamleitner, Mitchell, 2018; Cabral, 2021; Malinauskaitė-van de Castel, 2017; Zaleskis, 2019; Limba, Šidlauskas, 2020; Tamavičiūtė, 2019; Diker Vanberg, Ünver, 2017; Ooijen, Vrabec, 2019; Feth, 2020; Sánchez, ir kt. 2021; Dibble, 2019; Gobeo ir kt., 2018; Alkhaledi, Hawamdeh, 2020; Teixeira, 2019; Europos komisija (EK), 2020; Andrijauskas, Morkūnienė, 2020; Europos duomenų apsaugos valdyba; Alford, 2020; Gabel, Hickman, 2019; Presthus, Sønslien, 2021; Piras, 2019.

Kibernetinį saugumą, kaip reiškinį, nagrinėjo: Bayne, 2008; Jastiuginas, 2011; Asquith, Morgan, 2020; Möller, 2020; Nacionalinis kibernetinio saugumo centras (NKSC), Solms, von Solms, 2018; Štitilis, 2016; Horák, 2019; National Institute of Standards and Technology (NIST); International Organization for Standardization (ISO); Schreider, 2020; Raval, 2018; Corradini, 2020; Esparza, 2020; Thiéry, Fass, 2020; Chang, 2020; Wu, 2020; Reeves, 2020; Schreider, 2017; Agafonov, 2021; Hooper, McKissack, 2016; Ritchey, 2020; Maurer, 2021; Blum, 2020; Harknett, Grincevičius, 2019.

Asmens duomenų apsaugos priemones nagrinėjo: Štarchoň, Pikulík, 2019; Blanco-Lainé, 2019; Grütter, Schneider, 2019; Bock, 2021; Chassang, 2017; Valstybinė duomenų apsaugos inspekcija (VDAI); Pandit, 2019; Helbing, 2022; Hilberg, 2022; Valstybės kontrolė (VK); Drewer, 2018; Felici, 2013; Freitas, Silva, 2018; Mouratidis, 2016; Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA); International Organization for Standardization (ISO); Ryan, 2020; Haes, 2013; Demetzou, 2018; Europos duomenų apsaugos valdyba; Aven, 2016; Shimonski, 2016; Gibson, 2014; Tikkinen-Piri, 2018; Barnard-Wills, 2019; Perry, 2019; Werner, 2020; Carey, 2019; Tiliute, 2019; Harkous, 2018; Linden, 2018; Wolford, 2022; Degeling, 2018; Eijk, 2019; Nouwens, 2020; SANS institutas.

Kibernetinio saugumo priemones nagrinėjo: Cheng, 2020; Alghamdi, 2021; Ghelani, 2022; Kahyaoglu, Caliyurt, 2018; Lubua, Pretorius, 2019; Aliyeva, Hwang, 2019; Patterson, 2017; Koskelo, 2020; Wang, 2018; Cabaj, 2018; Hooper, McKissack, 2016; Kaselis, Pivoras, 2012; Scarfone, 2021; Buccafurri, 2015; Chapple, 2018; Gollmann, 2015; Menard, 2017; Kovács, 2018; Cains ir kt., 2022; Rea-Guaman, 2020; Black, 2018; Fielder, 2018; Claroty, 2021; Zimmermann, Renaud, 2019; Chowdhury, 2019; Chochlova, 2022; Dean, McDermott, 2017; Aldawood, 2020; Lois, 2020; Fernando, 2017; Bisson, 2021; Aoyama, 2015; Baig, 2022; George, 2021; Mandritsa, 2018.

Mokslinė problema – Koks turi būti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, siekiant sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas?

Mokslinio tyrimo objektas – Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio priemonės.

Mokslinio tyrimo tikslas – parengti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį, kuris padėtų sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas.

Siekiant iškelto tikslo, disertacijoje sprendžiami tokie uždaviniai:

1. Išanalizuoti asmens duomenų apsaugos ir kibernetinio saugumo sąveikos teorinius aspektus.
2. Atlikti kokybinius dokumentų analizės, atvejo analizės ir ekspertų nuomonės tyrimus, kuriais remiantis būtų nustatyti asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių kriterijai modeliui sukurti.
3. Pasiūlyti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį.
4. Įvertinti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkius ir galimybes.

Mokslinio tyrimo metodai ir pagrindiniai šaltiniai. Siekiant iškelto tikslo ir sprendžiant iškeltus uždavinius disertacijos teorinėje dalyje atliekama mokslinės literatūros šaltinių sisteminė lyginamoji analizė ir apibendrinimas. Rengiant disertacijos empirinę dalį pasitelkta atvejo studija, taikomi vienas kitą papildantys kokybiniai empiriniai tyrimai: dokumentų analizė, ekspertinis interviu, kokybinė turinio analizė, antrinių šaltinių duomenų analizė. Empirinė tyrimo dalis grindžiama teorinėje dalyje išdėstytomis įžvalgomis ir remiamasi interpretacinės paradigmų teorinėmis prielaidomis.

Disertacijos ginamieji teiginiai:

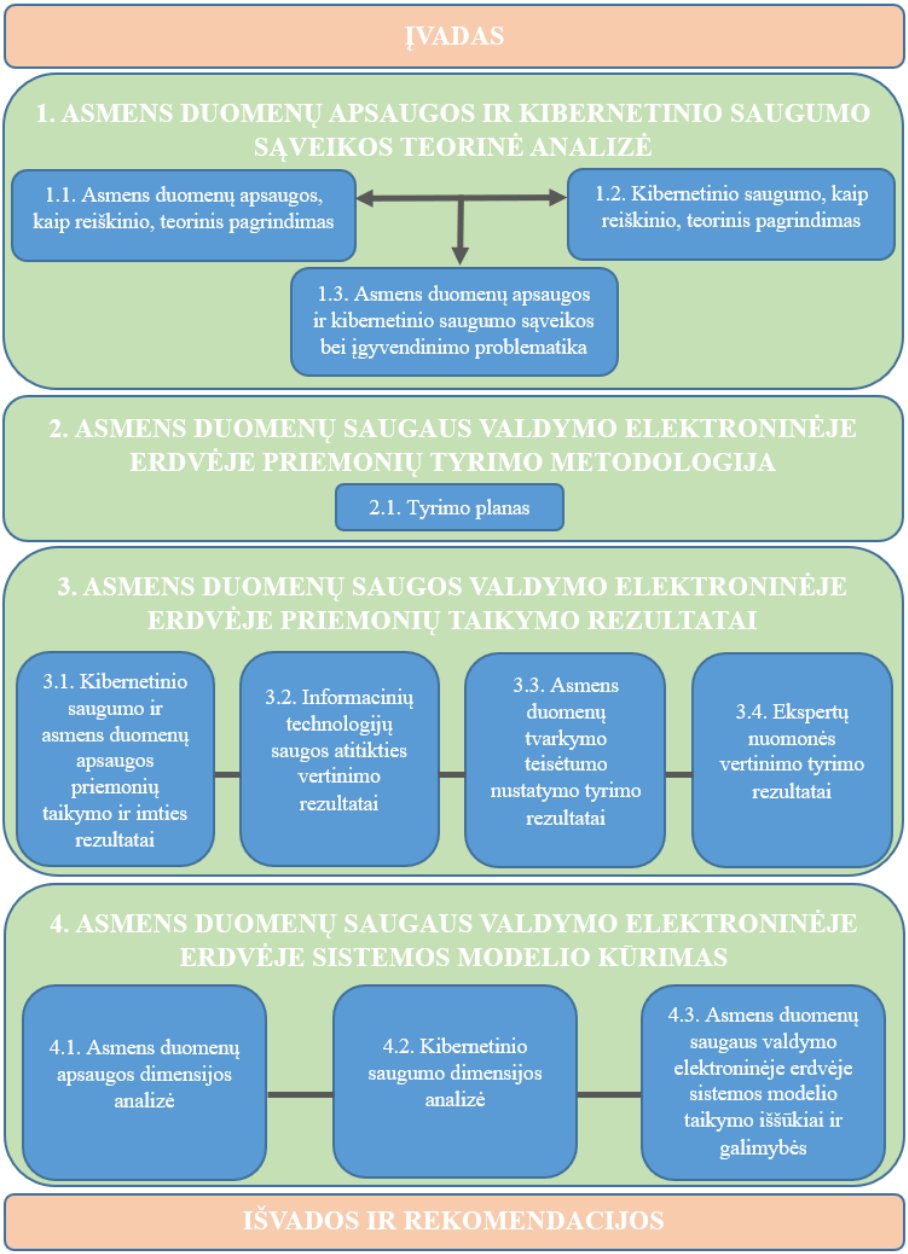
1. Kibernetinis saugumas yra asmens duomenų apsaugos dalis.
2. Kibernetinio saugumo užtikrinimas neapsaugo nuo rizikos įvykti asmens duomenų saugumo pažeidimui.
3. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis sumažina riziką įvykti asmens duomenų saugumo pažeidimui ir kibernetiniam incidentui.

Tyrimo teorinis ir praktinis reikšmingumas. Sukurtas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, kurio asmens duomenų apsaugos ir kibernetinio saugumo dimensijose nagrinėjamos įvairios asmens duomenų saugaus valdymo priemonės, kurių tikslas yra sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo rizikas, siekiant užtikrinti elektroninės informacijos, įskaitant duomenis ir asmens duomenis, prieinamumą, vientisumą bei konfidencialumą bet ir užtikrinti pagrindinius asmens duomenų tvarkymo principus, apsaugant fizinių asmenų teises ir laisves dėl asmens duomenų tvarkymo.

Pažymėtina, kad šį asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį galės naudoti visos organizacijos, valdančios arba tvarkančios asmens

duomenis, kurios siekia pagerinti asmens duomenų apsaugą ir kibernetinį saugumą bei jų valdymą ir sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelyje kiekviena tiek asmens duomenų apsaugos, tiek kibernetinio saugumo dimensijos priemonė, nuo I iki III lygio, galės būti įgyvendinama atskirai, atsižvelgiant į organizacijos veiklos ypatumus, valdomus išteklius, turimus resursus bei finansines galimybes. Tačiau asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio IV lygmuo bus siejamas su visų asmens duomenų apsaugos ir kibernetinio saugumo dimensijose išvardintų priemonių įgyvendinimu, siekiant virsmo į integruotą asmens duomenų apsaugos ir kibernetinio saugumo valdymo sistemą, kurioje priemonės yra susietos bei veiks viena kitą papildydamos.

Darbo struktūra. *Darbo pradžioje* yra pateikiamas įvadas. Darbą sudaro keturios dalys. *Pirmoje dalyje* yra nagrinėjama asmens duomenų apsaugos ir kibernetinio saugumo sąveikos teorinė analizė: Asmens duomenų apsaugos, kaip reiškinio, teorinis pagrindimas; Kibernetinio saugumo, kaip reiškinio, teorinis pagrindimas; Asmens duomenų apsaugos ir kibernetinio saugumo sąveikos bei įgyvendinimo problematika. *Antroje dalyje* yra pristatoma asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių tyrimo metodologija: Tyrimo planas. *Trečioje dalyje* yra pateikti asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių taikymo rezultatai: Kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymo ir imties rezultatai; Informacinių technologijų saugos atitikties vertinimo rezultatai; Asmens duomenų tvarkymo teisėtumo nustatymo tyrimo rezultatai; Ekspertų nuomonės vertinimo tyrimo rezultatai. *Ketvirtoje dalyje* yra atliekamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kūrimas: Asmens duomenų apsaugos dimensijos analizė; Kibernetinio saugumo dimensijos analizė; Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkiai ir galimybės. *Darbo pabaigoje* yra pateikiamos išvados ir rekomendacijos (žr. 1 pav.).



1 pav. Disertacinio darbo struktūros loginė schema

Šaltinis: sudaryta autoriaus

1. ASMENS DUOMENŲ APSAUGOS IR KIBERNETINIO SAUGUMO SĄVEIKOS TEORINĖ ANALIZĖ

1.1. Asmens duomenų apsaugos, kaip reiškinio, teorinis pagrindimas

1.1.1. Asmens duomenų samprata, klasifikavimas ir jų tvarkymo pagrindai bei pagrindiniai principai

Praeito dešimtmečio pradžioje Pasaulio ekonomikos forume asmens duomenys buvo apibūdinti kaip nauja turto klasė, kurią sudaro asmens duomenis renkančių, analizuojančių ir jais prekiaujančių subjektų ekosistema (Schwab ir kt., 2011). Vėliau Spiekermann ir kt. (2015) pabrėžė, kad asmens duomenys yra laikomi nauju turtu, nes jie gali sukurti pridėtinę vertę įmonėms ir vartotojams. Neturint asmens duomenų, kai kurių paslaugų teikimas taptų neįmanomu. Acquisti ir kt. (2016) pastebėjo, kad asmens duomenų naudojimas vykdant komercinę veiklą gali sumažinti vartotojų privatumą, o kartais ir socialinę gerovę. Įvykus asmens duomenų saugumo pažeidimui arba kibernetiniam incidentui, viena svarbiausių rizikų įmonei yra klientų pasitikėjimo praradimas ir neigiamas poveikis būsimam verslui. Todėl kibernetinis saugumas ir asmens duomenų apsauga turėtų būti laikomi organizacijų prioritetu, siekiant išsaugoti pasitikėjimą verslu (Corradini, Nardelli, 2020).

Kiekviena valstybė turi imtis priemonių, užtikrinančių asmens duomenų apsaugą skaitmeninėje erdvėje. Tarp populiariausių priemonių yra teisės aktų priėmimas ir infrastruktūros kibernetinei erdvei sukūrimas (Jasmontaitė, Burloiu, 2017). ES Bendrasis duomenų apsaugos reglamentas (toliau – Reglamentas arba BDAR) įsigaliojo 2018 metų gegužės 25 dieną. Reglamento tikslas yra apsaugoti fizinių asmenų pagrindines teises ir laisves, visų pirma jų teisę į asmens duomenų apsaugą. Reglamentas taikomas visoms įmonėms, tvarkančioms ir laikančioms ES gyvenančių duomenų subjektų asmens duomenis, neatsižvelgiant į įmonės buvimo vietą (Schreider, 2020). Be abejo, Reglamentas pakeitė tarptautinių kompanijų strategijas, susijusias su Europa (Axinte ir kt., 2018). Taip pat svarbu pažymėti, kad Reglamentas turi būti neutralus technologijoms, siekiant užtikrinti, kad asmens duomenų apsauga nepriklausytų nuo apdorojimo metodų ir būtų pritaikyta naujoms technologijoms (Cortez, 2021). Reglamentu siekiama išspręsti dabartinius iššūkius, susijusius su asmens duomenų apsauga, sustiprinti privatumo teises internete ir skatinti skaitmeninę ekonomiką (Limba ir kt., 2020). Tačiau vien teisės akto priėmimas savaime negarantuoja jo veiksmingumo, siekiant numatyto tikslo (Awesta, 2021). Ankstyvas būtinų pakeitimų priėmimas ne tik garantuoja atitiktį Reglamentui, tačiau taip pat gali suteikti konkurencinį pranašumą (Tikkinen-Piri ir kt., 2018). Europos Komisija (2018) teigia, kad organizacijos, kurios nesugeba tinkamai apsaugoti asmens duomenų, gali prarasti vartotojų pasitikėjimą, kuris yra būtinas skatinant žmones naudotis naujais gaminiais ir paslaugomis.

Kartu su Reglamento taikymo pradžia veiklą pradėjo ES valstybių narių asmens

duomenų apsaugos priežiūros institucijas vienijanti Europos duomenų apsaugos valdyba (toliau – Valdyba) – nepriklausoma ES institucija, kuri padeda užtikrinti nuoseklų duomenų apsaugos taisyklių taikymą visoje ES. Ypatingas Valdybos vaidmuo asmens duomenų apsaugos srityje yra oficialiai aiškinti Reglamento nuostatas, šitaip užtikrinant vienodą šio teisės akto taikymą visoje ES. Vienas svarbiausių Valdybos veiklos elementų – gairių, rekomendacijų ir geriausios praktikos pavyzdžių pateikimas visuomenei.

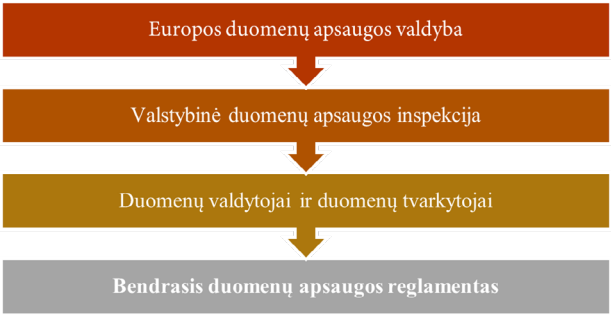
Lietuvos Respublikos asmens duomenų apsaugos priežiūros institucija yra VDAI, kurios misija – ginti žmogaus teisę į asmens duomenų apsaugą. Valdybos ir VDAI pateikta rekomendacinė medžiaga yra naudinga duomenų valdytojams ir tvarkytojams, siekiant įgyvendinti Reglamento reikalavimus.

Norint pasiekti Reglamento atitiktį, reikia dar daug dirbti visame pasaulyje. „*Thompson Reuters*“ pranešime, paskelbtame maždaug po vienerių metų nuo tos dienos, kai Reglamentas įsigaliojo, teigiama:

- Daugiau organizacijų nesilaiko Reglamento nei laikosi.
- Daugeliui organizacijų Reglamento atitikties įgyvendinimas tapo daug didesniu iššūkiu, nei buvo tikėtasi.
- Pusei visų organizacijų kyla pavojus neįgyvendinti Reglamento.
- Vis daugiau organizacijų patiria spaudimą įgyvendinti Reglamento reikalavimus.
- Organizacijos tampa mažiau atviros ir iniciatyvios vartotojų atžvilgiu.
- Mažėja organizacijos aukščiausios vadovybės ir žemesnės grandies vadovų susirūpinimas ir įsitraukimas į duomenų apsaugos klausimus.
- Reglamento įgyvendinimas organizacijose reikalauja finansinių išteklių.

Duomenų valdytojai yra pagrindinius sprendimus priimantys asmenys, nes nusprendžia, kodėl ir kaip bus tvarkomi asmens duomenys. Duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairius tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms. Prireikus techninės ir organizacinės priemonės yra peržiūrimos ir atnaujinamos, kad būtų užtikrintas pavojų atitinkančio lygio saugumas. Duomenų valdytojas, įgyvendindamas atitinkamą duomenų apsaugos politiką ir taikydamas tinkamas priemones, privalo įrodyti, kad duomenys tvarkomi laikantis Reglamento reikalavimų.

Valdyba ir VDAI atlieka kontrolės mechanizmo funkciją, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų Reglamento nuostatas (žr. 2 pav.).



2 pav. Reglamento taikymas ir priežiūros kontrolė

Šaltinis: sudaryta autoriaus

Reglamentu siekiama užtikrinti vienodo ir aukšto lygio fizinių duomenų apsaugą bei nuoseklų ir vienodą taisyklių, kuriomis reglamentuojama fizinių asmenų pagrindinių teisių ir laisvių apsauga tvarkant asmens duomenis, taikymą. Šiam tikslui pasiekti Reglamento 5 straipsnis įtvirtina septynis principus, kuriais savo veikloje yra įpareigoti vadovautis visi duomenų tvarkytojai ir duomenų valdytojai tam, kad bet koks asmens duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga. Pagrindiniai asmens duomenų tvarkymo principai (žr. 1 lentelę).

1 lentelė. Pagrindiniai asmens duomenų tvarkymo principai

Principas	**Apibūdinimas**
Teisėtumo, sąžiningumo ir skaidrumo principas	Asmens duomenys duomenų subjekto atžvilgiu turi būti tvarkomi teisėtu, sąžiningu ir skaidriu būdu
Tikslo apribojimo principas	Asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu
Duomenų kiekio mažinimo principas	Asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi
Tikslumo principas	Asmens duomenys turi būti tikslūs ir prireikus atnaujinami. Turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi
Saugojimo trukmės apribojimo principas	Asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi

Principas	Apibūdinimas
Vientisumo ir konfidencialumo principas	Asmens duomenys turi būti tvarkomi tokiu būdu, kad, taikant atitinkamas technines ar organizacines priemones, būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo
Atskaitomybės principas	Duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi duomenų tvarkymo principų, ir turi sugebėti įrodyti, kad jų laikomasi

Šaltinis: Bendrojo duomenų apsaugos reglamento 5 straipsnis.

Organizacijoms už netinkamą asmens duomenų tvarkymą gresia įvairios sankcijos. VDAI gali teikti nurodymus dėl pažeidimų ištaisymo, papeikimus, nustatyti laikiną arba galutinį draudimą tvarkyti duomenis ir kt. Pažeidus Reglamento nuostatas, gali būti skiriamos administracinės baudos, kurios kiekvienu konkrečiu atveju turi būti veiksmingos, proporcingos ir atgrasomos. Taigi bauda gali siekti iki 2–4 proc. ankstesnių finansinių metų bendros metinės pasaulinės apyvartos, arba iki 10 000000 – 20 000000 eurų. Tai maksimalios baudos, tačiau žemutinė baudų riba gali būti bet kuri minimali skaitinė išraiška.

Tinkamas duomenų apsaugos mechanizmas yra viešasis interesas, kurį patenkinti valstybei yra gyvybiškai svarbu. Nors asmens duomenų apsauga nėra absoliuti teisė, tačiau ji įgauna vis svarbesnį vaidmenį kasdieniniame gyvenime (Batutytė, 2019).

Asmens duomenų apibrėžimas yra platus, lankstus ir pritaikomas prie technologinio konteksto (Purtova, 2018). Reglamente apibrėžta, kad asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius. Šis apibrėžimas paaiškina, kad asmens duomenys yra bet kokia informacija, kuri gali būti naudojama atskirai arba kartu su kita informacija asmeniui identifikuoti, susisiekti (kontaktuoti) ar jo buvimo vietai nustatyti. ES 29 straipsnio duomenų apsaugos darbo grupė (toliau – ES 29 straipsnio darbo grupė) suskirstė asmens duomenis į keturis pagrindinius elementus (2007). Šie elementai glaudžiai susiję ir vienas nuo kito priklausomi, o visi kartu leidžia nustatyti, ar informaciją reikia laikyti asmens duomenimis:

1. *Bet kokia informacija*. Reikalauja plačiai aiškinti sąvoką, neatsižvelgiant į informacijos pobūdį ar turinį ir techninį formatą, kuriuo ji pateikiama. Tai reiškia, kad tiek objektyvi, tiek subjektyvi informacija apie asmenį bet kokia forma gali būti laikoma „*asmens duomenimis*“, neatsižvelgiant į techninę laikmeną, kurioje ji pateikiama.

2. *Informacija, susijusi su asmeniu.* Apima informaciją, kuri gali daryti aiškų poveikį tam, kaip su asmeniu elgiamasi arba kaip jis vertinamas.
3. *Asmuo, kurio tapatybė yra nustatyta arba gali būti nustatyta.* Atsižvelgia į sąlygas, kurioms esant reikia laikyti, kad asmens „*tapatybę galima nustatyti*“, ir ypač į priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar kitas asmuo to asmens tapatybei nustatyti. Šioje analizėje labai svarbus konkretus kontekstas ir ypatingos situacijos aplinkybės.
4. *Fizinis asmuo.* Susijęs su nuostata, kad asmens duomenys yra informacija apie „*gyvus asmenis*“.

Organizacijos, pradėdamos veiklą, kuri apima asmens duomenų tvarkymą, visada turėtų apsvarstyti, koks būtų tinkamas teisėtas numatomo duomenų tvarkymo pagrindas. Duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šių Reglamento 6 straipsnio sąlygų:

1. Asmuo davė sutikimą tvarkyti duomenis.
2. Tvarkyti duomenis būtina, siekiant įvykdyti sutartį (sutartinė prievolė).
3. Tvarkyti duomenis būtina, kad būtų įvykdyta teisinė prievolė.
4. Tvarkyti duomenis yra būtina, siekiant atlikti užduotį, vykdomą viešojo intereso labui.
5. Tvarkyti duomenis būtina, siekiant apsaugoti gyvybinius asmens interesus.
6. Tvarkyti duomenis būtina, siekiant teisėtų organizacijos interesų, išskyrus atvejus, kai asmens teisės yra viršesnės už organizacijos interesus.

Reglamente apibrėžiamos kai kurios asmens duomenų kategorijos, kurios yra neskelbtinos ir nustato draudimą juos tvarkyti, išskyrus tam tikras išimtis. Šios duomenų kategorijos vadinamos specialiai saugomais duomenimis, specialiomis asmens duomenų kategorijomis arba neskelbtinais duomenimis (Cabañas ir kt., 2020). Reglamento 9 straipsnyje rašoma, kad draudžiama tvarkyti asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją. Išskyrus Reglamente numatytus atvejus. Asmens duomenis, susijusius su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis, pagal Reglamento 10 straipsnį, galima tvarkyti tik prižiūrint valdžios institucijai arba kai tai leidžiama pagal ES ar nacionalinę teisę.

Svarbu pabrėžti, kad asmens duomenims, kurie buvo pseudonimizuoti, taikoma Reglamento taikymo sritis. Reglamente rašoma, kad pseudonimų suteikimas yra asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės, siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti. Akivaizdu, kad duomenys, kuriems taikoma pseudonimizacija, yra asmens duomenys (Mourby ir kt., 2018). Pseudonimų suteikimas asmens duomenims gali sumažinti atitinkamiems duomenų subjektams kylančius pavojus ir padėti duomenų valdytojams ir duomenų

tvarkytojams įvykdyti savo duomenų apsaugos prievoles. Europos duomenų apsaugos teisės vadove (2014) rašoma, kad duomenų pseudonimizavimas yra viena svarbiausių priemonių, naudojamų dideliam kiekiui duomenų apsaugoti, kai neįmanoma visiškai atsisakyti duomenų naudojimo. Asmens duomenys, kurių žymenys tapatybei nustatyti yra užšifruoti, naudojami įvairiomis aplinkybėmis, siekiant užtikrinti asmenų tapatybės slaptumą. Tai ypač naudinga tuomet, kai duomenų valdytojai turi užtikrinti, kad būtų tvarkomi tų pačių duomenų subjektų duomenys, tačiau jiems nereikia ir jie neprivalo žinoti tikrosios duomenų subjektų tapatybės.

Anoniminiai duomenys yra priešingi asmens duomenims ir nurodo informaciją, kuri nėra susijusi su identifikuotu ar atpažįstamu asmeniu. Voigt ir Von dem Bussche (2017) rašo, kad anonimizavimas yra asmens duomenų modifikavimo būdas, kuomet nėra arba neišlieka jokio ryšio su asmeniu. Anonimizuoti duomenis galima naudojant keletą metodų, paprastai priskiriamų dviem kategorijoms:

1. Atsitiktinis pasirinkimas – tai duomenų tikslumo keitimas, siekiant pašalinti duomenų ir asmens ryšį. Jei duomenys tampa pakankamai neapibrėžti, jie nebegali būti priskirti konkrečiam asmeniui.

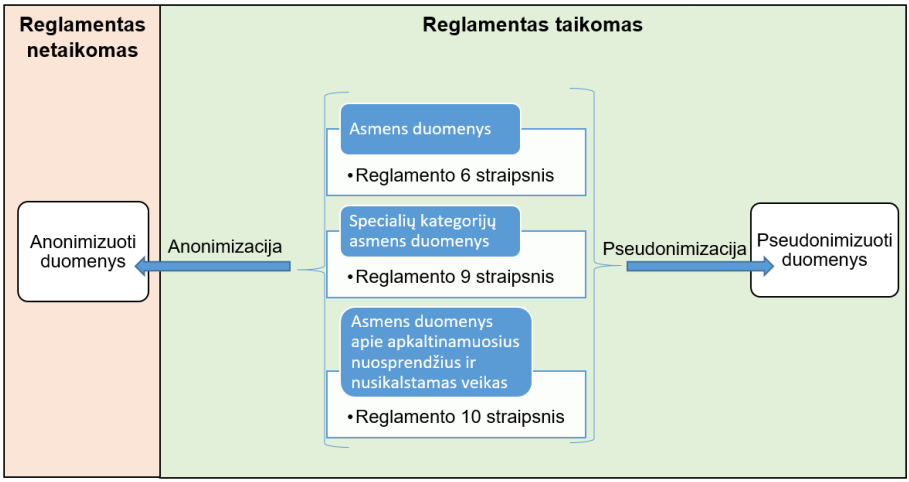
2. Apibendrinimas – apima duomenų subjektų požymių apibendrinimą, modifikuojant atitinkamą duomenų skalę ar tvarką.

Anonimiškos informacijos tvarkymui Reglamentas netaikomas. ES 29 straipsnio darbo grupė (2007) suformulavo tris pagrindinius patikimos anonimizavimo metodo vertinimo kriterijų klausimus, į kuriuos turėtų būti atsakyta neigiamai, norint išlaikyti anonimiškumo testą:

1. Ar vis dar įmanoma išskirti asmenį iš kitų?
2. Ar vis dar įmanoma susieti tam tikrus duomenis su asmeniu?
3. Ar iš turimos informacijos galima daryti išvadą apie asmenį?

Jei duomenų valdytojas ar duomenų tvarkytojas gali atkurti anoniminę informaciją arba kyla tikimybė, tai bus laikoma asmens duomenimis. Organizacijos dažnai saugo ir renka labai didelius duomenų kiekius, nors jų apdorojimo veiklai galiausiai reikia tik nedidelės dalies duomenų, todėl anonimizavus šiuos duomenis nebereikia laikytis Reglamento reikalavimų.

Teoriniame duomenų tvarkymo modelyje matome, kokiems duomenims (įskaitant jų tvarkymo pagrindą) yra taikomi Reglamento reikalavimai (žr. 3 pav.).



3 pav. Teorinis asmens duomenų tvarkymo modelis

Šaltinis: Limba ir Šidlauskas, 2020

Apibendrinant galima teigti, kad asmens duomenys tapo labai vertingu organizacijų, duomenų valdytojų ir tvarkytojų, turtu, kuris dažnai yra pagrindas teikti ir vystyti paslaugas. Tačiau organizacijoms tvarkant asmens duomenis turėtų būti svarbūs ne tik jų interesai, bet ir duomenų subjektų, t. y. asmenų, kurių asmens duomenis jos tvarko, nes įsigaliojus Reglamentui už netinkamą asmens duomenų tvarkymą gali kilti atsakomybė – teisinė, finansinė, reputacijos. Valdyba ir VDAI atlieka kontrolės mechanizmo funkciją, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų Reglamento nuostatas. Organizacijos tvarkančios asmens duomenis privalo pakeisti asmens duomenų tvarkymo procesus ir procedūras, kad užtikrintų pagrindinius asmens duomenų tvarkymo principus, siekiant apsaugoti fizinių asmenų pagrindines teises ir laisves, visų pirma jų teisę į asmens duomenų apsaugą, kitu atveju duomenų tvarkymas bus neteisėtas. Reglamentas netaikomas asmens duomenims, kurie buvo anonimizuoti, tačiau pseudonimizuoti duomenys visiškai patenka į Reglamento taikymo sritį ir turi būti vertinami vienodai, atsižvelgiant į saugumą ir apdorojimą, lyg asmens duomenys. Pseudonimizacija nepašalina visos asmens identifikavimo informacijos iš duomenų, o tik sumažina duomenų rinkinio susiejimą su asmeniu. Atliekant anonimizavimą ir pseudonimizavimą galima palengvinti Reglamento įgyvendinimą organizacijoje ir apsaugoti atskirų duomenų subjektų teises į privatumą.

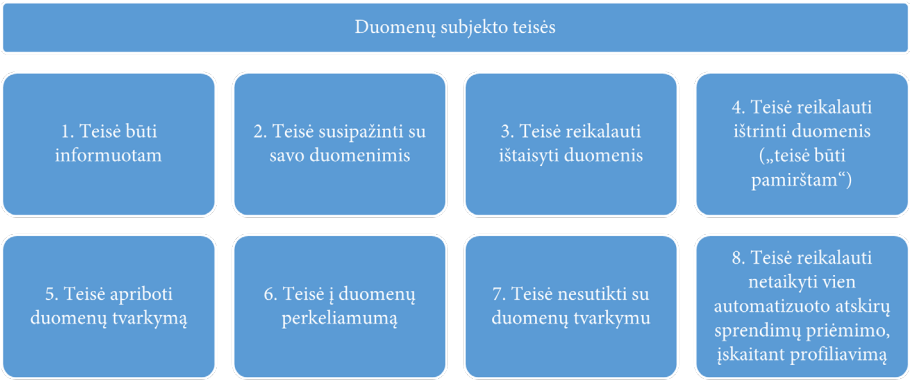
1.1.2. Duomenų subjektų teisių įgyvendinimas organizacijoje

Dėl padidėjusio technologinio sudėtingumo ir daugybės duomenų naudojimo verslo praktikoje vartotojams tampa vis sunkiau kontroliuoti savo asmens duomenis. Stebėdami šias tendencijas, mokslininkai perspėjo dėl daugybės grėsmių individualiai kontrolei, pavyzdžiui, informacijos pertekliaus ir duomenų nematomumo

(Kamleitner, Mitchell, 2018). Reglamentu siekiama sustiprinti duomenų subjektų teises ir sukurti pasitikėjimą bendrąja skaitmenine rinka (Dexe ir kt., 2020). Duomenų subjekto požiūriu, Reglamentas suteikia tvirtą apsaugą ir asmens duomenų tvarkymo skaidrumo garantijas (Cabral, 2021).

Duomenų subjekto teisės (angl. *Rights of data subject*) teisiniame reglamentavime numatytos specifinės teisės, įgalinančios duomenų subjektą kontroliuoti tai, kas vyksta su jo asmens duomenimis, o taip pat nustatančios tokios kontrolės įgyvendinimo ribas (Malinauskaitė-van de Castel, 2017).

Duomenų subjektas, kurio asmens duomenys tvarkomi, turi šias teises (žr. 4 pav.).



4 pav. Duomenų subjekto teisės

Šaltinis: sudaryta autoriaus pagal Reglamentą

1. ***Teisė būti informuotam***. Duomenų subjektas turi teisę būti informuotas apie jo duomenų tvarkymą, todėl duomenų valdytojas turi analogišką pareigą pateikti Reglamento 13 ir 14 straipsniuose nurodytą informaciją. ES 29 straipsnio darbo grupė (2018) teigia, kad duomenų valdytojas privalo imtis aktyvių veiksmų, kad duomenų subjektui pateiktų aptariamą informaciją arba aktyviai nukreiptų duomenų subjektą į vietą, kurioje ta informacija randasi.

2. ***Teisė susipažinti su savo duomenimis***. Reglamento 15 straipsnyje rašoma, kad duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis ir kita informacija, susijusia su asmens duomenų tvarkymu.

Duomenų valdytojas turėtų naudotis visomis pagrįstomis priemonėmis, kad patikrintų prašančio leisti susipažinti su duomenimis duomenų subjekto tapatybę (Urban ir kt., 2019). Užklausos teikėjo tapatybės patikrinimas yra svarbus šio proceso aspektas, nes būtina užkirsti kelią duomenų nutekėjimui neteisėtoms trečiosioms šalims. Reglamento duomenų užklausų tvarkymo politika ir praktika organizacijose labai skiriasi ir dažnai gali būti manipuliuojama, naudojant socialinės inžinerijos metodus, galimos to pasekmės yra neteisėta prieiga prie organizacijos asmens duomenų (Di Martino ir

kt., 2019). Kadangi socialinės inžinerijos keliami iššūkiai kompleksiniai ir dinamiški, jų žala tiesiogiai priklausoma nuo žmogaus pasirengimo tokios atakos atrėmimui (Šidlauskas ir Ungurytė-Ragauskienė, 2019).

3. ***Teisė reikalauti ištaisyti duomenis***. Reglamento 16 straipsnyje rašoma, kad duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištaisytų netikslius su juo susijusius asmens duomenis. Atsižvelgiant į tikslus, kuriais duomenys buvo tvarkomi, duomenų subjektas turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys, pateikdamas papildomą pareiškimą.

Duomenų tikslumą iš esmės reikėtų suprasti kaip duomenų ir faktinės, objektyvios tikrovės atitiktį. Duomenų tikslumas numato, kad naudojami duomenys turi būti aktualūs tikslui pasiekti, nes priešingu atveju duomenų valdytojas, žinodamas, kad duomenys pasenę ir juos toliau naudotų, tai reikštų duomenų tikslumo principo pažeidimą (Zaleskis, 2019). Rekomenduojama, kad duomenų vartotojai turėtų žinoti apie naudojamų duomenų ribotumą ir galimus apribojimus (Dimitrova, 2021).

4. ***Teisė reikalauti ištrinti duomenis („teisė būti pamirštam“)***. Reglamento 17 straipsnio 1 dalyje nustatytas bendras principas, kad duomenys ištrinami šiais šešiais atvejais:

- Asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi.
- Duomenų subjektas atšaukia sutikimą, kuriuo grindžiamas duomenų tvarkymas.
- Duomenų subjektas pasinaudojo savo teise nesutikti, kad jo asmens duomenys būtų tvarkomi teisėto intereso pagrindu arba tiesioginės rinkodaros tikslu.
- Asmens duomenys buvo tvarkomi neteisėtai.
- Duomenys ištrinti, laikantis teisinės prievolės.
- Asmens duomenys buvo surinkti teikiant informacinės visuomenės paslaugas nepilnamečiui.

Remiantis šiais aukščiau išvardintais pagrindais, JK informacijos komisaro biuro rekomendacijose (2021) rašoma, kad duomenų valdytojas, gavęs užklausą ar prašymą ištrinti asmens duomenis, turėtų juos ištrinti ne tik iš savo veikiančių sistemų, bet ir kitų sistemų, saugančių atsargines šių duomenų kopijas.

„*Teisė būti pamirštam*“ nėra absoliuti ir nesąlygoja atitinkamos informacijos pašalinimo iš originalių šaltinių, ji apsunkina šios informacijos prieinamumą bei sklaidą eliminuojant ją iš paieškos variklių pateikiamo rezultatų sąrašo. Kad duomenis būtų galima pašalinti, jie turi būti „*neadekvatūs, ne(be)reikšmingi arba pertekliniai*“. Tik konkrečiam atvejui būdingos aplinkybės (pvz., profesinis aplaidumas, neišnykęs teistumas, asmens padėtis viešajame gyvenime) gali lemti prioriteto suteikimą konkuruojančiam visuomenės interesui turėti prieigą prie šios informacijos asmens privatumo atžvilgiu (Tamavičiūtė, 2019). Duomenų valdytojai privalo, atsižvelgdami į turimas technologijas ir įgyvendinimo sąnaudas, imtis pagrįstų veiksmų, įskaitant technines priemones, kad informuotų kitus duomenis tvarkančius duomenų valdytojus, jog duomenų subjektas paprašė, kad tokie duomenų valdytojai ištrintų visas nuorodas į tuos asmens duomenis arba jų kopijas ar dublikatus.

5. ***Teisė apriboti duomenų tvarkymą***. Reglamento 18 straipsnyje 1 dalyje rašoma, kad duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas apribotų duomenų tvarkymą kai taikomas vienas iš šių atvejų:

- Asmens duomenų subjektas užginčija duomenų tikslumą tokiam laikotarpiui, per kurį duomenų valdytojas gali patikrinti asmens duomenų tikslumą.
- Asmens duomenų tvarkymas yra neteisėtas ir duomenų subjektas nesutinka, kad duomenys būtų ištrinti, ir vietoj to prašo apriboti jų naudojimą.
- Duomenų valdytojui nebereikia asmens duomenų nustatytais tvarkymo tikslais, tačiau jų reikia duomenų subjektui siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus.
- Duomenų subjektas paprieštaravo duomenų tvarkymui, kol bus patikrinta, ar duomenų valdytojo teisėtos priežastys yra viršesnės už duomenų subjekto priežastis.

6. ***Teisė į duomenų perkeliamumą***. Teisė į duomenų perkeliamumą yra numatyta Reglamento 20 straipsnyje. Tai galima vertinti kaip asmens prieigos teisės pagal Reglamento 15 straipsnį išplėtimą. Joje yra du pagrindiniai elementai: duomenų subjekto teisė gauti asmens duomenų kopiją iš duomenų valdytojo ir teisė tuos duomenis perduoti iš vieno duomenų valdytojo kitam. Šios tesės taikymo sritis yra labai apribota, nes duomenų valdytojas gali perduoti duomenis kitam duomenų valdytojui tik tuomet, kai toks perdavimas yra „techniškai įmanomas". Reglamentas nepateikia paaiškinimo, ką reiškia techniškai įmanoma, o tai gali suteikti didelę laisvę duomenų valdytojams, kurie gali nenorėti duomenų perduoti kitam duomenų valdytojui (Diker Vanberg, Ünver, 2017).

7. ***Teisė nesutikti su duomenų tvarkymu***. Duomenų subjektas turi teisę dėl su jo konkrečiu atveju susijusių priežasčių bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi, kai toks asmens duomenų tvarkymas vykdomas remiantis užduotimi, vykdoma viešojo intereso labui, organizacijai pavestomis viešosios valdžios funkcijomis arba teisėtais organizacijos arba trečiosios šalies interesais, įskaitant ir profiliavimą, atliekamą remiantis paminėtais pagrindais. Duomenų valdytojas nebetvarko asmens duomenų, išskyrus atvejus, kai duomenų valdytojas įrodo, kad duomenys tvarkomi dėl įtikinamų teisėtų priežasčių, kurios yra viršesnės už duomenų subjekto interesus, teises ir laisves, arba siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus.

8. ***Teisė reikalauti netaikyti vien automatizuoto atskirų sprendimų priėmimo, įskaitant profiliavimą***. Sprendimų priėmimas tik automatizuotu būdu reiškia, kad sprendimai bus priimami technologinėmis priemonėmis, tokiomis kaip algoritmai, be jokio žmogaus įsikišimo. Profiliavimas atliekamas tada, kai vertinami duomenų subjekto asmeniniai aspektai, kad būtų padarytos prognozės, net jeigu nebus priimtas joks sprendimas. Automatizuotas sprendimų priėmimas ir asmenų profiliavimas – įprasta praktika įvairiuose sektoriuose, kuriuose kaupiami didelės apimties asmens duomenys. Toks sprendimų priėmimas duomenų valdytojui yra naudingas, kadangi sudaro galimybes sumažinti žmogiškuosius ir materialinius išteklius, leidžia didinti veiklos efektyvumą (Novikovienė, Pedaniuk, 2020). Reglamento 22 straipsnyje rašoma, kad

duomenų subjektas turi teisę, kad jam nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam kyla teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį.

Toks reglamentavimas suteikia ES piliečiams galimybę geriau žinoti, kur naudojami jų duomenys, kaip jie naudojami, kas juos naudoja, kam jie naudojami, ir ES piliečiams teisėtai prieštarauti, taisyti ir labiau kontroliuoti (Woods, 2019). VDAI 2019 m. gautų skundų analizė rodo, kad duomenų subjektai aktyviai naudojasi savo teise į pažeistų teisių gynimą: apie 7 proc. visų VDAI gautų skundų sudaro asmenų skundai dėl teisių pažeidimų. Dažniausiai skundai teikiami dėl teisės susipažinti su savo duomenimis pažeidimo, taip pat dėl teisės būti pamirštam ir nesutikti su duomenų tvarkymu netinkamo įgyvendinimo.

Mokslininkai van Ooijen ir Vrabec (2019) daro išvadą, kad asmenys turi daugiau galimybių kontroliuoti savo duomenų apimtį ir srautą tais atvejais, kai duomenų tvarkymas yra teisėtas ir taikoma teisė juos ištrinti. Labai reikia kurti technologijas, kurios padėtų asmenims tvarkyti savo asmeninę informaciją, ir tuo pačiu reikia remti įmones, kad jos geriau valdytų atitiktį (Esteves ir Rodríguez-Doncel, 2021). Dauguma privatumo priemonių gali būti veiksmingos tik tuo atveju, jei vartotojai sugeba suprasti, kaip tvarkomi jų duomenys ir kaip saugomas jų privatumas. Pavyzdžiui, jei vartotojai nori prasmingai pasinaudoti savo teise prieštarauti, jie turi žinoti ir suprasti savo teises, mokėti susieti abstrakčią teisę su esama situacija ar paslauga, mokėti naudotis savo teise ir suprasti pasekmes (Feth, 2020).

Internete privatumo politika yra standartinė priemonė, siekiant skaidrumo. Organizacijos tekstu aprašo būdą, kaip jos renka, naudoja, tvarko ar atskleidžia vartotojo duomenis. Tačiau dabartinė privatumo politika nėra sukurta taip, kad būtų tinkama vartotojams pasiekti skaidrumą, ir neatitinka skaidrumo reikalavimų, kurių reikalauja Reglamentas. Obaro ir Oeldorfo-Hirscho apklausoje (2016) teigiama, kad 74% vartotojų visiškai praleido privatumo politiką. Likusių 26% vidutinė skaitymo trukmė buvo tik 73 sekundės, nors vidutinė privatumo politikos trukmė yra apie 2700 žodžių (Waldman, 2016). Privatumo politikos pateikimo trūkumai. Visų pirma, jų ilgis, sudėtinga kalba, didelis abstrakcijos lygis ir gana paslėptas padėties nustatymas lemia mažą priimtinumą (Feth, 2017). Taigi turime ieškoti naujų būdų, kaip modeliuoti ir pateikti privatumui svarbią informaciją vartotojams. Privatumo politika neišspręs jokių problemų tol, kol vartotojai jų neskaitys ar negalės jų suprasti (Sánchez, ir kt. 2021).

Apibendrinant pasakytina, duomenų subjektai turi Reglamente įtvirtintas specifines teises, įgalinančias juos kontroliuoti savo asmens duomenimis, kuriuos valdo ir tvarko organizacijos. Tačiau visų pirma norėdami jomis pasinaudoti, turėtų gebėti jas suprasti. Organizacijos siekdamos užtikrinti asmens duomenų subjektų teisių įgyvendinimą, visų pirma privalo skaidriai informuoti duomenų subjektus apie jų teises, visų antra sukurti mechanizmus ir procedūras joms įgyvendinti.

1.1.3. Duomenų apsaugos pareigūno organizacijoje ir duomenų apsaugos priežiūros institucijos vaidmenų analizė

Reglamente atsirado nauja pareigybė – duomenų apsaugos pareigūnas (toliau – Pareigūnas), jis yra nepriklausomas subjektas, užtikrinantis, kad organizacija laikytųsi Reglamento. Duomenų valdytojas yra atsakingas už saugumo priemones, skirtas duomenims apsaugoti ir yra įpareigotas užtikrinti duomenų tvarkymo operacijų kokybę. Duomenų valdytojas turi bendradarbiauti su Pareigūnu ir gali su juo konsultuotis bet kokiu su duomenų tvarkymu susijusiu klausimu (European Data Protection Supervisor, 2019). Duomenų valdytojas turi imtis tam tikrų organizacinių ir techninių saugumo priemonių, siekiant užtikrinti atitiktį Reglamentui (Šidlauskas, 2019).

Pareigūnas, atsižvelgdamas į Reglamentą, turi konkretų vaidmenį ir konkrečias pareigas, susijusias su duomenų apsauga ir asmens duomenų tvarkymu. Paskirtas Pareigūnas, kuris gali būti (esamas ar naujas) darbuotojas arba išorės konsultantas, turėtų turėti žinių apie duomenų apsaugą reglamentuojančius teisės aktus (Dibble, 2019). Zaleskis (2019) teigia, kad Pareigūno funkcijų patikėjimą išorės paslaugų teikėjams gali lemti duomenų valdytojo ir duomenų tvarkytojo patirties duomenų apsaugos teisės srityje trūkumas, siekis sutaupyti laiko, žmogiškųjų ir administracinių išteklių.

ES 29 straipsnio darbo grupė teigia, kad Pareigūnas yra atskaitomybės pagrindas ir kad paskyrus Pareigūną galima sudaryti palankesnes sąlygas laikytis reikalavimų, o, be to, verslo subjektams tai gali tapti konkurenciniu pranašumu. Pareigūnas ne tik padeda laikytis reikalavimų, įgyvendindamas atskaitomybės priemones, bet ir veikia kaip tarpininkas tarp įvairių suinteresuotųjų subjektų. Pareigūnas turi būti lankstus ir veikti kaip arbitras tarp įstatymų ir organizacijos veiksmų (Gobeo ir kt., 2018; Štareikė, Kausteklytė-Tunkevičienė, 2018). Pareigūno institutas turi veikti lyg duomenų valdytojo „saugiklis“, vykdyti galimų Reglamento nuostatų pažeidimų prevenciją, o kartu – padėti išvengti dėl galimų pažeidimų gresiančių didelių finansinių nuostolių (Januševičienė, 2018).

Duomenų valdytojas ir duomenų tvarkytojas, vadovaudamasis BDAR 37 straipsniu, privalo paskirti duomenų apsaugos pareigūną, kai:

1. Duomenis tvarko valdžios institucijos arba įstaigos.
2. Pagrindinė duomenų valdytojo arba duomenų tvarkytojo veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų duomenų subjektai yra reguliariai bei sistemingai stebimi dideliu mastu.
3. Pagrindinė duomenų valdytojo arba duomenų tvarkytojo veikla yra specialių kategorijų duomenų tvarkymas dideliu mastu arba asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu.

Reglamento 97 konstatuojamojoje dalyje numatyta, kad būtinas Pareigūnų ekspertinių žinių lygis turėtų būti nustatomas atsižvelgiant į atliekamas duomenų tvarkymo operacijas ir reikiamą tvarkomų asmens duomenų apsaugą. ES 29 straipsnio darbo grupė teigia, kad:

1. Pareigūnai privalo turėti nacionalinės ir Europos duomenų apsaugos teisės aktų bei praktikos žinių ir išsamiai suprasti Reglamentą; duomenų valdytojo vykdomas duomenų tvarkymo operacijas, informacines sistemas, duomenų apsaugos poreikius; organizacijos administracines taisykles ir procedūras.
2. Gebėjimas atlikti Pareigūnui skiriamas užduotis turėtų būti aiškinamas ir jo asmeninių savybių, ir žinių požiūriu, taip pat atsižvelgiant į jo statusą organizacijoje. Asmeninės savybės, pavyzdžiui, galėtų būti profesinis sąžiningumas ir aukšta profesinė etika. Pareigūnas atlieka itin svarbų vaidmenį, skatindamas organizacijoje duomenų apsaugos kultūrą, ir padeda įgyvendinti esminius Reglamento elementus.

Reglamento 37 straipsnio 5 dalyje numatyta, kad Pareigūnas paskiriamas remiantis profesinėmis savybėmis, visų pirma duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis, taip pat gebėjimu atlikti Reglamento 39 straipsnyje nurodytas užduotis. Pareigūnas informuoja duomenų valdytojo arba duomenų tvarkytojo ir duomenis tvarkančius darbuotojus apie jų prievoles pagal Reglamentą ir konsultuoja šiais klausimais: stebi, kaip laikomasi Reglamento, duomenų valdytojo (tvarkytojo) politikos asmens duomenų apsaugos srityje. Taip pat konsultuoja dėl poveikio duomenų apsaugai vertinimo ir stebi jo atlikimą. Pareigūnas bendradarbiauja su VDAI ir atlieka kontaktinio asmens funkciją VDAI kreipiantis su duomenų tvarkymu susijusiais klausimais. Taip pat Pareigūnas, vykdydamas šias užduotis, turėtų tinkamai įvertinti su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus.

Pareigūnas, nepriklausomai nuo to, ar jis yra duomenų valdytojo darbuotojas, savo pareigas ir užduotis turėtų galėti atlikti nepriklausomai, todėl svarbus jo statusas organizacijoje. Reglamento 38 straipsnyje nurodytos Pareigūno statuso nuostatos, ES 29 str. darbo grupė pateikė jų įgyvendinimo rekomendacijas (žr. 1 priedą).

ES 29 straipsnio darbo grupė teigia, kad niekas neužkerta kelio organizacijai, kuri teisiškai neprivalo paskirti Pareigūno ir nepageidauja jo paskirti savanoriškai, vis tiek įdarbinti darbuotojų arba samdyti išorės konsultantų, kuriems būtų pavestos su asmens duomenų apsauga susijusios užduotys. Šiuo atveju svarbu užtikrinti, kad nekiltų painiavos dėl jų pareigybės pavadinimo, statuso, pareigų ir užduočių. Taigi, visuose įmonės vidaus pranešimuose ir bendraujant su duomenų apsaugos institucijomis, duomenų subjektais ir plačiąja visuomene reikėtų aiškiai nurodyti, kad šis asmuo ar konsultantas nėra Pareigūnas.

Svarbu pabrėžti, kad Reglamento atitikties priežiūra organizacijoje nereiškia, kad Pareigūnas yra asmeniškai atsakingas už reguliavimo pažeidimus. Duomenų apsaugos atitiktis yra priskiriama duomenų valdytojo ar duomenų tvarkytojo, o ne Pareigūno atsakomybei. Ne visos organizacijos, tvarkančios asmens duomenis, privalo paskirti Pareigūną, tačiau visos privalo užtikrinti Reglamento atitiktį.

Daugelis organizacijų bando gauti daugiau naudos iš duomenų, kad patobulintų savo teikiamus produktus ir paslaugas, siūlytų naujus ir optimizuotų savo vidines operacijas (Hintze ir El Emam, 2018). Reglamento vykdymas padiktavo poreikį organizacijoms laikytis jo reikalavimų. Kadangi Priežiūros institucijos gali taikyti sankcijas,

kai tik nustatomas neatitikimas, organizacijos turi peržiūrėti savo procesus ir procedūras, kad užtikrintų atitiktį ir išvengtų sankcijų (Tikkinen-Piri ir kt., 2018; Teixeira ir kt., 2019). Įvykęs pokytis pakeitė duomenų apsaugos sistemą iš esmės – ne Priežiūros institucija aprobuoja asmens duomenų tvarkymo teisėtumą prieš pradedant asmens duomenų tvarkymo veiksmus, o pats duomenų valdytojas, įgyvendindamas atskaitomybės principą, įrodo įvairiomis Reglamente įtvirtintomis priemonėmis nepriklausomai Priežiūros institucijai, kad asmens duomenys tvarkomi teisėtai (Andrijauskas ir Morkūnienė, 2020).

Valdyba atsakinga už Reglamento taikymą. Ją sudaro visų Priežiūros institucijų vadovai ir Europos duomenų apsaugos priežiūros pareigūnas arba jų atstovai. Valdyba buvo sukurta siekiant spręsti prieštaringus ES narių sprendimus, teikti Priežiūros institucijoms nuomones ir gaires dėl konkrečių Reglamento nuostatų ir prižiūrėti, kad Reglamentas būtų nuosekliai taikomas ES. Valdyba taip pat priima privalomus sprendimus ginčuose dėl tarpvalstybinio tvarkymo, kad įvairiose srityse būtų nuosekliai taikomos procedūros. ES teismai taip pat turi jurisdikciją Reglamento vykdymo srityje, taip užtikrindami vienodą taisyklių taikymą, kad tas pats ginčas nebūtų skirtingai nagrinėjamas įvairiose jurisdikcijose (Europos komisija, 2020). Pagrindiniai Valdybos tikslai – užtikrinti nuoseklų duomenų apsaugos ir privatumo teisės aktų taikymą visoje ES. Tai pasiekiama išleidžiant gaires nacionalinėms Priežiūros institucijoms ir palengvinant veiksmingą valstybių narių Priežiūros institucijų bendradarbiavimą. (Gobeo, 2018). Pagal Reglamentą trys teisminės institucijos – nacionaliniai teismai, Europos Žmogaus Teisių Teismas ir Europos Teisingumo Teismas – turi jurisdikciją nagrinėti ginčus, kylančius tarp Priežiūros institucijos ir paveikto subjekto ir gali apibrėžti neaiškias Reglamento nuostatas (Europos komisija, 2019).

Reglamento 51 straipsnio 1 dalyje rašoma, kad kiekviena valstybė narė užtikrina, kad viena arba kelios nepriklausomos valdžios institucijos yra atsakingos už šio Reglamento taikymo stebėseną, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės tvarkant duomenis ir sudarytos palankesnės sąlygos laisvam asmens duomenų judėjimui Sąjungoje (toliau – Priežiūros institucija). VDAI sprendžia atvejus, kai asmens duomenis profesiniais ar komerciniais tikslais tvarko įvairios įmonės, valstybinės institucijos ir kitos organizacijos: bankas, savivaldybė, e. parduotuvė, mokykla, ligoninė, policija, advokatas, notaras, nevyriausybinė organizacija bei fiziniai asmenys ir kt. Priežiūros institucijos, pavieniui arba kartu, pateikia autoritetingas gaires dėl Reglamento sąvokų ir nuostatų (Jasmontaitė-Zaniewicz ir kt., 2021). Mulder ir Tudorica (2019) nuomone, aktyvus Priežiūros institucijų vaidmuo galėtų paskatinti įmones būti atviresnes ir konkretesnes dėl duomenų tvarkymo tikslų. Priežiūros institucijos nepriklausomumas yra svarbiausias dalykas, todėl institucijos nariams neleidžiama imtis jokios veiklos, kuri nesuderinama su jų, kaip institucijos nario, pareigomis. Valstybės narės taip pat turi suteikti Priežiūros institucijoms pakankamai žmogiškųjų, finansinių ir techninių išteklių, reikalingų jų užduotims atlikti (Reuter, 2018).

Vieni iš svarbiausių Lietuvos Respublikos Vyriausybės poįstatyminių teisės aktų, reikšmingų asmens duomenų apsaugos teisei Lietuvoje, yra 1996 metų Lietuvos Respublikos Vyriausybės nutarimas, kuriuo įsteigta VDAI, bei 2001 m. nutarimas, kuriuo

patvirtinti šios įstaigos nuostatai. Po šio nutarimo priėmimo VDAI tapo pagrindine, už asmens duomenų apsaugą atsakinga, institucija Lietuvoje, kurios tikslas – plėtoti duomenų apsaugą, prižiūrėti asmens duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoti asmens duomenų tvarkymo teisėtumą, kovoti su duomenų tvarkymo pažeidimais ir užtikrinti duomenų subjekto teisių apsaugą (Lukoševičienė, 2021). VDAI 2019 metų veiklos ataskaitoje teigiama, VDAI paskirtis – prižiūrėti, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės tvarkant asmens duomenis bei sudarytos palankesnės sąlygos laisvam asmens duomenų judėjimui ES. VDAI pagrindiniai veiklos tikslai:

1. Dalyvauti formuojant valstybės politiką asmens duomenų apsaugos srityje.
2. Vykdyti Reglamento ir kitų asmens duomenų apsaugos teisės aktų stebėseną ir užtikrinti jų vykdymą.
3. Kontroliuoti asmens duomenų tvarkymą.
4. Įgyvendinti 1981 metų sausio 28 dieną Strasbūre sudarytos Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) ir jos protokolų nuostatas.

Lietuva išsiskiria iš bendro Europos Sąjungos valstybių narių konteksto, nes turi dvi duomenų tvarkymo priežiūros institucijas – VDAI ir žurnalistų etikos inspektoriaus tarnybą. Žurnalistų etikos inspektoriaus tarnyba stebi, kaip taikomas Reglamentas ir ADTAĮ, ir užtikrina, kad šie teisės aktai būtų taikomi, kai asmens duomenys tvarkomi žurnalistikos tikslais ir akademinės, meninės ar literatūrinės saviraiškos tikslais (Žurnalistų etikos inspektorius, 2018).

Reglamente tvirtinama, kad pagrindinė Priežiūros institucijų atsakomybė yra jos taikymo stebėjimas ir nuoseklumas, siekiant apsaugoti pagrindines fizinių asmenų teises ir laisves, susijusias su duomenų tvarkymu, ir palengvinti laisvą asmens duomenų judėjimą ES. Puiszis (2018) remdamasis Reglamento 57 straipsniu, rašo kad kiekviena Priežiūros institucija laikoma kompetentinga atlikti pagal Reglamentą reikalaujamas šias užduotis: Reglamento stebėjimas ir taikymo užtikrinimas; Visuomenės informuotumo, apie su duomenų tvarkymu susijusius pavojus, taisykles, apsaugos priemones ir teises bei jų supratimą, skatinimas; Konsultavimas nacionalinio parlamento, vyriausybės ir kitų institucijų bei įstaigų teisėkūros ir administracinių priemonių, susijusių su fizinių asmenų teisių ir laisvių apsauga tvarkant duomenis, klausimais; Duomenų valdytojų ir duomenų tvarkytojų informuotumo apie jų prievoles pagal Reglamentą skatinimas; Bendradarbiavimas su kitomis Priežiūros institucijomis, be kita ko, dalijimasis informacija; Duomenų subjektų ar jų atstovų skundų nagrinėjimas; Poveikio duomenų apsaugai vertinimo reikalavimų nustatymas; Standartinių sutarties sąlygų priėmimas ir privalomų įmonių taisyklių tvirtinimas; Sertifikavimo įstaigų akreditacijos vykdymas; Tvarkymas vidaus įrašų apie Reglamento pažeidimus ir priemones.

Priežiūros institucijoms taip pat suteikiami įgaliojimai: Atlikti duomenų apsaugos auditus; Įpareigoti duomenų valdytojus, duomenų tvarkytojus ir, kai taikoma, jų atstovus suteikti informaciją ir prieigą prie asmens duomenų arba patekti į patalpas, kai tai būtina užduotims atlikti; Įspėti apie galimus pažeidimus, pareikšti papeikimus už duomenų tvarkymo pažeidimus; Nurodyti suderinti duomenų tvarkymo operacijas su

Reglamentu; Įpareigoti duomenų valdytoją pranešti apie pažeidimą duomenų subjektams; Nustatyti apribojimus, įskaitant visišką duomenų tvarkymo draudimą; Už pažeidimus skirti administracines baudas; Įsakyti sustabdyti duomenų srautus už ES ribų.

Pagal Reglamento 31 straipsnį, tiek duomenų valdytojas, tiek duomenų tvarkytojas, taip pat jų atstovai, gavę prašymą bendradarbiauja su Priežiūros institucija, vykdančia savo užduotis.

Asmens duomenų apsauga Lietuvoje yra reglamentuota įvairios formos, turinio ir apimties, nevienodos teisinės galios, privalomojo ir rekomendacinio pobūdžio, tarpusavyje susijusių teisės normų, kurios yra nuolat keičiamos ir plečiamos, atsižvelgiant į visuomeninio gyvenimo pokyčius, sistema (Lukoševičienė, 2021).

Priežiūros institucijos nagrinėja visus skundus, kuriuos gauna iš asmenų, kurie mano, kad asmens duomenys apie juos yra tvarkomi ne pagal įstatymus, nebent Priežiūros institucija mano, kad tokie skundai yra nepagrįsti arba neproporcingi. Priežiūros institucija raštu praneša skundo pareiškėjui apie savo sprendimą dėl skundo. Taip pat Priežiūros institucija gali pradėti tyrimą savo iniciatyva, jeigu mano, kad gali būti pažeistos duomenų apsaugos teisės, arba mano, kad tikslinga užtikrinti duomenų apsaugos teisės aktų laikymąsi (Lambert, 2017).

Projekto „*SolPriPa*“ parengtose asmens duomenų apsaugos gairėse smulkiajam ir vidutiniam verslui rašoma, kad duomenų saugumas yra pažeidžiamas, kai įvyksta su duomenimis, už kuriuos įmonė yra atsakinga, susijęs saugumo incidentas, dėl kurio pažeidžiamas duomenų konfidencialumas, prieinamumas ar vientisumas. Galimi asmens duomenų saugumo pažeidimo (toliau – Pažeidimo) tipai:

1. Konfidencialumo pažeidimas – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų.
2. Prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba sunaikinami asmens duomenys.
3. Vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo ar netyčia. Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

Pažeidimai gali būti atsitiktiniai arba tyčiniai. Kiekviena organizacija turi turėti planą, kaip reaguoti į pastebėtus pažeidimus. Visi pažeidimai turėtų būti tinkamai užregistruoti, ištirti ir prireikus imtasi taisomųjų veiksmų. Ne apie kiekvieną duomenų pažeidimą reikia pranešti Priežiūros institucijai, organizacijos turi pareigą pranešti apie asmens duomenų pažeidimus Priežiūros institucijai per 72 valandas nuo sužinojimo apie pažeidimą. Jos taip pat privalo nepagrįstai nedelsdami informuoti atitinkamus asmenis, jei tikėtina, kad bus didelė rizika, kad pažeidimas turės neigiamos įtakos jų teisėms ir laisvėms. Priežiūros institucija gali reikalauti, kad įmonė imtųsi taisomųjų veiksmų arba skirti administracinę baudą ar sankcijas už reikalavimų nesilaikymą (Alford, 2020). VDAI 2022 m. I pusmečio pranešimų apie asmens duomenų saugumo pažeidimus apžvalgoje nurodo organizacinės ir techninės saugumo priemonės, padėsiančios išvengti Pažeidimų:

- Reguliariai daryti atsargines kopijas (angl. *Backup*).

- Užtikrinti kritinių operacinių sistemos saugos atnaujinimų diegimą reguliariai ir nedelsiant.
- Sukonfigūruoti išorinėje komunikacijoje dalyvaujančius serverius ir kitą įrangą pagal gerąsias praktikas.
- Apriboti išorinio prisijungimo galimybes tokiais protokolais kaip *Windows Remote Desktop Protocol*, daiktų interneto *SSH* prievadais ir pan.
- Prie maršrutizatorių leisti jungtis tik iš žinomų IP adresų (angl. *Allow list*) arba prisijungimui naudoti virtualaus privataus tinklo technologijas (angl. *Virtual private network, VPN*).
- Įdiegti pažangią antivirusinę programinę įrangą.
- Nenaudoti tų pačių slaptažodžių skirtingoms paskyroms, naudoti kelių faktorių autentifikavimą.
- Įdiegti el. pašto filtravimo mechanizmus, gebančius filtruoti laiškus pagal žinomus grėsmių indikatorius ir specifinius raktažodžius.
- Parengti ir reguliariai testuoti veiklos tęstinumo planą.
- Įdiegti prieigos kontrolę pagal organizacijos saugumo politiką, taikant principą „*būtina žinoti*".
- Reguliariai mokyti darbuotojus apie IT sistemų saugumo reikalavimus.

Vienas iš pagrindinių Reglamento pakeitimų yra tas, kad Priežiūros institucijos turi žymiai padidintus įgaliojimus skirti dideles baudas ir kitas sankcijas organizacijoms, kurios nesilaiko Reglamento (Dibble, 2019). VDAI sankcijų skyrimo klausimais laikosi teisės aktų reikalavimų. Kiekvienas atvejis vertinamas atskirai, taikant sankcijas atsižvelgiama ir į galimus neaiškumus dėl tam tikrų Reglamento nuostatų. VDAI pataria, nurodo ištaisyti Reglamento reikalavimų neatitikimus. Kai kuriais atvejais sprendimai priimami netgi ES lygiu Valdyboje, formuojama bendra europinė baudų skyrimo praktika. Baudos sumokėjimas niekaip neapsaugo duomenų tvarkytojo ar duomenų valdytojo nuo pareigos atlyginti asmeniui patirtą turtinę ir neturtinę žalą.

Be anksčiau paminėtų institucijų, įvairius atvejus, susijusius su asmens duomenų tvarkymu ir privatumu, Lietuvoje taip pat sprendžia NKSC, policija ir teismai.

VDAI taip pat yra viena iš institucijų, įgyvendinančių kibernetinio saugumo politiką. Ji prisidėjo prie kibernetinio saugumo sistemos Lietuvoje kūrimo priimant Kibernetinio saugumo įstatymą, toliau prisideda prie jos tobulinimo ir užtikrinimo dalyvaudama Kibernetinio saugumo tarybos veikloje, kartu su kitomis atsakingomis institucijomis rengia Lietuvos kibernetinio saugumo ataskaitą. Kibernetinis saugumas tiesiogiai susijęs su Inspekcijos atliekama asmens duomenų saugumo pažeidimų nagrinėjimo veikla, kai tiriant asmens duomenų saugumo pažeidimus prireikus bendradarbiaujama ir su Nacionaliniu kibernetinio saugumo centru (VDAI, 2022).

Apibendrinant galima teigti, kad organizacijos atitiktis Reglamento reikalavimams yra priskiriama duomenų valdytojo ar duomenų tvarkytojo, o ne Pareigūno atsakomybei. Ne visos organizacijos, tvarkančios asmens duomenis, privalo paskirti Pareigūną, tačiau visos privalo užtikrinti Reglamento atitiktį. Pareigūnas užtikrina, kad organizacijoje būtų tinkamai įgyvendinami BDAR reikalavimai, todėl labai svarbu, kad duomenų valdytojas bendradarbiautų su Pareigūnu – kuo ankstyvesniu etapu įtrauktų

į visus su duomenų apsauga susijusius klausimus ir suteiktų reikiamus išteklius – pakankamą laiką užduotims atlikti ir mokytis, darbuotojus, kurie, esant poreikiui, vykdytų jo nurodytas užduotis. Priežiūros institucijos yra nepriklausomi viešieji subjektai, teikiantys konsultacijas duomenų apsaugos klausimais ir nagrinėjantys skundus dėl pažeidimų. Priežiūros institucija patvirtina asmens duomenų tvarkymo teisėtumą organizacijoje prieš jai pradedant asmens duomenų tvarkymo veiksmus, o organizacija, įgyvendindama atskaitomybės principą, įrodo Priežiūros institucijai, kad asmens duomenys tvarkomi teisėtai pagal Reglamento reikalavimus. Priežiūros institucijos turi įgaliojimus skirti dideles baudas ir kitas sankcijas organizacijoms, kurios nesilaiko Reglamento. Baudos sumokėjimas niekaip neapsaugo organizacijos nuo pareigos atlyginti asmeniui patirtą turtinę ir neturtinę žalą. Organizacijos siekdamas užtikrinti Reglamento reikalavimus ir sumažinti Pažeidimo riziką, turėtų asmens duomenis tvarkyti teisėtai, skaidriai ir sąžiningai konkrečiam tikslui pasiekti bei įdiegti tinkamas technines ir organizacines apsaugos priemones. Kiekviena organizacija turi turėti planą, kaip reaguoti įvykus Pažeidimui – tinkamai užregistruoti, ištirti ir prireikus imtasi taisomųjų veiksmų.

1.2. Kibernetinio saugumo, kaip reiškinio, teorinis pagrindimas

1.2.1. Kibernetinio saugumo samprata, turinys ir principai

Naudojant terminą „*kibernetinė erdvė*“ trūksta sutarimo (Kademi ir Koltuksuz, 2017). Kompiuteriai ir tinklo įrenginiai yra svarbūs apibrėžiant kibernetinę erdvę; rečiau yra būtina įtraukti ir žmones. Žmogus netiesiogiai yra neatsiejamas nuo kibernetinės erdvės ir yra aktyvi jos dalis. Internetinė erdvė dažnai konceptualizuojama kaip trys tarpusavyje sujungtų tinklų sluoksniai – socialinis, informacinis ir fizinis (Bayne, 2008). Žmogaus pažinimo svarbą kibernetinei ir žmogaus sąveikai taip pat pabrėžia Jinhua ir kt. (2013), kurie kibernetinę erdvę apibūdina kaip tradicinei erdvei lygiagrečią erdvę, į kurią projektuojame fizinių ir socialinių elementų simuliacijas (Zhuge, 2018). Tai yra naudinga sąvoka, nes ji pripažįsta žmones, kaip šios projekcijos kūrėjus ir pateikia juos, kaip būtinas sąlygas kibernetinei erdvei. Tai yra netiesioginis žmogaus elementas kibernetinėje erdvėje ir tai būdinga tokioms sritims, kaip kibernetinis saugumas, kur į žmones orientuoti tyrimai atsiliko nuo technologinių aspektų (Asquith ir Morgan, 2020).

Terminas „*kibernetinio saugumas*“ vartojamas vis dažniau. Susidomėjimą kibernetiniu saugumu skatina pripažinimas, kad kibernetinių technologijų plėtrą varžo mokslinių kibernetinių reiškinių, ypač pagrindinių dėsnių, teorijų ir teoriškai pagrįstų bei empiriškai patvirtintų modelių, supratimo stoka (Kott, 2014). Kibernetinis pasaulis yra be galo besiplečianti erdvė, siūlanti didžiules skaitmeninės transformacijos galimybes dėl esamo didelio kibernetinio potencialo ir tarpusavio ryšio. Šioje erdvėje žaliava ir skaitmeninės transformacijos pagrindas yra duomenys. Skaitmeninė transformacija reiškia kibernetinio pasaulio skaitmeninių technologijų integravimą į visas fizines sritis

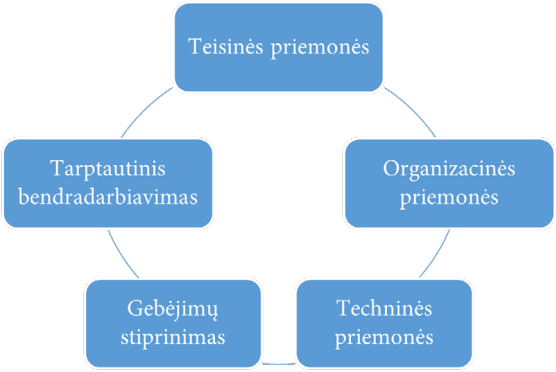
(Möller, 2020). Kibernetinis saugumas reiškia tinklų ir informacinių sistemų apsaugą nuo žmogaus klaidų, stichinių nelaimių, techninių gedimų ar kenkėjiškų išpuolių (Europos Komisija, 2016). KSĮ sąvokose kibernetinis saugumas yra apibūdinamas, kaip visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę RIS perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, RIS netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę RIS veiklą. Möller ir Haas (2019) teigia, kad kibernetinis saugumas yra žinių apie technologijas, procesus ir praktiką, siekiant apsaugoti kompiuterius, duomenų šaltinius, tinklus ir programas nuo kibernetinių grėsmių atakų, sugadinimo ar neteisėtos prieigos, visuma. Kibernetinis saugumas – tai priemonių, politikos, saugumo koncepcijų, saugumo užtikrinimo priemonių, gairių, rizikos valdymo metodų, veiksmų, mokymų, geriausios praktikos pavyzdžių, užtikrinimo ir technologijų rinkinys, naudojami kibernetinėje erdvėje ir organizacijos bei vartotojo turtui apsaugoti. Organizacijos ir vartotojo turtas apima prijungtus skaičiavimo įrenginius, personalą, infrastruktūrą, programas, paslaugas, telekomunikacijų sistemas ir visą perduodamą ir (arba) saugomą informaciją kibernetinėje erdvėje (Telekomunikacijų sąjunga, 2014). Kibernetinio saugumo tikslas yra apsisaugoti nuo rizikos, kylančios dėl to, kad organizacija yra vienaip ar kitaip prijungta prie interneto (von Solms ir von Solms, 2018).

Anot Sharma (2019) kibernetinis saugumas Reglamente plačiau aptariamas kaip „*tvarkymo saugumas*“ ir viena iš pagrindinių Pareigūno pareigų. Kibernetinis saugumas Reglamente apibrėžiamas, kaip techninės ir organizacinės priemonės, kurias įgyvendina duomenų valdytojas, siekdamas kovoti su bet kokia rizika, kylančia tvarkant asmens duomenis. Reglamentas įpareigoja užtikrinti kibernetinį saugumą atliekant bet kokią apdorojimo operaciją, kuriai taikomas Reglamentas. Yra keletas būdų, kaip praktiškai spręsti kibernetinio saugumo klausimus:

1. Kibernetinio saugumo priemonių įgyvendinimas ir duomenų valdytojo / duomenų tvarkytojo atsakomybė už jų vientisumą.
2. Pareigūno paskyrimas ir išteklių jam suteikimas.
3. Trečiosios šalies rangovo pasamdymas atlikti Pareigūno funkcijas.
4. Pareigūno reguliarus kibernetinio sąmoningumo ugdymo mokymų organizavimas.

Visų pirma, skaitmenizuotoje visuomenėje kibernetinis saugumas (IT saugumas ar duomenų saugumas) siaurąja prasme tapo pagrindine asmens duomenų apsaugos prielaida (Schünemann ir Baumann, 2017). Pavyzdžiui, Reglamente, reikalaujama, kad duomenų valdytojai ir tvarkytojai įgyvendintų tinkamas technines ir organizacines priemones, kad užtikrintų rizikai tinkamą saugumo lygį.

Pasaulinis kibernetinio saugumo indeksas yra iniciatyva, kuria bandoma įvertinti šalių įsipareigojimą kibernetiniam saugumui (Telekomunikacijų sąjunga, 2015). Pasaulinis kibernetinio saugumo indeksas pateikia šalių kibernetinio saugumo raidos lygio apžvalgą, įskaitant penkias sritis (žr. 5 pav.).



5 pav. Kibernetinio saugumo sritys
Šaltinis: Telekomunikacijų sąjunga, 2015

Teisinės priemonės suteikia suderintą subjektų sistemą, kad jie atitiktų bendruosius reguliavimo reikalavimus ir sumažintų kibernetines grėsmes. Technologijos yra pagrindinė apsauga nuo kibernetinių ir kitų internetinių grėsmių. Techninėmis priemonėmis ir funkcijomis galima aptikti kibernetines atakas ir su jomis kovoti, siekiant sumažinti pažeidžiamumą. Kuriami rodikliai, kuriais siekiama įgyvendinti tarptautiniu mastu pripažintus kibernetinio saugumo standartus viešajame sektoriuje ir ypatingos svarbos infrastruktūroje. Organizacinės priemonės yra esminės organizacinių ir bendradarbiavimo strategijų kūrimui. Šios priemonės yra naudojamos kiekvienai nacionalinei kibernetinio saugumo iniciatyvai įgyvendinti. Be to, gebėjimų stiprinimas, susijęs su žmonių gebėjimų ugdymu priimant teisines, technines ir organizacines kibernetinio saugumo priemones. Darbo jėgai būtinos technologijų žinios. Žmogiškųjų ir institucinių gebėjimų stiprinimas yra naudingas gerinant žinias įvairiuose sektoriuose, taikant tinkamiausius sprendimus ir skatinant specialistų kompetencijos pažangą. Kibernetinis saugumas apima daugelio suinteresuotųjų šalių požiūrį. Galiausiai, norint užtikrinti geresnį dialogą ir koordinavimą, būtina sąlyga yra bendradarbiavimas. Dalijimasis informacija yra naudingas viešajame ir privačiajame sektoriuose, taip pat nacionaliniu ir tarptautiniu lygiu (Athanassouli, 2019).

Demokratinės visuomenės principai leidžia suskaidytą reguliavimą kurti pagal atskiras iniciatyvas, kurias teisėtai kelia interesų grupės, tačiau norint, kad visas reguliavimo procesas būtų nuoseklus, būtina planuoti ir nustatyti reguliavimo gaires; planavimo ir prognozavimo procesą nustato strategija. Patartina nustatyti tik specialius kibernetinio saugumo strategijos principus arba principus, kurie kibernetinio saugumo kontekste tampa svarbesni nei kitose žmogaus veiklos srityse. Tačiau labai svarbu, kad į strategiją įtraukti bendrieji ar specialieji principai iš tikrųjų būtų pagrindiniai, siekiant kibernetinio saugumo; tada, nustatę tokius principus viename dokumente, turime nuoseklią principų sistemą (Štitilis ir kt., 2016).

NATO kibernetinės gynybos pastangos grindžiamos svarbiausiais prevencijos (angl. *Prevention*) ir atsparumo (angl. *Resilence*) bei nekartojimo (angl. *Non-dublication*)

principais. Prevencija ir atsparumas yra ypač svarbūs, atsižvelgiant į realybę, kad tam tikros grėsmės išliks, nepaisant visų pastangų jas apsaugoti ir gintis. Norint užkirsti kelią tokiems išpuoliams pirmiausia reikia didinti pasirengimo lygį ir mažinti riziką, ribojant sutrikimus ir jų pasekmes. Atsparumas yra pagrindinis dalykas, nes jis palengvina greitą atsigavimą po atakos. Pripažindama visuotinį kibernetinės erdvės pobūdį ir su ja susijusias grėsmes, NATO ir sąjungininkai veikia su partneriais, tarptautinėmis organizacijomis, akademine visuomene ir privačiu sektoriumi taip, kad būtų skatinamas bendradarbiavimas ir išvengta dubliavimosi. Anot Horák ir kt. (2019), bendradarbiavimas ir keitimasis informacija bei žiniomis yra gyvybiškai svarbūs užtikrinant kibernetinį saugumą. Kibernetinio saugumo bendruomenės dalijasi grėsmių žvalgyba, pažeidžiamumo ataskaitomis ir teismo ekspertizės duomenimis, taip pat reagavimo į įvykius gairėmis, ataskaitomis ir geriausia praktika. Dalijimasis tokia informacija leidžia geriau suprasti situaciją.

KSĮ 3 straipsnyje nurodyta, kad kibernetinis saugumas grindžiamas šiais kibernetinio saugumo principais:

1. Kibernetinės erdvės nediskriminavimo – teisės aktų nuostatos yra taikomos, o gėriai yra saugomi vienodai tiek fizinėje, tiek kibernetinėje erdvėje.
2. Kibernetinio saugumo rizikos valdymo – taikomos kibernetinio saugumo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą.
3. Kibernetinio saugumo proporcingumo – taikomos teisinės, organizacinės ir techninės kibernetinio saugumo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai būtina.
4. Viešojo intereso viršenybės – taikomos kibernetinio saugumo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje.
5. Standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais RIS kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės.
6. Subsidiarumo – už RIS ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai. Srityse, kurios priklauso išimtinei kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos veiksmų imasi tik tada, kai RIS ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai.

Stallings (2018) teigia, kad daugybė organizacijų, remdamosi plačiu profesiniu indėliu, sukūrė kibernetinio saugumo užtikrinimo geriausios praktikos dokumentų tipus, taip pat jų įgyvendinimo ir vertinimo standartus. Žymiausi kibernetinio saugumo standartų kūrėjai:

- Nacionalinis standartų ir technologijų institutas (NIST). NIST sukūrė daugybę saugumo leidinių, įskaitant 9 federalinius informacijos apdorojimo standartus (FIPS) ir gerokai daugiau nei 100 aktyvių specialiųjų leidinių (SP), kuriuose pateikiamos rekomendacijos praktiškai visais kibernetinio saugumo aspektais.
- Tarptautinės standartizacijos organizacijos (ISO) 27000 standartų serija dėl informacijos saugumo valdymo sistemų.
- Organizacija, parengusi kibernetinio saugumo standartus ir gaires, ISACA / COBIT: Informacijos saugumui ir susijusiems dokumentams skirtas COBIT-5, kuris yra plačiai naudojamas pramonėje.
- Tarptautinė telekomunikacijų sąjungos telekomunikacijų standartizavimo sektorius (ITU-T): Svarbiausios yra saugos valdymo serijos X.1050 – X.1069.
- Informacijos saugumo forumas (ISF) parengė informacijos saugumo gerosios praktikos standartą (SGP). Šiame beveik 300 puslapių dokumente pateikiama daugybė geriausios praktikos pavyzdžių, pagrįstų pramonės ir vyriausybės organizacijų sutarimu.

Kitos gerbiamos organizacijos taip pat pateikė nemažai panašių dokumentų. Taigi yra labai daug praktiškos, plačiai priimtos medžiagos. Problema ta, kad informacijos kiekis yra toks didelis, kad kibernetinio saugumo specialistams sunku ja pasinaudoti kuriant ir palaikant veiksmingas kibernetinio saugumo sistemas ir politiką. Anot Schreider (2020), kad būtų laikomasi kibernetinį saugumą reglamentuojančių teisės aktų, reikalinga pagrindinė kontrolė ar atsakomosios priemonės, skirtos spręsti konkrečias problemas, siekiant atitikties teisės aktams. Tinkamo standarto pasirinkimas ir jo laikymasis yra saugumo garantas, kad organizacija atitinka tam tikrus numatytus reikalavimus.

Kai globalaus verslo aplinkoje vis labiau remiamasi duomenimis, iškyla kibernetinio saugumo problemų, susijusių su konfidencialumu, vientisumu ir prieinamumu (Tziogas ir Tsolakis, 2019). Informacijos saugumas yra apibrėžiamas kaip saugoma informacija ir informacinės sistemos nuo neteisėtos prieigos, naudojimo, atskleidimo, sutrikimų, modifikavimo ar sunaikinimo (Andress, 2011). Todėl trys pagrindiniai informacijos saugumo principai yra konfidencialumas, vientisumas ir prieinamumas, kurie paprastai vadinami CIA triada – modelis, kuriuo vadovaujamasi, vykdant viešųjų ar privačių organizacijų saugumo politiką (Hasib, 2014). Informacijos saugumas yra nenutrūkstamas sistemos procesas, kurio tikslas – išlaikyti sistemos saugomų ar perduotų duomenų: prieinamumą, konfidencialumą ir vientisumą. Naudodami saugumo mechanizmus, sistemos kūrėjai nukreipia tris pagrindinius saugumo komponentus:

- *Vientisumas*. Užtikrinama, kad informacija būtų apsaugota nuo pašalinių vartotojų modifikavimo.
- *Konfidencialumas*. Sistemos išteklių, informacijos ir proceso slėpimas nuo neteisėtos prieigos. Jis daugiausia susijęs su prieigos kontrolės mechanizmais, kurie priklauso nuo politikos, leidžiančios arba neleidžiančios sistemos prieigos užklausų.
- *Prieinamumas*. Jis reikalingas, kad sistema būtų prieinama įgaliotiems vartotojams. Programinės įrangos kūrimo srityje saugumo mechanizmai

standartizuojami įvairiomis formomis, tokiomis kaip sertifikavimas, šifravimo stiprumas, autentifikavimas ir kt. (Almousa ir kt., 2020).

CIA triados modelis laikomas saugumo koncepcijos ištaka saugumo politikos ir saugumo modelių srityje, kuris taikomas standarte ISO 27001, kuriant informacijos saugos valdymo sistemą. Informacija yra nematerialiai vertybė, ją gali sudaryti duomenys, informacija ir žinios, turintys vertę informacijos valdytojui. Tačiau ši nematerialiai vertybė turi materialų pagrindą, tai – informacijos saugojimo laikmenos, ryšio linijos, kuriomis informacija perduodama, taip pat informacinės sistemos, kuriose ta informacija yra apdorojama (Grigaitytė ir Mackevičiūtė, 2020). Daugelis paslaugų teikėjų organizacijų taip pat mano, kad ISO 27001 sertifikatas padeda įgyti konkurencinį pranašumą ir suteikia joms verslo vertės. Dėl to daugelis organizacijų (paslaugų teikėjų) įdiegė ISO 27001 praktiką ir sukūrė informacijos saugos valdymo sistemą (ISVS), sukurtą pagal ISO 27001 sistemą, o vėliau gavo ISO 27001 sertifikatą, kurį suteikė nepriklausomos sertifikavimo institucijos. Manoma, kad „*atitikties priežastys*“ yra svarbiausias ISO 27001 diegimo veiksnys, po to seka „*verslo vertė*“, o po to seka „*konkurencinis pranašumas*“, o po to seka „pažeidimų mažinimas“ (Makhija, 2021).

Štitilis ir kt. (2016) teigia, kad istoriškai elektroninės informacijos sauga buvo paremta tam tikrais svarbiausiais principais, kurių aktualumas išlieka iki šiol:

1. *Suvokimo principas*. Siekiant užtikrinti elektroninės informacijos saugą, reikia suvokti apsisaugojimo priemonių nuo galimos grėsmės elektroninei informacijai naudojimo būtinybę.
2. *Atsakomybės principas*. Kiekvienas elektroninės informacijos naudotojas turi suvokti savo atsakomybę ir funkcijas saugant elektroninę informaciją. Elektroninės informacijos saugą informacinėse sistemose turi užtikrinti valstybės institucijos vadovas, o ją įgyvendinti privalo saugos įgaliotiniai.
3. *Reagavimo principas*. Elektroninei informacijai kyla įvairi grėsmė, todėl būtina laiku aptikti saugos incidentus ir užkirsti kelią, be to valstybės institucijos viduje nuolat keistis informacija apie elektroninei informacijai kylančią grėsmę ir kovos su ja priemones.
4. *Demokratiškumo principas*. Elektroninės informacijos sauga turi būti įgyvendinama ir derėti su esminėmis demokratiškos visuomenės vertybėmis.
5. *Rizikos įvertinimo principas*. Siekiant nustatyti esamą elektroninės informacijos saugos lygį ir parinkti būtinas elektroninės informacijos saugos priemones, būtina periodiškai įvertinti elektroninės informacijos saugos pavojus informacinėse sistemose.
6. *Elektroninės informacijos saugos kultūros ugdymo principas*. Siekiant užtikrinti elektroninės informacijos saugą, būtina ypač dėmesingai mokyti nuolatinius elektroninės informacijos naudotojus elektroninės informacijos saugos ir taip ugdyti elektroninės informacijos saugos kultūrą.
7. *Elektroninės informacijos saugos priemonių projektavimo ir diegimo principas*. Elektroninės informacijos sauga turi būti kuriama kartu su informacine sistema. Elektroninės informacijos sauga turi būti pamatinis visų informacinės

sistemos paslaugų elementas, kuriam būtina užtikrinti nuolatinį lėšų, neviršijančių pačios elektroninės informacijos vertės, skyrimą.

Ilgą laiką išskirtinai vyravę techniniai informacijos saugumo klausimai tebėra aktualūs, tačiau pastebima akivaizdi informacijos saugumo mokslinių tyrimų problematikos slinktis link platesnio, vis daugiau aspektų apimančio vadybinio požiūrio. Šiuo metu plačiausiai taikomų informacijos saugumo valdymo priemonių (metodikų, standartų, modelių) raidos analizė leidžia konstatuoti augančią taikomų priemonių turinio asimiliaciją, tačiau pastebint tai, kad nuolat kyla informacijos saugumo problemų, aiškėja, kad esamos priemonės nėra pakankamos informacijos saugumui valdyti (Jastiuginas, 2012). Jei neteisėti subjektai įsigyja svarbiausią informacinį turtą, pasekmės gali būti katastrofiškos ir sukelti didelių verslo nuostolių. Todėl saugus informacijos apdorojimas, neatsižvelgiant į jo formą, tapo būtinas visų dydžių įmonėms įvairiose pramonės šakose. Informacijos apsaugai įmonės aplinkoje būtina derinti techninius sprendimus su organizacine kontrole (Geko ir Tjoa, 2018). Cherdantseva ir Hilton (2013) teigimu, informacinis saugumas yra daugiadisciplininė studijų ir profesinės veiklos sritis, susijusi su visų prieinamų tipų (techninių, organizacinių, žmogiškųjų ir teisinių) saugumo priemonių kūrimu ir įgyvendinimu, siekiant išlaikyti informaciją be grėsmių. Jastiuginas (2012) teigia, kad, norint užtikrinti informacijos saugą, vien techninių priemonių neužtenka. Informacijos saugumo valdymas apima tris dimensijas:

1. Strateginę – tai administravimas, organizavimas, valdymas, standartų, teisinių priemonių ir gerųjų praktikų laikymasis.
2. Žmogiškąją – tai saugumo kultūra, kompetencija, mokymai, psichologiniai aspektai.
3. Technologinę – tai techninės ir programinės įrangos priemonės.

Bendrąja prasme saugumas – tai būsena, kai joks pavojus negresia. Tačiau absoliutaus saugumo pasiekti neįmanoma, bet tinkamai parinktos ir taikomos saugumo priemonės gali sumažinti rizikos laipsnį ir praradimų mastą.

Terminai „*kibernetinis saugumas*“ ir „*informacijos saugumas*“ dažnai vartojami pakaitomis. Kai kurie kibernetinio saugumo terminą naudoja kaip informacijos saugumo, IT saugumo ir informacijos rizikos valdymo sinonimą. Nors skirtingos grupės linkusios pritaikyti terminologiją savo tikslams, yra keletas svarbių skirtumų tarp kibernetinio saugumo ir informacijos saugumo. Informacijos saugumas susijęs su informacija, neatsižvelgiant į jos formatą – ji apima popierinius dokumentus, skaitmeninę ir intelektinę nuosavybę žmonių galvose ir žodinę ar vaizdinę komunikaciją. Kita vertus, kibernetinis saugumas yra susijęs su skaitmeninio turto apsauga – viskas, pradedant tinklais, baigiant aparatine įranga ir informacija, kurią apdoroja, saugo ar gabena IS (ISACA, 2017). Von Solms ir Van Niekerk (2013) teigia, kad informacijos saugumas yra informacijos, kuri yra turtas, apsauga nuo galimos žalos, kylančios dėl įvairių grėsmių ir pažeidžiamumų. Kita vertus, kibernetinis saugumas nebūtinai yra tik pačios kibernetinės erdvės apsauga, bet ir tų, kurie veikia virtualioje erdvėje, ir bet kokio jų turto, kurį galima pasiekti virtualioje erdvėje, apsauga. Kibernetinis saugumas gali būti apibrėžiamas kaip pačios kibernetinės erdvės, elektroninės informacijos, IRT,

palaikančių kibernetinę erdvę, ir kibernetinės erdvės vartotojų apsauga, atsižvelgiant į jų asmeninius, visuomenės ir nacionalinius pajėgumus, įskaitant bet kurį jų materialųjį interesą, arba nematerialų, kurie yra pažeidžiami virtualioje erdvėje kylančių atakų. Iš aukščiau pateiktų apibrėžimų tampa aišku, kad kibernetinio saugumo sritis yra kur kas platesnė už informacijos saugumą.

Svarbu, kad kibernetinio saugumo tyrimai plėtotų teorines ir praktines žinias, kurias pritaikius būtų galima įgyti reikiamų mąstymo įgūdžių panaudoti kibernetinį saugumą užtikrinančias priemones. Kritinio mąstymo įgūdžiai yra pagrindinė kibernetinio saugumo specialistų kompetencija (Nowduri, 2018). Grėsmėms kibernetiniam saugumui ir įgyvendinamoms apsaugos priemonėms didėjant ir vystantis, kibernetinio saugumo specialistai turi būti pasirengę prisitaikyti, kurti, plėtoti, įgyvendinti, prižiūrėti, vertinti ir suprasti visus kibernetinio saugumo aspektus (Kothari ir kt., 2018).

Pasaulį skiria sienos, tačiau internetas mažina ribas. Išpuoliai prieš asmenis, organizacijas ir vyriausybes gali būti surengti bet kurioje interneto vietoje ir įvykdyti taip, kad būtų padaryta dar neregėto masto žala. Tam reikalingos žinios apie įvairias atakas, jų vykdymą ir poveikio mastą (Raval ir kt., 2018). Išaugęs kibernetinio saugumo incidentų skaičius išryškino kibernetinio saugumo problemos mastą ir sudėtingumą (Alkhaledi ir Hawamdeh, 2020), nepaisant to, kad yra prieinami naujoviški technologiniai sprendimai ir svarbūs teisės aktai, skirti asmens duomenims apsaugoti. Kibernetinio saugumo supratimo programos yra reikalingos, norint atsikratyti atotrūkio tarp žmonių ir skaitmeninių technologijų (Safa, 2016). Tačiau vis dar išlieka tendencija daugiausia dėmesio skirti techninei perspektyvai, manant, kad naujoviški sprendimai, gali išspręsti esamas ir būsimas saugumo problemas (Corradini, 2020). Kibernetinis saugumas nėra tik techninė problema, tai yra verslo ir žmogaus klausimas, kuriame žmonių saugumo suvokimą formuoja socialinis ir pažintinis klausimas, susijęs su kultūra, norminiais įsitikinimais ir proto būsena. Suprasti ekonominius, situacinius ir elgesio klausimus, reguliuojančius žmonių rizikos suvokimą, yra labai svarbu kovojant su kibernetinio saugumo atakomis (Overfelt, 2016). Saugumo atakų nustatymas priklauso nuo technologinių ir žmogiškųjų veiksnių (Sababa ir kt., 2020).

Albanese ir kt. (2014) apibendrino, kad kibernetinės situacijos suvokimą galima vertinti kaip trijų fazių procesą:

1. *Situacijos suvokimas*. Suvokimas suteikia informacijos apie atitinkamų aplinkos elementų būseną, atributus ir dinamiką.
2. *Situacijos supratimas*. Situacijos supratimas apima tai, kaip žmonės sujungia, interpretuoja, kaupia ir saugo informaciją
3. *Situacijos projekcija*. Aplinkos (situacijos) elementų projekcija artimiausioje ateityje apima galimybę prognozuoti, remiantis žiniomis, įgytomis suvokiant ir suprantant.

Kai kibernetinio saugumo grėsmės tampa vis sudėtingesnės ir įvairesnės, organizacijos raginamos nuolat priimti ir atnaujinti priemones, skirtingas skirtingų tipų išpuoliams kontrastuoti (Esparza ir kt., 2020). Norint išvengti rizikos, reikia mokėti įvertinti susijusius žmogiškuosius veiksnius, tokius kaip situacijos supratimas ir procesai, kurie atsakingi už jos valdymą. Trys pagrindinių komponentų kategorijos daro

įtaką kibernetiniam saugumui kiekviename socialinės ir techninės sistemos organizaciniame lygmenyje:

1. Techninė rizika ir jų veiksniai.
2. Žmogaus rizika ir jų veiksniai.
3. Organizacinė rizika ir jų veiksniai.

Taigi, nesupratimas ar neįvertinimas kibernetinės rizikos yra pavojus organizacijai, į kurį reikia atsižvelgti valdybos lygiu. Kadangi kibernetinė rizika yra ne tik virtuali, bet ir reali, atsižvelgimas į šį rimtą pavojų yra situacijos ir rizikos suvokimo klausimas, atsižvelgiant į žinias, kognityvinį šališkumą ar emocines būsenas, kurios dalyvauja suvokiant riziką ir daro įtaką sprendimų priėmimo ir kontrolės procesams (Thiéry ir Fass, 2020). Bendros žinios apie saugumą ir privatumą yra kibernetinio saugumo pamatinio supratimo dalis. Itin svarbu turėti tiek techninių, tiek socialinių ir elgsenos žinių apie kibernetinį saugumą vis labiau susietoje visuomenėje (Chang ir kt., 2020).

Norint padidinti vartotojų supratimą apie saugumą, būtina užtikrinti, kad vartotojai suprastų pateiktą informaciją, kad galėtų praktiškai pritaikyti joje pateiktus patarimus. Subjektyvaus tyrimo metu buvo vertinama, kaip vartotojai supranta saugumo tekstus. Pastebėta, kad 61% rašytiniuose šaltiniuose naudojamų saugumo ekspertų terminų yra sunkiai suprantami visuomenei, net žmonėms, turintiems tam tikrą IT išsilavinimą. Taip pat pastebėta, kad 88% rašytinių šaltinių turi bent vieną tokį terminą (Wu ir kt., 2020).

Apibendrinant šį skyrių teigtina, kad organizacijos norėdamos užtikrinti kibernetinį saugumą turėtų taikyti visumą teisinių, informacijos sklaidos, organizacinių ir techninių priemonių. Absoliutaus saugumo pasiekti neįmanoma, bet tinkamai parinktos ir taikomos saugumo priemonės gali sumažinti rizikos laipsnį ir praradimų mastą. Kai kibernetinio saugumo grėsmės tampa vis sudėtingesnės ir įvairesnės, svarbu, kad organizacijos plėtotų teorines ir praktines žinias, kurias pritaikius įgytų reikiamų mąstymo įgūdžių panaudoti kibernetinį saugumą užtikrinančias priemones. Organizacijos norėdamos sustiprinti kibernetinį saugumą, turėtų investuoti ne tik į technines priemones, nes žmogiškosios klaidos faktorius vaidina didelį vaidmenį apsisaugant nuo kibernetinių incidentų, todėl darbuotojams svarbu suteikti techninių, socialinių ir elgsenos žinių apie kibernetinį saugumą.

1.2.2. Kibernetinio saugumo politikos įgyvendinimo organizacijose aspektai

Grėsmių nacionaliniam saugumui vertinime (2018) rašoma, kad Lietuva, kaip ir kitos pasaulio valstybės, kuriose aktyviai naudojamasi IRT teikiamomis galimybėmis, turinčios puikiai išplėtotą plačiajuosčio ryšio infrastruktūrą, tampa patraukli ne tik pavieniams asmenims, jų grupuotėms ar organizuotoms grupėms, bet ir LR valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie LR KAM rengiamose kasmetinėse Grėsmių nacionaliniam saugumui vertinimo ataskaitose įvardytoms valstybėms, keliančioms grėsmę Lietuvos nacionaliniam saugumui ir vykdančioms priešišką veiklą pasaulio ir Lietuvos kibernetinėje erdvėje.

NKSC, atsižvelgdamas į būtinybę incidentus klasifikuoti pagal poveikį, nuo 2019

m. kibernetiniais incidentais traktuoja atvejus, kada specialistai įvykius apdoroja betarpiškai – priskiria poveikio reikšmę bei nustato incidento kategoriją. Nuo šiol atskiriami automatinėmis priemonėmis ir programomis apdoroti procesai, kurie traktuojami kaip kibernetiniai įvykiai. Tokia klasifikacija, kai kibernetiniai įvykiai atskiriami nuo kibernetinių incidentų, įvesta siekiant suvienodinti klasifikavimą pagal ES kibernetinio saugumo agentūros bei kitų šalių kibernetinių incidentų valdymo komandų taksonomiją. Didinami pajėgumai ir gerinama kibernetinio saugumo branda leido aiškiau identifikuoti kibernetines grėsmes. Lietuvoje 2019 m. registruotas 3241, o 2020 m. 4330 kibernetinis incidentas, kai jų tyrimams atlikti reikėjo tiesioginio specialistų dalyvavimo. Automatinėmis priemonėmis apdorotų kibernetinių įvykių skaičius Lietuvos IP rėžyje 2019 m. siekė daugiau kaip 300000, o 2020 metais 306453, rašoma Nacionalinėse kibernetinio saugumo būklės ataskaitose. NKSC surinkti duomenys rodo, kad Lietuva nuolat susiduria su įvairaus tipo kibernetiniais incidentais. Kibernetinių incidentų skaičius Lietuvoje 2014 - 2022 m. (žr. 2 lentelę).

2 lentelė. Kibernetinių incidentų skaičius Lietuvoje 2014 - 2022 m.

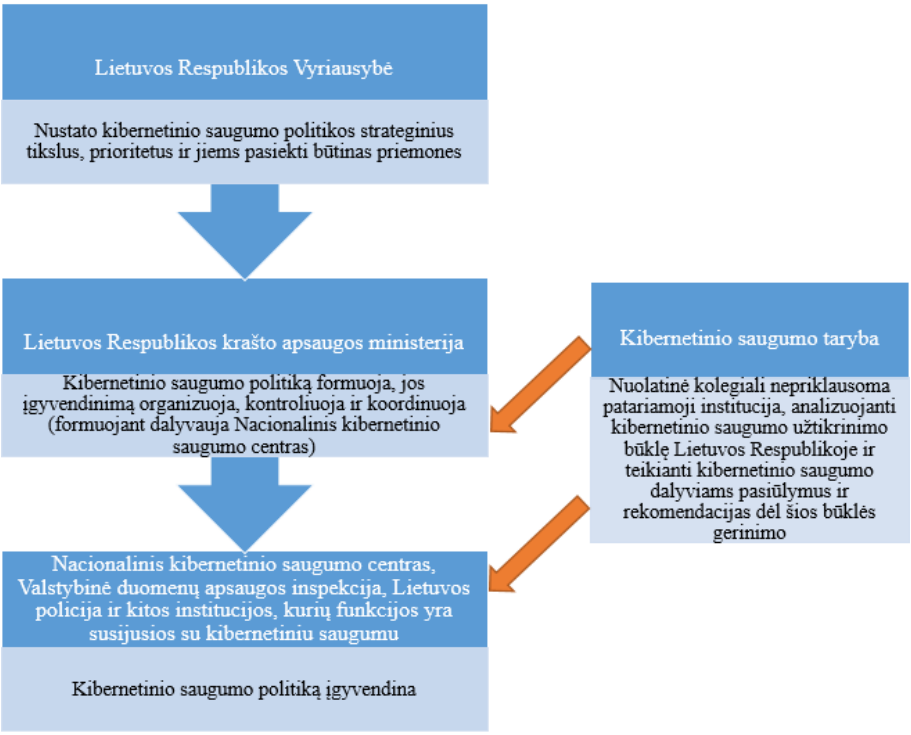
Metai	Kibernetinių incidentų skaičius Lietuvoje
2014	36136
2015	41583
2016	49463
2017	54414
2018	53183
2019	3241
2020	4330
2021	4088
2022	4080

Šaltinis: sudaryta autoriaus pagal nacionalines 2014 – 2022 m. kibernetinio saugumo būklės ataskaitas

Nusikalstamos veikos kibernetinėje erdvėje daro didelį neigiamą poveikį pasaulio ekonomikai. Kibernetinių nusikaltimų ataskaitos (2017) duomenimis, pasaulinė nusikalstamų veikų kibernetinėje erdvėje padaryta žala siekia šimtus milijardų eurų per metus ir numatoma jos augimo tendencija. Prognozuojama, kad ateityje jų skaičius ir mastas nemažės. Situacija Lietuvoje atspindi bendras pasaulio tendencijas, Pasaulinių rizikų ataskaitoje (2020) taip pat nurodoma, kad ateityje kibernetinių atakų tikimybė augs, kartu augs pavojus sutrikdyti YSII darbą. Kibernetinės atakos tampa labiau paplitusios, brangesnės ir daug sudėtingesnės (Augenbaum, 2019). Lietuva yra tarp lyderių pagal nacionalinį kibernetinio saugumo indeksą, užima trečiąją vietą po Graikijos ir Belgijos (E-Governance Academy, 2023).

KSĮ rašoma, kad Lietuvoje kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato LR Vyriausybė. LR KAM

kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja. Kibernetinio saugumo politiką įgyvendina NKSC, VDAI, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu. Kibernetinio saugumo taryba yra nuolatinė kolegiali nepriklausoma patariamoji institucija, kuri analizuoja kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikia kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijoms, kibernetinio saugumo subjektams, mokslo ir studijų institucijoms ir informacinių technologijų srityje veiklą vykdantiems verslo subjektams pasiūlymus dėl kibernetinio saugumo užtikrinimo būklės gerinimo (žr. 6 pav.).



6 pav. Kibernetinio saugumo politikos nustatymo, formavimo ir įgyvendinimo bei patariamosios institucijos

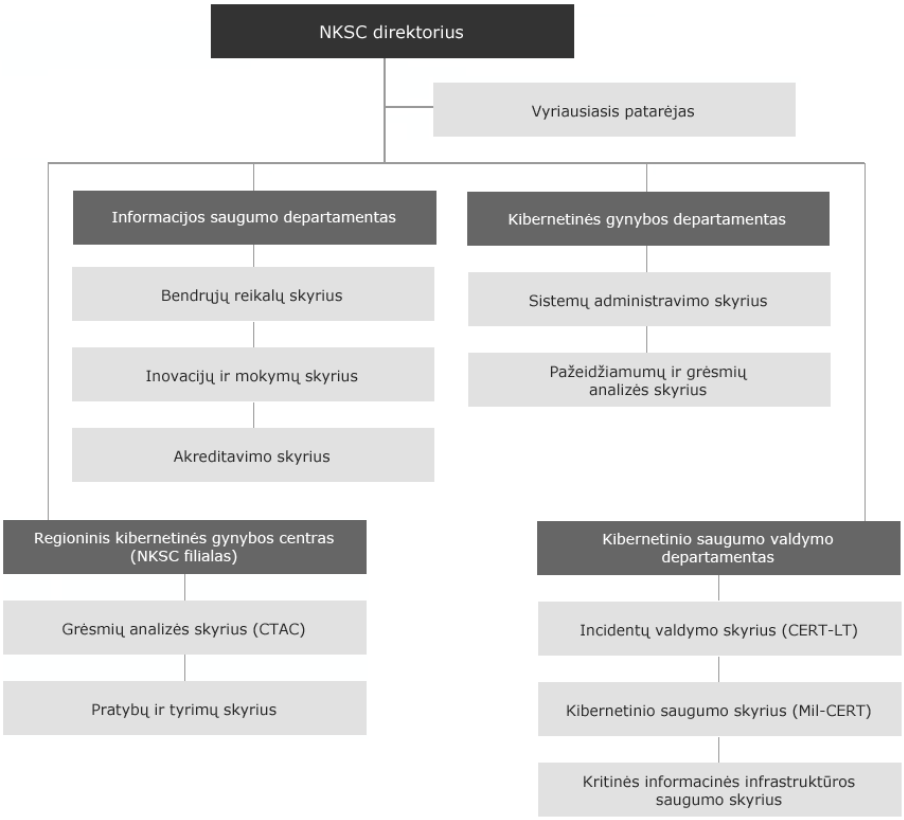
Šaltinis: sudaryta autoriaus pagal Lietuvos Respublikos kibernetinio saugumo įstatymą

Įgyvendinant KSĮ nuostatas, 2015 m. sausio 1 d. buvo įsteigtas NKSC prie KAM. NKSC yra pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę, YSII kibernetinį saugumą ir informacinių išteklių akreditaciją. Tai yra svarbiausia Lietuvos kibernetinio saugumo institucija. NKSC įgyvendina nacionalinę kibernetinio saugumo politiką ir vykdo valstybės informacinių išteklių

(skirstomi į keturias rūšis – ypatingos svarbos, svarbius, žinybinės svarbos ir kitus valstybės informacinius išteklius) ir YSII kibernetinių incidentų valdymo padalinio veiklą, taip pat įgyvendina valstybės įslaptintos informacijos apsaugos politiką įslaptintos informacijos RIS srityje.

Pagal KSĮ YSII yra RIS ar jos dalis, RIS grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams. Konkretus valstybės kritinės infrastruktūros sąrašas yra įslaptintas, jis apima valstybinius ir privačius energetikos, finansų sistemos, transporto, komunikacijų ir kitų sektorių IT sistemų valdytojus. Valstybinio audito ataskaitoje (2018) rašoma, kad ypatingos svarbos informacijos praradimas ir informacinių sistemų, kurios tvarko šią informaciją, nepasiekiamumas gali turėti skaudžių pasekmių visuomenės saugumui ir gerovei bei ekonomikai. Tinkamai sukurti ir efektyviai įgyvendinami informacinių technologijų procesai sudaro sąlygas veiksmingai apsaugoti informacinius išteklius nuo kylančių kibernetinių grėsmių.

NKSC vadovauja direktorius, kurį ketverių metų kadencijai LR valstybės tarnybos įstatymo nustatyta tvarka priima į pareigas ir atleidžia iš jų krašto apsaugos ministras. NKSC direktoriumi paskirtas asmuo šias pareigas eiti gali ne daugiau kaip dvi kadencijas iš eilės. NKSC personalą sudaro profesinės karo tarnybos kariai, valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis. NKSC ir jo personalas veikia pagal direktoriaus patvirtintas vidaus tvarkos taisykles, departamentų ir skyrių nuostatus, pareigybių aprašymus ir pareiginius nuostatus. NKSC direktorius planuoja, organizuoja ir kontroliuoja NKSC veiklą, kad būtų įgyvendinti NKSC tikslai, funkcijos ir užduotys, o atsiskaito už veiklą krašto apsaugos ministrui. NKSC sudaro trys departamentai ir vienas filialas (žr. 7 pav.).



7 pav. Nacionalinio kibernetinio saugumo centro struktūra

Šaltinis: Nacionalinis kibernetinio saugumo centras, 2020

NKSC veiklos tikslai – įgyvendinti nacionalinę kibernetinio saugumo politiką, atlikti Saugumo priežiūros tarnybos ir Nacionalinės komunikacijų apsaugos tarnybos funkcijas bei vykdyti informacijos sklaidos, tyrimų ir analizės kibernetinio saugumo klausimais veiklą.

Subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ir YSII valdytojams taikomi organizaciniai kibernetinio saugumo reikalavimai. Pagal Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 7 punktą, informacinės sistemos valdytojas privalo turėti pagal LR Vyriausybės patvirtintas Saugos dokumentų turinio gaires parengtus ir su NKSC suderintus bei patvirtintus šiuos saugos dokumentus:

1. Saugos nuostatus.
2. Saugaus elektroninės informacijos tvarkymo taisykles.
3. Informacinės sistemos veiklos tęstinumo valdymo planą.
4. Informacinės sistemos vartotojų administravimo taisykles.

Bendrieji elektroninės informacijos saugos reikalavimai reglamentuoja saugos organizavimą, incidentų valdymą, rizikos vertinimą, informacinės sistemos pokyčių valdymą, informacinių technologijų saugos atitikties vertinimą ir informacinės sistemos vartotojų atsakomybę (Štitilis ir kt., 2016). Saugos dokumentai institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus informacinės sistemos valdytojo vadovo nustatyta tvarka. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas arba institucijoje įvyksta esminių organizacinių, sisteminių ar kitokių pokyčių. Taip pat šie subjektai yra įsipareigoti:

1. Ne rečiau kaip kartą per metus arba po esminių organizacinių ar sisteminių pokyčių organizuoti ir atlikti RIS rizikos vertinimą.
2. Ne rečiau kaip kartą per metus organizuoti ir atlikti valstybės informacinių išteklių atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimą.
3. Ne rečiau kaip kartą per mėnesį atlikti valstybės informacinių išteklių ir valstybės informacinių išteklių naudotojų veiksmų audito įrašų analizę.
4. Ne rečiau kaip kartą per mėnesį atlikti saugasienių (angl. *Firewall*) užfiksuotų įvykių analizę ir pašalinti pastebėtas neatitiktis saugumo reikalavimams.
5. Ne rečiau kaip kartą per mėnesį įvertinti kibernetiniam saugumui užtikrinti naudojamų priemonių programinius atnaujinimus, klaidų taisymus ir šiuos atnaujinimus diegti.
6. Pirkdami paslaugas, darbus ar įrangą, susijusius su valstybės informaciniais ištekliais, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, pirkimo dokumentuose iš anksto nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrintų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

Techniniai kibernetinio saugumo reikalavimai subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ir YSII valdytojams nustatomi pagal jų svarbą – YSII, pirma kategorija, antra kategorija, trečia kategorija, ketvirta kategorija. Šiems subjektams taikomos techninės kibernetinių saugumo priemonės, kurių turinį sudaro:

1. Atpažinties, tapatumo patvirtinimo ir naudojimosi RIS saugumas ir kontrolė.
2. RIS, RIS naudotojų ir RIS administratorių atliekamų veiksmų auditas ir kontrolė.
3. Įsibrovimų aptikimas ir prevencija.
4. Belaidžio tinklo saugumas ir kontrolė.
5. Mobiliųjų įrenginių, naudojamų prisijungti prie RIS, saugumas ir kontrolė.
6. RIS naudojamos svetainės, pasiekiamos iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė.
7. RIS naudojamo interneto saugumas ir kontrolė.

Svarbu pabrėžti, kad šių priemonių konkretūs įgyvendinimo reikalavimai priklauso nuo subjekto svarbos. Bendrosios kibernetinio saugumo subjektų pareigos nurodytos KSĮ 11 straipsnyje, pagal jį kibernetinio saugumo subjektai:

1. Atsako už jų valdomų RIS ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams.
2. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, nustatyta tvarka atlieka rizikos vertinimą ir įdiegia kitas, naujausiais technikos laimėjimais paremtas ir nustatytai rizikai proporcingas, technines ir organizacines kibernetinio saugumo priemones.
3. Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka praneša NKSC apie jų valdomose ir (arba) tvarkomose RIS įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones.
4. Policijos generalinio komisaro nustatyta tvarka teikia policijai informaciją, reikalingą teisės pažeidimams, turintiems nusikalstamų veikų požymių, kibernetinėje erdvėje užkardyti ir tirti, ir vykdo kitus policijos nurodymus, duotus šio įstatymo nustatytais pagrindais. Policijos nurodymus dėl paslaugų teikimo jų gavėjui apribojimo privaloma įvykdyti ne vėliau kaip per 8 valandas nuo policijos nurodymo gavimo.
5. Paskiria kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Nacionaliniam kibernetinio saugumo centrui pateikia šio asmens ar padalinio kontaktinę informaciją.
6. Vykdo nustatytus NKSC nurodymus, siekiant įgyvendinti nacionalinę kibernetinio saugumo politiką.

Šios aukščiau išvardytos bendrosios kibernetinio saugumo subjektų pareigos nuostatos netaikomos skaitmenines paslaugas LR ir (arba) kitoje ES valstybėje narėje teikiančioms mažoms ir labai mažoms įmonėms, kurios yra apibrėžtos Smulkiojo ir vidutinio verslo plėtros įstatyme. Valstybės kontrolė 2022 m. spalio 27 d. valstybinio audito ataskaitoje „Kibernetinio saugumo užtikrinimas“ teigia:

1. *Saugumo valdymo sistema nepakankamai veiksminga*. Informacija apie kibernetinio saugumo subjektų identifikuotas kibernetinio saugumo rizikas nekaupiama bei nacionaliniu lygiu nevaldoma. Daugiau kaip trečdalis kibernetinio saugumo subjektų neatlieka kibernetinio saugumo rizikos vertinimo. Kibernetinio saugumo rizikos vertinimo procesas reikalauja specifinių šios srities žinių, todėl įstaigų rizikos vertinimą atliekantys specialistai kokybiškai įvertinti kibernetinio saugumo rizikų negali. Daugiau nei pusė vertinimus atlikusių kibernetinio saugumo subjektų informacijos apie identifikuotas kibernetinio saugumo rizikas NKSC nepateikia. Teisės aktuose neįtvirtinta prievolė kibernetinio saugumo subjektams periodiškai teikti NKSC rizikos vertinimo ataskaitas. Kadangi nėra identifikuotų nacionalinių kibernetinio saugumo rizikų, nėra sudarytas nacionalinių kibernetinio saugumo rizikos valdymo priemonių planas ir nenustatyta priimtina nacionalinė kibernetinio saugumo rizika, jos tolerancijos ribos, todėl nacionaliniu lygiu nėra koordinuojamas rizikos valdymo procesas, kuriuo būtų užtikrinamas reikiamų apsaugos, prevencijos ir atsako priemonių bei pajėgumų panaudojimas. Beveik pusė valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų nė karto neatliko informacinių

technologijų saugos atitikties vertinimo. 2021 m. nepateikta net 81 proc. valstybės informacinių išteklių informacinių technologijų saugos atitikties vertinimo ataskaitų. Didelė dalis (41 proc.) informacinių technologijų saugos atitikties vertinimus atlikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų duomenų ARSIS neteikė. Krašto apsaugos ministerijai 2015 m. perėmus kibernetinio saugumo ir 2018 m. valstybės informacinių išteklių (elektroninės informacijos saugos) politikos formavimo funkcijas nebuvo konsoliduota šių sričių teisinė bazė, todėl tam tikri skirtinguose teisės aktuose išdėstyti reikalavimai kibernetiniam saugumui ir elektroninės informacijos saugai užtikrinti yra tapatūs, o tai apsunkina saugumo reikalavimų įgyvendinimą kibernetinio saugumo subjektams.

2. *Tobulintinas kibernetinių incidentų valdymas*. Kibernetinius incidentus valdančios ir (ar) tiriančios institucijos (NKSC, VDAI, Lietuvos policija) ne visais atvejais keičiasi informacija apie kibernetinius incidentus, kurie joms aktualūs pagal jų veiklos pobūdį, todėl šios institucijos nesudaro prielaidų greitai atpažinti skirtingo pobūdžio kibernetinius incidentus ir perduoti kompetentingoms institucijoms informaciją, kad pastarosios galėtų laiku atlikti nusikalstamų veikų ar pažeidimų užkardymą, dėl to gali nukentėti kibernetinio saugumo subjektai ir visuomenė. Kibernetinio saugumo pratybos, mokymai ir konsultacijos kibernetinio saugumo klausimais vykdomos, bet yra nepakankamai rezultatyvios siekiant stiprinti kibernetinio saugumo subjektų gebėjimus efektyviai atremti kibernetines atakas ir užkirsti joms kelią. Kas ketvirtas kibernetinio saugumo subjektas (26 proc., 55 iš 212) neturi kibernetinių incidentų valdymo plano (tvarkos).
3. Neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas. Iš 28 Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniame veiklos plane numatytų priemonių tik 17 buvo visiškai įgyvendintos, 4 – neįgyvendintos, 7 – vykdytos, bet dėl COVID-19 pandemijos ir neįvykusių viešųjų pirkimų procedūrų buvo įgyvendintos ne visa apimtimi arba dėl baigtos priemonių įgyvendinimo stebėsenos nežinoma jų įgyvendinimo būklė. Dėl tų pačių priežasčių 11 (iš 38) strateginių rodiklių reikšmės nėra pasiektos, 5 (iš 38) – reikšmė nežinoma. Nenuoseklus suplanuotų kibernetinio saugumo stiprinimo priemonių įgyvendinimas ir nepakankama stebėsena lėmė tai, kad nacionalinių kibernetinio saugumo planavimo dokumentų nustatyti tikslai ir uždaviniai stiprinant valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, skatinant kibernetinio saugumo kultūrą ir inovacijų plėtrą, nėra visiškai pasiekti vertinant 2021 m. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo rezultatus pagal numatytus vertinimo kriterijus.

Atsižvelgiant į Valstybės kontrolės ataskaitoje nustatytus kibernetinio saugumo įgyvendinimo trūkumus KAM rekomenduojama:

1. Turi būti diegiamas ir nacionaliniu mastu koordinuojamas informacinių technologijų saugumo rizikų (įskaitant kibernetines) valdymo procesas, kuris leistų

gautą informaciją apie kibernetinio saugumo rizikingumo būklę naudoti priimant strateginius sprendimus dėl kibernetinio saugumo stiprinimo.

2. Sukurti bendrą valstybės informacinių išteklių kibernetinio saugumo ir informacinių technologijų saugos atitikties vertinimo metodiką, sudarančią galimybes atlikti išsamų atitikties teisės aktuose nustatytiems reikalavimams vertinimą, leisiančią priežiūrą ir stebėseną atliekančiai institucijai rezultatyviau pateikti duomenimis grįstą faktinės būklės nacionalinio lygiu analizę, įžvalgas, apibendrinimą.
3. Patvirtinti priemones, kurios užtikrintų sklandesnį komunikavimą apie kibernetinius incidentus naudojantis kibernetinio saugumo informaciniu tinklu; įpareigoti kibernetinio saugumo subjektus dalyvauti nacionalinėse kibernetinio saugumo pratybose ir numatyti NKSC vykdomos švietimo veiklos vertinimo rodiklius bei periodiškai juos stebėti; parengti ir patvirtinti detalų tipinį kibernetinių incidentų valdymo planą ir įpareigoti kibernetinio saugumo subjektus, pagal šio standartinio plano pavyzdį, parengti ar atnaujinti savo vidinius kibernetinių incidentų valdymo planus / tvarkas.

Apibendrinant šį skyrių, Lietuvoje kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato LR Vyriausybė. LR KAM kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja. Kibernetinio saugumo politiką įgyvendina NKSC, VDAI, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu. Kibernetinio saugumo valdymo sistema Lietuvoje nepakankamai veiksminga, tobulintinas kibernetinių incidentų valdymas, neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas. Valstybės kontrolės siūlomos rekomendacijos yra labai aktualios, nes prisidėtų prie kibernetinio saugumo stiprinimo. Visų pirma konsolidavus elektroninės informacijos saugos ir kibernetinio saugumo teisinę bazę, kibernetinio saugumo subjektams būtų lengviau įgyvendinti saugumo reikalavimus. Visų antra apibrėžus suderintą rizikos valdymo metodiką, kurios laikytųsi visi kibernetinio saugumo subjektai, o jų atliktų rizikos vertinimų rezultatai būtų teikiami ir kaupiami nacionaliniame rizikos registre, kibernetinio saugumo valdymas būtų rezultatyvus, nes leistų suformuoti kibernetinio saugumo rizikos profilį ir parengti Nacionalinę kibernetinio saugumo rizikos vertinimo ataskaitą bei patvirtinti Nacionalinį rizikos valdymo priemonių planą. Visų trečia užtikrinus sklandesnį komunikavimą apie kibernetinius incidentus, informacijos apsikeitimas įvyktų tarp NKSC, VDAI ir Lietuvos policijos reikiamu laiku ir leistų reaguoti į kibernetinius incidentus, o vadovaujantis patvirtintu tipiniu kibernetinių incidentų valdymo planu kibernetinio saugumo subjektai žinotų veiksmus, kaip reaguoti įvykus kibernetiniam incidentui.

1.3. Asmens duomenų apsaugos ir kibernetinio saugumo sąveikos bei įgyvendinimo problematika

Kibernetinio saugumo problema skiriasi nuo kitų saugumo problemų – tai epifenomenas, kompiuterių ir interneto revoliucijos pasekmė. Kai šimtai tūkstančių

žmonių visame pasaulyje atrado kompiuterio patogumą, jie įsigijo įrenginį ir skyrė jam svarbią vietą savo namuose, verslo vietoje arba vyriausybinėje įstaigoje. Visur esantis kompiuteris ir internetas, jungiantys vieną kompiuterį su kitu, siūlo didžiulį efektyvumą ir pritaikomą patogumą. Tačiau šis efektyvumas ir patogumas kainuoja nemažą kainą (Harknett ir Stever, 2011). KAM Nacionalinio kibernetinio saugumo būklės ataskaitoje už 2020 metus rašoma, kibernetinio saugumo priemonių taikymas ir jų laikymasis asmens duomenų apsaugos srityje yra būtina sąlyga, kad visuomenė pasitikėtų valstybės ir savivaldybių institucijomis ir įstaigomis ir kitomis organizacijomis bei naudotųsi jų teikiamomis informacinės visuomenės paslaugomis. Todėl šiuolaikinėje skaitmeninėje visuomenėje nepaprastai svarbus tiek viešojo, tiek privataus sektoriaus atstovų tinkamas dėmesys kibernetiniam ir asmens duomenų saugumui organizaciniame ir įgyvendinimo lygmenyje bei pačios visuomenės kibernetinio saugumo sąmoningumo lygis.

Kadangi Reglamento reikalavimai yra labai abstraktūs, juos galima interpretuoti. Tiesą sakant, kiekviena organizacija turi savo būdą, kaip įgyvendinti Reglamentą ir įrodyti atitiktį. Kiekviena ES valstybė narė nustato Priežiūros instituciją (gali būti kelios), kuri yra atsakinga už Reglamento atitikties stebėseną. Organizacijos privalo įrodyti atitiktį tik tada, kai Priežiūros institucija įtaria pažeidimą arba kai duomenų subjektas pateikia skundą Priežiūros institucijai (Truong ir kt, 2019). Reglamentas sukūrė nuoseklią teisinę sistemą, suteikiančią duomenų subjektams teises ir jų įgyvendinimo mechanizmą, bei veiksmingas teisinės gynybos priemones, kurios prieinamos kiekvienam fiziniam asmeniui (Novikovienė ir Pedaniuk, 2020). Tačiau Priežiūros institucijų gebėjimas atlikti savo funkcijas priklauso nuo įvairių veiksnių, kurie gali keistis atsižvelgiant į nacionalines aplinkybes (t. y. nuo to, kaip jos aprūpintos finansiniais ir žmogiškaisiais ištekliais). Dėl tokio nustatymo įmonėms kyla neaiškumų, kaip tvarkyti asmens duomenis, ir neleidžiama pasinaudoti veiksminga vienoda teisine erdve šioje srityje. Visoje Europoje Priežiūros institucijos ir kitos priežiūros institucijos Reglamentą taiko ir interpretuoja skirtingai. Taip kartais gali būti net vienoje šalyje, kai duomenų apsaugos taisykles taiko kelios institucijos. Todėl įmonės dažnai nėra tikros, ar iki galo laikosi Reglamento nuostatų. Galutinį sprendimą, kaip spręsti susidariusią situaciją, priima pati organizacija, kuri prisiima teisines to pasekmes (Jasmontaitė-Zaniewicz ir kt., 2021).

Anot autorių Daigle ir Khan (2020) naujausių duomenų apie faktines pinigines baudas, kurias skyrė konkrečios Priežiūros institucijos, tendencijos rodo, kad Rytų Europos šalių Priežiūros institucijos skyrė mažiau baudų, ir vengė didelių baudų; be to, jos paprastai lėčiau skirdavo baudas nei Vakarų Europos kolegos, kurios gali turėti didesnius reguliavimo pajėgumus, kad užtikrintų Reglamento vykdymą atitinkamose šalyse (ypač tarptautinėms įmonėms). Dauguma šių piniginių baudų, kurias taiko Rytų Europos šalys, buvo skirtos įmonėms, kurių pagrindinė būstinė yra šalyje, nedidelėms organizacijoms, valstybės įmonėms, politinėms partijoms ar bankams. Priežiūros institucijų skirtumai Reglamento taikymo interpretacijose ir baudų skyrimo praktikoje rodo nenuoseklų ES duomenų apsaugos teisės aktų vykdymą visoje Europoje. Tačiau kai kuriais atvejais gali kilti netikrumo, kai Priežiūros institucijų gairės prieštarauja

EDAV rekomendacijoms (Gabel ir Hickman, 2019). Duomenų privatumo ekspertai tvirtina, kad netolygus vykdymo ir baudų lygis už Reglamento pažeidimus visoje ES sukėlė neapibrėžtumą (Satariano, 2020).

Reglamentas suteikia Priežiūros institucijoms daug įvairių vykdymo galių, pradedant nuo įgaliojimų atlikti tyrimus, prašyti informacijos ir skelbti įspėjimus iki galimybės skirti dideles administracines baudas už duomenų apsaugos taisyklių pažeidimus, o tai paprastai laikoma įtikinamiausia motyvacija. Priežiūros institucijos taip pat turi teisę uždrausti vykdyti duomenų tvarkymo veiklą ir įsakyti sustabdyti duomenų srautus, o tai gali sustabdyti organizacijos efektyvų funkcionavimą ir galiausiai nutraukti organizacijos veiklą. Siekdamos suderinti reguliavimo veiklą visoje Europoje, Priežiūros institucijos privalo bendradarbiauti tarpusavyje ir laikytis nuoseklumo užtikrinimo mechanizmo pagal Reglamentą, kad būtų užtikrintas nuoseklus požiūris į svarbiausius sprendimus.

Reglamente reikalaujama, kad organizacijos įgyvendintų „*tinkamas technines ir organizacines*“ asmens duomenų apsaugos priemones. Kokios priemonės yra tinkamos, priklauso nuo duomenų jautrumo ir rizikos laipsnio, jei asmens duomenys bus pažeisti. Iš esmės, kuo jautresni duomenys (pvz., žmogiškųjų išteklių įrašai, finansiniai duomenys, sveikatos įrašai), tuo griežtesnių priemonių reikia, kad jie būtų apsaugoti. BDAR sunku taikyti ir dėl jo ilgio, sudėtingumo, apimančio daugelį aspektų ir nepateikiamos išsamios informacijos apie taikytinas technines ir organizacines saugumo priemones. Kadangi teisiniai reikalavimai dažnai yra pernelyg abstraktūs, jie gali palikti vietos įvairioms interpretacijoms. Pavyzdžiui, BDAR nurodo, kad organizacijos turi užtikrinti pagrįstą asmens duomenų apsaugos lygį, nepaaiškindamos, ką tiksliai reiškia „protingas“ (Nadeau, 2017; Piras ir kt., 2019).

Pažymėtina tai, kad vartotojai pasitiki teisės aktais, tačiau ne tiek pasitiki įmonėmis, kurios tvarko asmens duomenis; jie nori kontroliuoti savo duomenis, o ne palikti juos valdyti įmonėms (Mangini ir kt., 2020). Mokslininkai Presthus ir Sønslien (2021) remdamiesi 277 asmens duomenų saugumo pažeidimų ir sankcijų analize, nustatė penkis pagrindinius pažeidimus:

1. Neteisėtas asmens informacijos tvarkymas.
2. Asmeninės informacijos atskleidimas.
3. Subjektų teisių nesilaikymas.
4. Asmeninės informacijos neužtikrinimas.
5. Nepakankamas bendradarbiavimas su priežiūros institucija.

Vienas iš didžiausių iššūkių, su kuriais susiduria organizacijos, norėdamos apsaugoti duomenis, yra tiesiog suprasti, kokius duomenis šiuo metu tvarko, koks jų judėjimas ir kas prie jų gali prisijungti. To nesuprantant, sunku kontroliuoti duomenis ir nustatyti jų tvarkymo riziką (Datta ir kt., 2015; van Ooijen ir Vrabec, 2019). Viena svarbiausių silpnos apsaugos priežasčių – bendras nesuvokimas, kad rūpintis sauga yra būtina. Iš kitų priežasčių galima paminėti nepatyrusius saugos srityje dirbančius specialistus ir finansavimo (saugai užtikrinti reikalingų lėšų) trūkumą (Štitilis ir kt., 2016). Organizacijos, privalo suprasti, kokie Reglamento reikalavimai yra joms taikomi, kad duomenų subjektai nustatytų savo teises, kad duomenų valdytojai

ir tvarkytojai suprastų savo pareigas. Organizacijų pasitikėjimas esama valdomos infrastruktūros apsauga, informacinių sistemų aptarnaujančio personalo žiniomis, naudojama technologine įranga ir jos atliekamomis funkcijomis bei supančios aplinkos suvokimo problematika sukelia galimybes rengti sėkmingas kibernetines atakas prieš organizacijas ir sistemas (Agafonov, 2021).

Nacionalinėje kibernetinio saugumo ataskaitoje (2020) rašoma, organizacijos dažnai atitinka arba beveik atitinka saugos politikos *de jure* kriterijų. Tikrinami subjektai turi formaliai apsibrėžę saugos procesus, gaires, tačiau saugos užtikrinimas dažnai vertinamas kaip biurokratinė našta. Saugos dokumentai būna parengti formaliai, pagal nebegaliojančius Lietuvos Respublikos teisės aktus, o dokumentų turinyje apibrėžti procesai nebūna priskirti pagal kompetenciją.

Pats rizikų valdymo procesas Lietuvos viešajame sektoriuje neblogai reglamentuotas, tačiau rekomenduojama atnaujinti metodines priemones; kasmet atliekami rizikų vertinimai ganėtinai formalūs; į bendrą rizikų procesą rekomenduojama įtraukti daugiau organizacijos atstovų, ne tik Saugos įgaliotinius (Grincevičius, 2019).

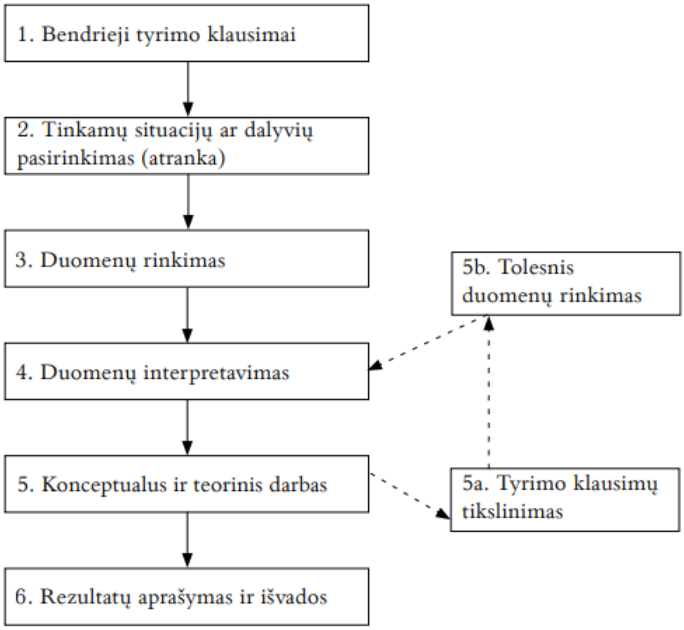
Apibendrinus galima teigti, kad Reglamento reikalavimai yra labai abstraktūs, juos galima įvairiai interpretuoti, kiekviena organizacija turi savo būdą, kaip užtikrinti pagrindinius asmens duomenų principus ir įrodyti atitiktį Reglamento reikalavimams, kuomet Priežiūros institucija įtaria asmens duomenų saugumo pažeidimą arba kai duomenų subjektas pateikia skundą Priežiūros institucijai. Priežiūros institucijų skirtumai Reglamento taikymo interpretacijose ir baudų skyrimo praktikoje rodo nenuoseklų ES duomenų apsaugos teisės aktų vykdymą visoje Europoje. Kibernetinio saugumo priemonių taikymas ir jų laikymasis asmens duomenų apsaugos srityje yra būtina sąlyga, kad visuomenė pasitikėtų organizacijomis ir naudotųsi jų teikiamomis paslaugomis. Reglamente reikalaujama, kad organizacijos įgyvendintų „*tinkamas technines ir organizacines*“ asmens duomenų apsaugos priemones. Kokios priemonės yra tinkamos, priklauso nuo duomenų jautrumo ir rizikos laipsnio, jei asmens duomenys bus pažeisti. Todėl organizacijoms svarbu įsivertinti kokius duomenis šiuo metu tvarko, siekiant juos apsaugoti. Organizacijos *de jure* dažnai atitinka arba beveik atitinka kibernetinio saugumo reikalavimus, nes turi formaliai apsibrėžę saugos procesus, gaires, kurie nebūtinai atitinka realią situaciją organizacijoje, siekiant užtikrinti kibernetinį saugumą ir asmens duomenų apsaugą.

2. ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE PRIEMONIŲ TYRIMO METODOLOGIJA

2.1. Tyrimo planas

Socialinių mokslų tyrėjas yra tiriamo objekto dalis, nes teoriškai ir empiriškai analizuoja visuomenėje žmonių tarpusavio santykius ir kartu dalyvauja kurdamas visuomeninį gyvenimą (subjektas) (Coleman, 2005; Hunt ir Colander, 2008). Socialinių mokslų tyrimai apima kertines tyrimų atlikimo stadijas: problemos formulavimą, tyrimo projekto parengimą, duomenų rinkimą, kodavimą ir analizavimą, duomenų interpretavimą (Bailey, 2008). Pozityvizmas remiasi deterministine filosofija, kurios esmė yra priežastingumo ir pasekmės ryšiai. Todėl pozityvistai savo tyrimais siekia identifikuoti ir įvertinti šiuos ryšius (Skukauskaitė ir Rupšienė, 2017). Pozityvizmo požiūriu socialinis mokslas turi padėti paaiškinti socialinių reiškinių priežasties ir pasekmės ryšius, kad būtų galima socialinius reiškinius „pozityviai" paveikti siekiant visuomenės tobulėjimo (Trochim, 2006). Atliekant tyrimus remtasi pozityvizmo moksline paradigma. Pozityvizmo paradigmoje atsižvelgiama į realybę, kaip susidedančią iš atskirų įvykių, kurie gali būti stebimi žmogaus pojūčiais. Vienintelis priimtinas šios realybės žinojimas yra kildinamas iš patyrimo. Pozityvizmas atmeta visas teoretines ar metafizines idėjas, kurios nėra kildinamos iš patyrimo. Teigiama, kad viskas, kas nėra patvirtinama patyrimu – neturi prasmės (Blaikie, 2007).

Kokybinis tyrimas yra grindžiamas griežtomis metodologinėmis tradicijomis ir nagrinėja socialines bei žmonių problemas, todėl prieš atliekant kokybinį tyrimą yra svarbus tinkamos strategijos pasirinkimas. Tyrimo strategija apima tyrimo planavimą, duomenų rinkimą ir apibendrinimą, tyrimo procedūrų panaudojimo tvarką, informacijos šaltinius ir jos rinkimo bei analizės metodus (Bitinas, Rupšienė, Žydžiūnaitė, 2008; Creswell, 1998). Kokybinių tyrimų tikslas yra pateikti išsamią ir iliustratyvią informaciją, kad būtų galima suprasti įvairius analizuojamos problemos aspektus. Todėl kokybiniai tyrimai yra susiję su realybės aspektais, kurių negalima kiekybiškai įvertinti, daugiausia dėmesio skiriant socialinių santykių dinamikos supratimui ir paaiškinimui (Queirós ir kt., 2017). Kokybinis tyrimas turi pranašumą, lyginant su kiekybiniu tyrimu, kuomet kuriamos naujos idėjos. Kokybinis tyrimas atlieka žvalgybinę funkciją, padedančią pasirengti kiekybiniam tyrimui (Bitinas, Rupšienė ir Žydžiūnaitė, 2008). Bryman (2008) pateikta schema gana aiškiai atskleidžia kokybinio tyrimo proceso savitumą (žr. 8 pav.).



8 pav. Kokybinio tyrimo procesas

Šaltinis: Bryman, 2008

Tyrimo metodologija remiasi keliais tyrimų metodais, kurie padidina tyrimo rezultatų tikslumą, pagerina atskirų metodų ribotą pritaikomumą bei padeda užčiuopti silpnai išreikštus reiškinius. Norint pasiekti pagrindinį tyrimo tikslą buvo atlikti keturi tyrimai:

- **Pirmasis tyrimas**. Naudojant *dokumentų analizės metodą* 2021 – 2022 m. buvo išanalizuoti kibernetinio saugumo ir asmens duomenų teisės aktai, standartai ISO 27001 ir ISO 27002 bei VDAI parengtas gairės „*Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*“, siekiant nustatyti kokios yra kibernetinio saugumo ir asmens duomenų apsaugos taikomos priemonės ir imtis Lietuvoje. Tyrimo metu buvo sudarytas svarbiausių kibernetinio saugumo ir asmens duomenų srities teisės aktų, standartų ir gairių sąrašas su juose įtvirtintais reikalavimais ir/ar priemonėmis (žr. 2 priedas). Šių dokumentų ir juose nustatytų reikalavimų ir/ar priemonių pagrindu buvo atliekamas antrasis tyrimas – informacinių technologijų saugos atitikties vertinimas ir rengiama ketvirtojo tyrimo pusiau struktūruoto klausimyno IV-oji dalis (žr. 3 lentelę). Remiantis pirmojo tyrimo metu gautais apibendrintais duomenimis buvo kuriamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, kuriame buvo nurodytos privalomos pagal teisės aktus taikyti priemonės, siekiant užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą organizacijose.

- **Antrasis tyrimas**. Naudojant *atvejo analizės metodą* 2021 – 2022 m. buvo atlikti trijų organizacijų informacinių technologijų saugos atitikties teisės aktų, reglamentuojančių kibernetinį saugumą ir asmens duomenų apsaugą, standartų ir gairių, vertinimai (toliau – Atitikties vertinimas), siekiant nustatyti pagrindines neatitiktis ir jų keliamas grėsmes organizacijų kibernetiniam saugumui ir asmens duomenų apsaugai. Atitikties vertinimo rezultatų pagrindu buvo rengiama ketvirtojo tyrimo pusiau struktūruoto klausimyno V-oji dalis (žr. 3 lentelę). Taip pat remiantis šio antrojo tyrimo metu gautais apibendrintais duomenimis buvo kuriamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, kuriame buvo nurodytos priemonės, siekiant pašalinti antrojo tyrimo metu nustatytas neatitiktis ir užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą organizacijose.
- **Trečiasis tyrimas**. Naudojant *atvejo analizės ir lyginamąjį metodą* 2022 m. kovo – balandžio mėn. buvo atliktas asmens duomenų tvarkymo teisėtumo nustatymo tyrimas 100 Lietuvos populiariausių svetainių, siekiant įvertinti organizacijų asmens duomenų, konkrečiai slapukų (angl. *Cookies*) naudojimo teisėtumą interneto svetainėse. Tyrimo metu gauti rezultatai palyginti su anksčiau 2020 metų spalio – lapkričio mėnesiais atliktu tyrimu, siekiant įvertinti, kaip pakito situacija, ar organizacijos skiria daugiau dėmesio asmens duomenų apsaugai tvarkydamos slapukus interneto svetainėse. Asmens duomenų tvarkymo teisėtumo nustatymo tyrimo rezultatų pagrindu buvo rengiama ketvirtojo tyrimo pusiau struktūruoto klausimyno VI-oji dalis (žr. 3 lentelę). Taip pat remiantis šio trečiojo tyrimo metu gautais apibendrintais duomenimis buvo kuriamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, kuriame buvo nurodytos priemonės padėsiančios užtikrinti teisėtą asmens duomenų tvarkymą organizacijose.
- **Ketvirtasis tyrimas**. Naudojant *ekspertų interviu metodą* 2022 m. birželio mėn. – 2023 m. sausio mėn. buvo atliktas pusiau struktūruotas interviu, kurio metu buvo apklausti 9 ekspertai, siekiant sužinoti jų nuomonę apie elektroninių duomenų saugaus valdymo priemones ir jų taikymą. Apdorojant gautus duomenis remtasi turinio (angl. *Content*) analize. Remiantis šio ketvirtojo tyrimo metu gautais apibendrintais duomenimis buvo kuriamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, kuriame buvo nurodytos priemonės padėsiančios užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą bei sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio incidento rizikas.

2.1.1. Kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymo ir imties nustatymo tyrimas

Dokumentai gali būti laikomi socialinės situacijos duomenimis, kuriais individai, grupės, socialinės aplinkos, institucijos ir organizacijos prisistato ir atsiskaito (Coffey, 2014). Dokumentuose pateikiama informacija apie tam tikrą socialinį fenomeną

egzistuoja nepriklausomai nuo tyrėjo veiksmų (Corbetta, 0213). Dokumentų analizei keliamas reikalavimas, kad duomenys būtų nagrinėjami ir interpretuojami, siekiant išsiaiškinti prasmę, įgyti supratimo ir plėtoti empirines žinias (Corbin ir Strauss, 2008). Analizės procedūra apima dokumentuose esančių duomenų suradimą, atranką, įvertinimą (įprasminimą) ir sintezę. Dokumentų analizės metu gaunamos duomenų ištraukos, citatos ar visos ištraukos, kurios vėliau suskirstomos į pagrindines temas, kategorijas ir atvejų pavyzdžius, konkrečiai naudojant turinio analizę (Labuschagne, 2003). Bowen, (2009) teigia, kad dokumentuose esanti informacija gali pasiūlyti kai kuriuos klausimus, kuriuos reikia užduoti, ir situacijas, kurias reikia stebėti atliekant tyrimą, pvz. Goldstein ir Reiboldt (2004) atliko dokumentų analizę, kad padėtų generuoti naujus interviu klausimus. Jų tyrimai parodė, kaip vienas metodas gali interaktyviai papildyti kitą. Taigi, informacija ir įžvalgos, gautos iš dokumentų, gali būti vertingi žinių bazės papildymai. Dažnai dokumentiniai įrodymai derinami su duomenimis iš interviu ir stebėjimų, siekiant sumažinti šališkumą ir užtikrinti patikimumą (Bowen, 2009).

Šiame tyrime dokumentų analizės metodas naudojamas kaip papildomas duomenų rinkimo metodas.

Atlikta 2021 – 2022 m. aktualių dokumentų analizė buvo svarbi rengiant ekspertų apklausos klausimyną. Taip pat dokumentų analizės metodas papildė kitą duomenų rinkimo metodą – ekspertų apklausą. Analizuojamų dokumentų tipas, oficialūs dokumentai – nacionaliniai ir tarptautiniai teisės aktai, standartai ir gairės. Oficialių dokumentų analizė svarbi dėl patikimos ir objektyvios faktinės informacijos gavimo apie tiriamą reiškinį. Svarbu pažymėti, jog ne visi analizuoti dokumentai yra laisvai prieinami, standartai ISO 27001 ir ISO 27002 yra parduodami Lietuvos standartizacijos departamento elektroninėje parduotuvėje.

Siekiant objektyviai išnagrinėti dokumentų tekstą, aktualūs dokumentai buvo analizuojami dokumento teksto analizės metodu, kuris koncentruojasi į tam tikrų žodžių reikšmę (Tidikis, 2003). Šis metodas pasirinktas dėl keliamo tyrimo tikslo – nustatyti kokios yra privalomos kibernetinio saugumo ir asmens duomenų apsaugos priemonės bei jų taikymo imtis Lietuvoje.

Disertacijos autorius pasirinko tuos dokumentus, kurie yra aktualūs ne specifinėms organizacijoms, bet visai Lietuvos viešojo valdymo sistemai. Tai – svarbiausių kibernetinio saugumo ir asmens duomenų srities teisės aktų, standartų ir gairių sąrašas su juose įtvirtintais reikalavimais ir/ar kontrolės priemonėmis, kurios išskirtos į organizacines ir technines.

Atkreiptinas dėmesys, kad autorius tyrimo metu vykdė tik vidinę dokumentų analizę, t. y. dokumento turinio analizę, kurios pagrindiniai elementai kibernetinio saugumo ir asmens duomenų apsaugos kontrolės priemonės. Detalus analizuotų dokumentų pristatymas pateiktas disertacijos 2 priede. Dokumentų analizė teikia pirminę informaciją ir leidžia vėliau tikslingai ir kryptingai taikyti kitus tyrimo metodus.

2.1.2. Informacinių technologijų saugos atitikties vertinimo tyrimas

Atvejo analizės metodas patogus tuo, kad yra analizuojami realūs konkrečios tikrovės atvejai, situacijos, kurios vėliau paverčiamos elgesio modeliais, sektinais pavyzdžiais. Šis metodas gali būti taikomas realioms gyvenimo, profesinės veiklos problemoms spręsti, nes padeda objektyviai suvokti įvairias jų atsiradimo aplinkybes ir priežastis (Kvieskienė ir Kvieska, 2018). Atvejo tyrimas apibūdinamas kaip empirinį metodas, padedantis tirti tam tikrą fenomeną, kai tarp fenomeno ir jo konteksto nėra akivaizdžios ribos, o moksliniam pagrindimui yra naudojamas ne vienas šaltinis (teorinis ir empirinis duomenų rinkimo metodas), bet ir gretutiniai įrodymai (Bitinas, 2016; Yin, 2009). Pasirinktas atvejo analizės metodas, leidžia nuodugniai išanalizuoti situaciją realiame kontekste ir apibūdinti bei paaiškinti tiriamą reiškinį (Lapoule, Lynch, 2018).

Kibernetinio saugumo vertinimu siekiama nustatyti vertinamo subjekto (vertinimo objekto) kibernetinio saugumo būseną (Bertoglio ir Zorzo, 2017; Qassim ir kt., 2019). Tai atsako į klausimą, kaip efektyviai subjektas įgyvendina konkrečius saugumo tikslus (Scarfone ir kt., 2008). Tai ciklišKas procesas, kuomet vertinami kibernetinio saugumo reikalavimai, atsižvelgiant į galimą riziką, grėsmių pasekmes ir susijusias išlaidas. Naudojant nustatytas apsaugos priemones, kibernetinio saugumo vertinimu siekiama įvertinti teisingą priemonių įgyvendinimą, atsižvelgiant į sistemos saugumo reikalavimų tenkinimą (Chapple ir kt., 2018). Labiausiai paplitę kibernetinio saugumo vertinimo tipai apima kontroliniu sąrašu pagrįstą vertinimą, atitikties patikrą, pažeidžiamumo nustatymą, formalią analizę ir peržiūras (Leszczyna, 2021).

2021 – 2022 metais buvo atlikti trijų organizacijų Atitikties vertinimai pagal informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „*Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo*“, nustatyta tvarka (toliau – Metodika).

Atitikties vertinimas buvo atliktas vertinant atitiktį šių tarptautinių ir nacionalinių teisės aktų, standartų ir gairių reglamentuojančių elektroninės kibernetinį saugumą ir asmens duomenų apsaugą, reikalavimams:

1. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“.
2. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų

(kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo".

3. Lietuvos standartas LST EN ISO/IEC 27001:2017 *„Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai".*
4. Lietuvos standartas LST EN ISO/IEC 27002:2017 *„Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai".*
5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo".
6. Valstybinės duomenų apsaugos inspekcijos parengtos gairės „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams" (3 versija, 2020-06-18).
7. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

Atitikties vertinimo metu buvo įvertintas trijų organizacijų aukščiau nurodytų tarptautinių ir nacionalinių teisės aktų, standartų ir gairių reikalavimų:

1. Reglamentavimas vidaus teisės aktuose.
2. Faktinis įgyvendinimas praktikoje.

Įgyvendinimo lygis saugumo reikalavimams vertintas, vadovaujantis Atitikties vertinimo metodika. Įgyvendinimo lygis nustatomas pagal penkių balų skalę, kurioje žemiausia reikšmė yra vienetas, o aukščiausia – penketas:

1. vienetas – saugos reikalavimas ar reikalavimai (toliau – saugos reikalavimai) neįgyvendinti ir nesiimta veiksmų šiems reikalavimams įgyvendinti;
2. dvejetas – saugos reikalavimai neįgyvendinti, tačiau imtasi veiksmų šiems reikalavimams įgyvendinti (informacinės sistemos valdytojas ar jo pavedimu informacinės sistemos tvarkytojas, siekdamas įgyvendinti saugos reikalavimus, patvirtino veiksmų planą, parengė teisės akto projektą, investicijų projektą ir pan.);
3. trejetas – saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant (vertintojo nuomone, labai vėluojama vykdyti Metodikos 1 punkte nurodytuose teisės aktuose ir standartuose bei saugos dokumentuose nustatytas procedūras arba jos iš viso nėra vykdomos, saugos dokumentai nustatytu laiku neperžiūrimi ir (ar) neatnaujinami, nepaskirti atsakingi vykdytojai arba jie nesupažindinti su atitinkamomis procedūromis, įgyvendintos informacinių technologijų saugos priemonės nepasiekia joms keltų tikslų ir pan.);
4. ketvertas – saugos reikalavimai įgyvendinami, tačiau nustatyta neesminių trūkumų (vertintojo nuomone, nedaug nukrypstama nuo saugos reikalavimams

keliamų kiekybinių rodiklių, nedaug vėluojama vykdyti Metodikos 1 punkte nurodytuose teisės aktuose ir standartuose bei saugos dokumentuose nustatytas procedūras, peržiūrėti ir (ar) atnaujinti saugos dokumentus ir pan.);

5. penketas – saugos reikalavimai įgyvendinami visa apimtimi.

Atitikties vertinimo tikslas nustatyti neatitiktis ir pateikti rekomendacijas nustatytų trūkumų pašalinimui. Kadangi trijų organizacijų Atitikties vertinimo imtis yra didelė, todėl rezultatai bus pateikiami tik tų nustatytų neatitikčių kurios įvertintos trejetu ir mažiau visose trijose organizacijose, o ne kiekvienoje atskirai.

Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 5 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" 9 punkte rašoma: „*Ne rečiau kaip kartą per metus turi būti organizuojamas ir atliekamas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros atitikties organizacinius ir techninius kibernetinio saugumo reikalavimus (toliau – Reikalavimams) vertinimas*."

Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo patvirtinto Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo" 8.2 punkte rašoma: „*ne rečiau kaip kartą per trejus metus atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai*."

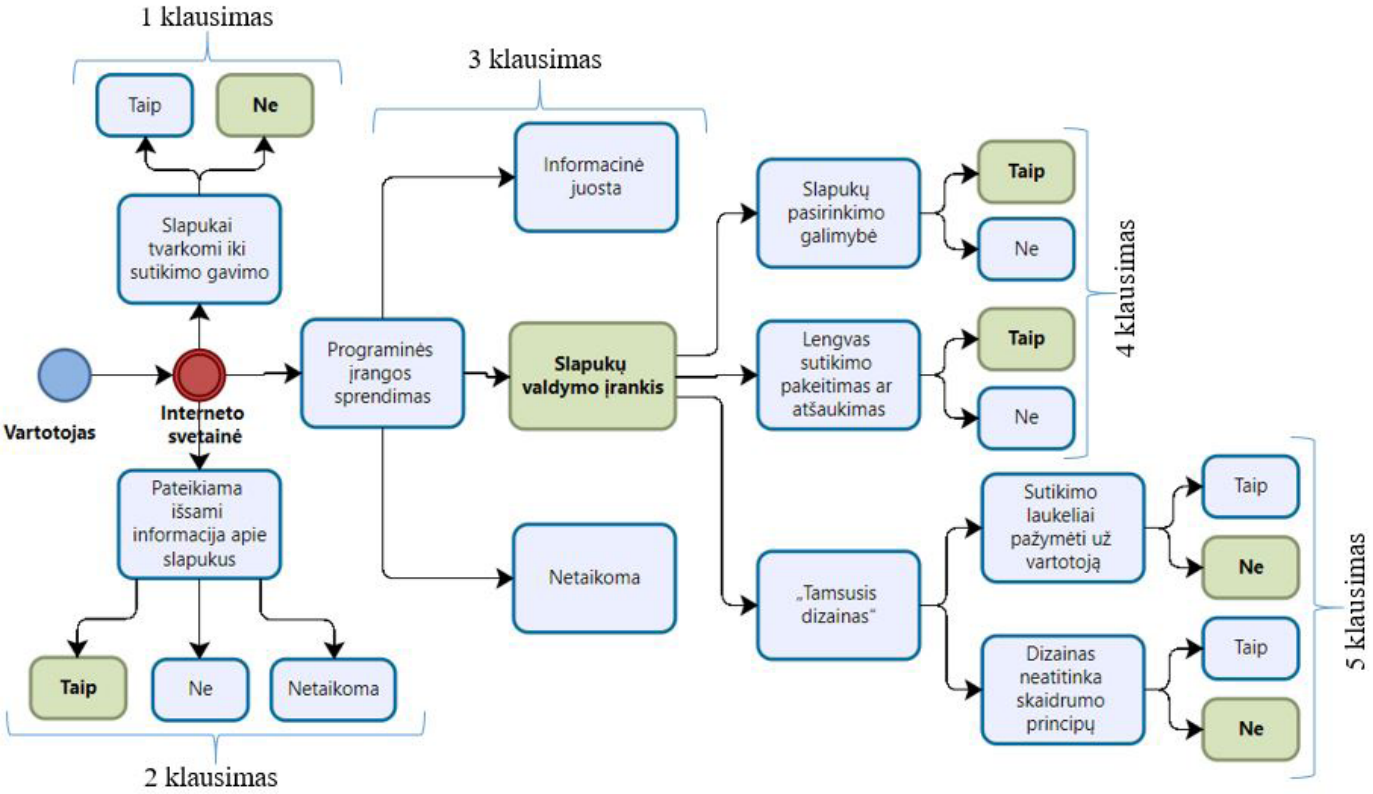
2.1.3. Asmens duomenų tvarkymo teisėtumo nustatymo tyrimas

Pasirinktas atvejo analizės (angl. *Case study*) tyrimo būdas, kai analizuojama vieno arba kelių subjektų, esančių vienoje grupėje, veikla. Analizuojant organizacijų asmens duomenų tvarkymo teisėtumą naudojant slapukus (ang. *Cookies*) internetinėse svetainėse. Pirmasis toks tyrimas kartu su bendraautoriais Limba ir Driauniu buvo atliktas 2020 m. spalio – lapkričio mėnesiais ir publikuotas 2021 metais „*Web of Science*" reitingą turinčiame moksliniame žurnale. Tyrimo metu buvo pasinaudota svetainių reitingavimo įrankiu „*Alexa rank*", kuris naudoja interneto srauto duomenis, kad sudarytų populiariausių interneto svetainių sąrašą. „*Alexa rank*" leidžia žinoti, interneto svetainės populiarumą, palyginus su visomis kitomis interneto svetainėmis (Slivka, 2020). Siekiant nustatyti populiariausias t. y. daugiausiai vartotojų lankomas interneto svetaines Lietuvoje, kurių internetinio adreso domenas yra „*lt*", iš viso „*Alexa rank*" įrankio pagalba buvo atsirinkta 100 interneto svetainių.

Šiame darbe 2022 metų kovo – balandžio mėnesiais buvo tiriamas 100 populiariausių Lietuvos interneto svetainių slapukų naudojimo teisėtumas pagal BDAR reikalavimų atitiktį. Kiekvienos organizacijos interneto svetainė buvo išnagrinėta atskirai, siekiant nustatyti:

1. Ar interneto svetainėje naudojami slapukai teisėtai t. y. prieš pradėdamas tvarkyti asmens duomenis (slapukus) duomenų valdytojas ar tvarkytojas gauna vartotojo sutikimą?
2. Ar interneto svetainės privatumo politikoje pateikiama vartotojui išsami informacija apie slapukų naudojimą, t. y. kokie slapukai naudojami, kokiu tikslu, koks jų saugojimo laikotarpis?
3. Koks programinės įrangos sprendimas naudojamas vartotojų sutikimui gauti slapukams interneto svetainėje naudoti?
4. Ar interneto svetainėje naudojama slapukų valdymo priemonė suteikia vartotojams šias galimybes:
   4.1. Pasirinkti konkrečius slapukus, kurie bus naudojami?
   4.2. Lengvai atšaukti (pakeisti) sutikimus interneto svetainėje naudoti slapukus?
5. Ar slapukų valdymo priemonė turi kurią nors iš šių „*tamsiojo dizaino*“ savybių:
   5.1. Sutikimo su slapukų tvarkymu skilčių laukeliai yra pažymėti iš anksto už vartotoją?
   5.2. Dizainas neatitinka skaidrumo principų t. y. spalvų kontrastas, šrifto dydis, laukų (langelių) išdėstymas ir pan. daro įtaką vartotojo apsisprendimui sutikti naudoti slapukus?

Svarbu pabrėžti, kad interneto svetainėje be vartotojo sutikimo gali būti naudojami tik būtinieji slapukai. Tyrimas susijęs su nebūtinųjų slapukų naudojimu svetainėje, t. y. tokiais, kuriems naudoti yra privalu gauti sutikimą pagal BDAR nuostatų reikalavimus. Sudaryta klausimų ir galimų atsakymų, nustatančių BDAR atitiktį, naudoti slapukus schema (žr. 9 pav.).



9 pav. Klausimų ir galimų atsakymų, nustatančių BDAR atitiktį, schema

Šaltinis: Limba ir kt., 2021

Atitiktis BDAR reikalavimams užtikrinama, jei visi atsakymai, susiję su konkrečia interneto svetaine, schemoje yra paryškinti žalia spalva.

Ši aukščiau aprašyta atvejo tyrimo metodika bus naudojama pakartotinai atlikti tyrimą. Gavus tyrimo empirinius tyrimo duomenis, lyginamosios analizės būdu, šio tyrimo rezultatai bus palyginti su anksčiau atsčiau atlikto tyrimo rezultatais, siekiant nustatyti, kaip pakito BDAR atitikties reikalavimams taikymo praktika organizacijose. Apibendrinus galutines šio tyrimo išvadas, jų pagrindu bus suformuluota dalis klausimų ekspertiniam interviu. Šis empirinis tyrimas (nuo duomenų rinkimo iki išvadų formulavimo proceso) vyko 2022 m. vasario – kovo mėnesiais.

2.1.4. Ekspertų nuomonės vertinimo tyrimas

Interviu metodu siekiama atskleisti tiriamojo reiškinio visumą jo įprastame kontekste bei leidžia tyrėjui įsigilinti į tyrimo dalyvių perspektyvas, surinkti gausius, detales ir unikalius niuansus apčiuopiančius duomenis (Gaižauskaitė, Valavičienė, 2016), todėl gali ne tik identifikuoti esamą situaciją, bet ir paaiškinti jos priežastis. K. Kardelis (2016) išskiria keturis interviu tipus:

1. Struktūrizuotas, klausimus ir visą procedūrą numatant iš anksto, interviu eigoje mažai ką keičiant;
2. Nestruktūrizuotas, be detalaus plano, klausinėjama laisva forma;
3. Neprimestinis, kuomet klausinėjantysis nesistengia išlaikyti numatytos pokalbio linijos, o pasiduodama respondento inicijuotai pokalbio eigai;
4. Kryptingas, ypatingą dėmesį kreipiant į subjektyvius respondento atsakymus apie jam žinomą situaciją, su kuria jis susipažino prieš interviu.

Renkantis elektroninių duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio empirinio tyrimo atlikimo metodą, buvo nuspręsta atlikti ekspertų interviu, kadangi disertaciniame darbe nagrinėjama kibernetinio saugumo ir asmens duomenų apsaugos valdymo tema yra specifinė, reikalaujanti ne tik IT ir vadybos žinių, bet ir teisinio šios temos reglamentavimo aspektų supratimo ir ekspertiškumo. Interviu leidžia suprasti, kaip skirtingų suinteresuotų šalių ekspertai kuria reikšmes remdamiesi autentiška patirtimi (Merriam, 2009). Pusiau struktūrizuoto interviu metu tyrimo dalyviams sudarytos sąlygos laisvai dalyvauti kuriant prasmes - siekiant duomenų analizės metu įvertinti platesnį kontekstą, lanksčiau interpretuoti susidariusią situaciją.

Tyrimo tikslo ir klausimų formulavimas. 2022 m. sudarytas pusiau struktūruotas klausimynas, kurį sudaro dvi dalys:

- Pirmoji dalis (I – III klausimai) remiasi atlikta moksline literatūros analize.
- Antroji dalis (IV – VI klausimai) remiasi empirinių tyrimų gautais rezultatais.

Klausimyne išskirtos pagrindinės tiriamosios dalys ir pagrindiniai klausimai (žr. 3 lentelę). Akcentuotina, kad reaguojant į interviu eigą pritaikyta lanksti klausimyno struktūra, t. y. prisitaikant prie natūralios pokalbio eigos atitinkamai keitėsi klausimų uždavimo tvarka, klausimų formuluotės, įterpti papildomi klausimai. Tyrimo dalyviams suteikta veiksmų laisvė remiantis savo patirtimi pateikti atsakymus. Tyrimo tikslas – sužinoti ekspertų nuomonę apie asmens duomenų apsaugą ir kibernetinį

saugumą bei jo įgyvendinimo problematiką, siekiant sukurti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį, atsižvelgiant į tyrimo metu gautus respondentų atsakymus.

3 lentelė. Pusiau struktūruotas klausimynas

Nr.	**Šaltiniai, kuriais remtasi**	**Tyrimo dalys**	**Pagrindinių interviu klausimų, atitinkančių tyrimo klausimą, formuluotės**
I	Teorinė literatūros analizė	Asmens duomenų apsaugos, kaip reiškinio, teorinis pagrindimas	1. Kokią reikšmę asmens duomenų apsaugos įgyvendinimas turi kibernetiniam saugumui? 2. Kokią įtaką asmens duomenų apsauga turi organizacijai? 3. Kaip tobulintumėte duomenų apsaugos pareigūno funkcijas, siekiant užtikrinti asmens duomenų apsaugą organizacijoje? 4. Kokių veiksmų privalo imtis organizacija, siekdama patobulinti savo valdymo procesus asmens duomenų apsaugos reiškinio kontekste?
II	Teorinė literatūros analizė	Kibernetinio saugumo, kaip reiškinio, teorinis pagrindimas	1. Kokią reikšmę kibernetinio saugumo įgyvendinimas turi asmens duomenų apsaugai? 2. Kokią įtaką organizacijai turi kibernetinio saugumo: • Teisinis reglamentavimas. • Priežiūros institucija (Nacionalinis kibernetinio saugumo centras). • Valdymo procesai. • Kultūra. • Komunikacija. 3. Kaip tobulintumėte informacijos saugos įgaliotinio funkcijas, siekiant užtikrinti kibernetinį saugumą organizacijoje?

III	Teorinė literatūros analizė	Asmens duomenų apsaugos ir kibernetinio saugumo įgyvendinimo problematika	1. Dėl kokių priežasčių daugelis organizacijų turi formaliai apsibrėžę saugos procesus, gaires? 2. Dėl ko kai kurios organizacijos nesilaiko pagrindinių asmens duomenų tvarkymo principų? 3. Kas lemia, kad organizacijos norėdamos užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą daugiau investuoja į technines priemones, o ne į organizacines? 4. Kaip vertinate Valstybinės duomenų apsaugos inspekcijos darbą užtikrinant kontrolę Bendrojo duomenų apsaugos reglamento reikalavimų įgyvendinimo kontekste? 5. Kaip vertinate Nacionalinio kibernetinio saugumo centro darbą užtikrinant kontrolę kibernetinio saugumo reikalavimų įgyvendinimo kontekste?
IV	Dokumentų analizė	Kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymo ir imties nustatymas	1. Kokių techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos įgyvendinimo priemonių pasigendate nacionaliniuose teisės aktuose? 2. Kaip tobulintumėte techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos priemonių įgyvendinimo procesą organizacijoje?
V	Atvejo tyrimas	Informacinių technologijų saugos atitikties vertinimas	1. Kaip užtikrinti nuolatinį kibernetinio saugumo ir asmens duomenų apsaugos dokumentacijos peržiūros ir, esant poreikiui, atnaujinimo procesą? 2. Kokios priežastys lemia, kad kai kurios organizacijos periodiškai neatlieka rizikos ir atitikties vertinimų, kaip būtų galima tobulinti šias priemones? 3. Kaip turėtų būti organizuojamas kibernetinio saugumo ir asmens duomenų apsaugos mokymo procesas organizacijoje? 4. Kaip užtikrinti/kontroliuoti paslaugų teikėjų atitiktį kibernetinio saugumo ir asmens duomenų apsaugos reikalavimams?
VI	Atvejo tyrimas	Asmens duomenų tvarkymo teisėtumo nustatymas	1. Dėl ko daugelis organizacijų neteisėtai tvarko interneto svetainių slapukus (angl. *Cookies*)? 2. Kaip paskatinti organizacijas tvarkyti interneto svetainių slapukus teisėtai?

Šaltinis: sudaryta autoriaus

Disertacinio darbo autoriaus tikslas gauti konkrečios populiacijos tipinės grupės problemos suvokimą ir matymą, siekiant sudaryti kuo tikslesnį specifinio reiškinio charakteristikų vaizdą, todėl buvo pasirinktas ekspertinio vertinimo metodas. Tyrimo imties sudarymo metu pasirinkti ekspertai, kurių žinių ir patirties lygis kibernetinio saugumo ir asmens duomenų srityje neapsiriboja vien tik techninių apsaugos priemonių panaudojimu. Tyrime dalyvaujantys ekspertai turi išmanyti kibernetinio saugumo ir asmens duomenų apsaugos teisinį reglamentavimą bei atitinkamų kontrolės priemonių užtikrinimą, kuris apima, bet neapsiriboja: kibernetinio saugumo politikos ir/ar asmens duomenų apsaugos politikos kūrimu, įgyvendinimu ir kontrole bei tobulinimu atsižvelgiant į organizacijos poreikius; Rizikos vertinimu; Atitikties vertinimu; poveikio duomenų apsaugai vertinimu; kibernetinių saugumo incidentų rizikų valdymu; bendravimu su atitinkamomis institucijomis, tokiomis kaip, VDAI ir NKSC. Taip pat kiekvienas iš respondentų turi turėti mažiausiai penkis metus darbo patirties kibernetinio ir/ar asmens duomenų saugumo srityje.

Toks ekspertų parinkimo metodas užtikrina, kad pasirinkti ekspertai išmanys ne tik kibernetinio saugumo ir asmens duomenų apsaugos teisinę bazę, bet ir organizacinių ir techninių priemonių įgyvendinimo aspektus.

Šios anksčiau išvardytos ekspertų kompetencijos ir praktinio darbo kibernetinio saugumo ir asmens duomenų apsaugos srityje patirtys leidžia manyti, kad atlikto ekspertinio tyrimo rezultatai bus išsamūs ir patikimi, o ekspertų grupės apklausos rezultatai patvirtins kuriamo elektroninių duomenų saugaus valdymo modelio praktinį pritaikomumą. Sudarant ekspertinio tyrimo imtį, buvo vadovaujamasi metodologinėmis prielaidomis, kad gautų įverčių tikslumas pakankamas tuomet, kai ekspertų skaičius svyruoja tarp 5 (penkių) ir 9 (devynių) (Sarantakos, 2004; Rudzkienė, 2005; Augustinaitis ir kt., 2009). Siekiant užtikrinti kuo aukštesnį tyrimo rezultatų patikimumą buvo nuspręsta apklausti ne mažiau nei 9 (devynis) ekspertus, pasinaudojant pusiau struktūrizuoto interviu metodu.

Empirinio tyrimo metu apklausiami kibernetinio saugumo ir asmens duomenų apsaugos ekspertai buvo pasirenkami vadovaujantis patogiosios imties principu – pasirinktas lengviausiai prieinamas, remiantis tyrėjų asmeniniais kontaktais, pagal nustatytus kriterijus. Svarbu pažymėti, kad apklausti 9 ekspertai turi ne tik specifinių kibernetinio saugumo ir asmens duomenų apsaugos srities žinių, bet ir atstovauja skirtingiems sektoriams – tyrime dalyvavo viešojo sektoriaus ir privataus sektoriaus atstovai bei akademinės bendruomenės nariai. Tokia skirtinga 9 ekspertų patirtis kibernetinio saugumo ir asmens duomenų apsaugos užtikrinimo srityje leidžia teigti, kad atlikto empirinio tyrimo duomenys yra patikimi, o empirinio tyrimo metu gautos išvados gali būti naudojamos Lietuvoje ir kitose pasaulio šalyse. Apklausti 9 ekspertai išreiškė norą dalyvauti empiriniame tyrime anonimiškai, neatskleidžiant nei jų tapatybės, nei turimos patirties, nei buvusios ar dabartinės darbovietės. Vadovaujantis tyrimų etikos principais, visiems ekspertams, dalyvavusiems empiriniame tyrime, buvo suteikti identifikatoriai. Ekspertinio vertinimo informacija yra pateikta toliau esančioje lentelėje (žr. 4 lentelę).

4 lentelė. Ekspertų ir interviu informacija

Eksperto identifikatorius	Interviu gavimo data
1E	2022-06-30
2E	2022-07-26
3E	2022-08-05
4E	2022-09-14
5E	2022-11-26
6E	2022 12 07
7E	2022 12 08
8E	2022 02 15
9E	2023-01-05

Šaltinis: sudaryta autoriaus

Ekspertams elektroniniu paštu buvo pateiktas struktūrizuotas klausimynas apie kibernetinio saugumo ir asmens duomenų apsaugos priemones, kuriomis siekiama užtikrinti saugų asmens duomenų elektroninėje erdvėje valdymą ir buvo prašoma pateikti išsamius atsakymus.

Tyrimo etika. Tyrimo metu buvo skiriamas dėmesys tyrėjo elgesio su tiriamaisiais etikai. Tyrime vadovautasi socialiniuose tyrimuose deklaruojamais etikos principais: dalyvavimo savanoriškumo, suteikiant visapusę informaciją apie tyrimą, nepažeisti respondentų privatumo (Bryman, Bell, 2007; Babbie, 2007).

Interviu metu klausimai buvo suformuoti taip, kad jie atskleistų tiriamųjų požiūrį į tyrimo objektą, o ne primestų kitą požiūrį, ar klaidintų. Buvo užtikrintas respondentų atsakymų konfidencialumas, disertaciniame darbe pateikiant tyrime dalyvaujančių respondentų charakteristikas, tačiau nenurodant jų atsakymų autorystės. Bet koks panašios informacijos platinimas be tiriamųjų sutikimo, pažeidžia privatumo principą, todėl negali būti leistinas. Siekiant objektyvios pateiktų duomenų analizės bei pagarbos asmens privatumui, respondentų pateikta informacija apie trečius asmenis, jų asmenines savybes bei charakteristikas disertaciniame darbe nebuvo pateikiama ir analizuojama.

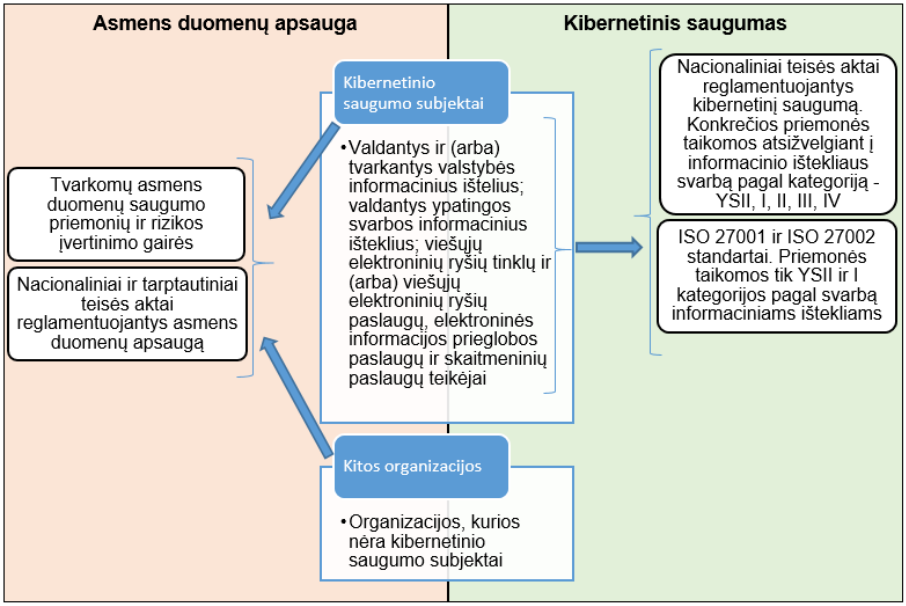
3. ASMENS DUOMENŲ SAUGOS VALDYMO ELEKTRONINĖJE ERDVĖJE PRIEMONIŲ TAIKYMO REZULTATAI

3.1. Kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymo ir imties rezultatai

Organizacijos norėdamos užtikrinti kibernetinį saugumą ir asmens duomenų apsaugą taiko įvairias priemones. Taikomos priemonės yra pateikiamos tarptautiniuose teisės aktuose, standartuose, atsakingų institucijų gairėse (žr. 2 priedas). Kibernetinės atakos klesti, tą patvirtina tarptautinės ir nacionalinės kibernetinio saugumo institucijos (ENISA, 2021; NKSC, 2021), ir sąmoningumo lygis apie būtinybę įgyvendinti atsakomąsias priemones visapusiškai išaugo (Al-Sartawi, 2020). Nors teisės aktai padeda apsaugoti asmens duomenis ir kompiuterių išteklius, jie žymiai padidino atitikties naštą ir organizacijų kibernetinių investicijų išlaidas (Lee, 2021).

Kibernetinio saugumo subjektai privalo naudoti kibernetinį saugumą užtikrinančias priemones, kurios įtvirtintos LR teisės aktuose, standartuose ISO 27001 ir ISO 27002 bei asmens duomenų apsaugos priemones, kurios nurodytos BDAR ir VDAI gairėse. Organizacijos kurios nėra kibernetinio saugumo subjektai t. y. nėra subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, nėra ypatingos svarbos informacinės infrastruktūros valdytojai, nėra viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjai neprivalo naudoti kibernetinį saugumą užtikrinančių priemonių, kurios nurodytos LR teisės aktuose, tačiau privalo naudoti priemones, kurios užtikrintų asmens duomenų saugumą pagal Reglamentą, kokios tai bus priemonės privalo įsivertinti pati organizacija (žr. 10 pav.).

Kibernetinio saugumo subjektai atlikę Atitikties vertinimą, turi jį pateikti ARSIS – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistema. ARSIS tikslas – automatiniu būdu vykdyti valstybės informacinių išteklių atitikties nustatytiems elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėseną.



10 pav. Kibernetinio saugumo ir asmens duomenų apsaugos taikymo imtis Lietuvoje

Šaltinis: sudaryta autoriaus

Apibendrinant galima teigti, kad tam tikri skirtinguose teisės aktuose ir standartuose ISO 27001 ir ISO 27002 bei VDAI gairėse išdėstyti reikalavimai kibernetiniam saugumui ir asmens duomenų apsaugai užtikrinti yra tapatūs, o tai apsunkina saugumo reikalavimų įgyvendinimą organizacijoms. Kibernetinio saugumo subjektai Atitikties vertimą privalo atlikti kiekvienais metais ir jo rezultatus pateikti NKSC įkeldami į ARSIS, o už šios prievolės nevykdymą gresia atsakomybė. Tuo tarpu organizacijos, kurios nėra kibernetinio saugumo subjektai, to daryti neprivalo, nes Atitikties vertinimo rezultatų pateikimas NKSC nėra reglamentuotas ir NKSC nevykdo šių organizacijų kibernetinio saugumo reikalavimų įgyvendinimo stebėsenos. Tačiau visos organizacijos privalo užtikrinti atitiktį Reglamentui, kuris įpareigoja taikyti tinkamas technines ir organizacines apsaugos priemones, ir ją įrodyti VDAI.

3.2. Informacinių technologijų saugos atitikties vertinimo rezultatai

Atitikties vertinimo metu buvo įvertintas trijų organizacijų kibernetinio saugumo ir asmens duomenų apsaugos reglamentavimas vidaus teisės aktuose ir faktinis jų įgyvendinimas praktikoje. Įgyvendinimo lygis saugumo reikalavimams įvertintas pagal penkių balų skalę, kurioje žemiausia reikšmė yra 1 (vienetas), o aukščiausia – 5 (penketas). Dėl didelės tyrimo imties pateikiami apibendrinti rezultatai, įvertinti nuo 1 (vieneto) iki 3 (trejeto), kurie sutampa visose trijose organizacijose. Detali metodika parašyta disertacijos skyriuje „*2.2.2 Informacinių technologijų saugos atitikties*

vertinimo tyrimas“.

Atitikties vertinimo tikslas nustatyti neatitiktis ir pateikti rekomendacijas nustatytų trūkumų pašalinimui. Kadangi trijų organizacijų Atitikties vertinimo imtis yra didelė, todėl rezultatai bus pateikiami tik tų nustatytų neatitikčių kurios įvertintos 3 (trejetu) ir mažiau visose trijose organizacijose, o ne kiekvienoje atskirai.

Žemiau yra pateikiami apibendrinti tyrimo rezultatai, nurodant trijų organizacijų, konkretiems teisės akto, standarto ar gairių reikalavimams, nustatytas neatitiktis ir jų įverčius:

1. Įvertinus tris organizacijas pagal Bendrųjų elektroninės informacijos saugos reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „*Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo*“ reikalavimus buvo nustatytos 4 neatitiktys įvertintos trejetu t.y. saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant:
   - Dokumentai reglamentuojantys kibernetinį saugumą ir asmens duomenų apsaugą yra neatnaujinti.
   - Periodiškai neatliekami rizikos vertinimai.
   - Periodiškai neatliekami Atitikties vertinimai.
   - Neorganizuojami periodiniai mokymai.
2. Įvertinus tris organizacijas pagal Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „*Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo*“ reikalavimus buvo nustatytos 5 neatitiktys įvertintos trejetu t. y. saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant:
   - Periodiškai neatliekami rizikos vertinimai.
   - Periodiškai neatliekami Atitikties vertinimai.
   - Veiklos tęstinumo valdymo ar kibernetinių incidentų valdymo planai yra neišbandomi praktikoje.
   - Kibernetinio saugumo politikos dokumentai neatnaujinami.
   - Sąlygos, dėl atitikties kibernetinio saugumo reikalavimams, su paslaugų tiekėjais nepakankamai reglamentuotos ir neužtikrinama jų kontrolė.
3. Įvertinus tris organizacijas pagal Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašą, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „*Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo*

metodikos patvirtinimo“ reikalavimus buvo nustatytos 2 neatitiktys įvertintos trejetu t. y. saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant:
   - Periodiškai neatliekami Atitikties vertinimai.
   - Periodiškai neatliekami rizikos vertinimai.
4. Įvertinus tris organizacijas pagal standarto ISO 27001 „*Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos*“ reikalavimus buvo nustatytos 3 neatitiktys įvertintos trejetu t. y. saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant:
   - Dokumentai reglamentuojantys kibernetinį saugumą ir asmens duomenų apsaugą yra neatnaujinti.
   - Periodiškai neatliekami rizikos vertinimai.
   - Periodiškai neatliekami Atitikties vertinimai.
5. Įvertinus tris organizacijas pagal standarto ISO 27002 „*Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai*“ reikalavimus buvo nustatytos 5 neatitiktys įvertintos trejetu t. y. saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant:
   - Dokumentai reglamentuojantys kibernetinį saugumą ir asmens duomenų apsaugą yra neatnaujinti.
   - Neorganizuojami periodiniai mokymai.
   - Sąlygos, dėl atitikties kibernetinio saugumo reikalavimams, su paslaugų tiekėjais nepakankamai reglamentuotos ir neužtikrinamą jų kontrolė.
   - Veiklos tęstinumo valdymo planas neišbandomas praktikoje.
   - Periodiškai neatliekami Atitikties vertinimai.
6. Įvertinus tris organizacijas pagal VDAI parengtas gairės „*Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*“ (3 versija, 2020-06-18) reikalavimus buvo nustatytos 4 neatitiktys įvertintos trejetu t. y. saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant:
   - Dokumentai reglamentuojantys asmens duomenų saugumo politiką ir procedūros neparengti, pilna apimtimi, arba neatnaujinti.
   - Duomenų tvarkytojai. Sąlygos, dėl atitikties kibernetinio saugumo (asmens duomenų apsaugos) reikalavimams, su paslaugų tiekėjais nepakankamai reglamentuotos ir neužtikrinama jų kontrolė.
   - Neatliekamas veiklos tęstinumo valdymo plano išbandymas.
   - Neorganizuojami periodiniai mokymai ir IS naudotojai nesupažindinami su saugos dokumentais.
7. Įvertinus tris organizacijas pagal Bendrojo duomenų apsaugos reglamento reikalavimus buvo nustatytos 4 neatitiktys įvertintos trejetu t. y. saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant:

- Dokumentai reglamentuojantys kibernetinį saugumą ir asmens duomenų apsaugą yra neatnaujinti.
- Periodiškai neatliekami rizikos vertinimai.
- Periodiškai neatliekami Atitikties vertinimai.
- Neorganizuojami periodiniai mokymai.

Atitikties vertinimo metu įvertinus trijų organizacijų atitiktį kibernetinio saugumo ir asmens duomenų apsaugos reikalavimams buvo nustatytos 27 neatitiktys (6 skirtingos neatitiktys), kurios sutampa visose trijose organizacijose ir yra įvertintos 3 balais – saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant. Atitikties vertinimo metu nustatytų neatitikčių suvestinė (žr. 5 lentelę).

5 lentelė. Atitikties vertinimo nustatytų neatitikčių suvestinė

Nr.	Vertinimas / Nustatytos neatitiktys	1. IS atitikties bendriesiems elektroninės informacijos saugos reikalavimams	2. IS atitikties techniniams kibernetinio saugumo reikalavimams	3. IS atitikties techniniams elektroninės informacijos saugos reikalavimams	4. ISO 27001 reikalavimams	5. ISO 27002 reikalavimams	6. VDAI parengtų gairių reikalavimams	7. Bendrojo duomenų apsaugos reglamento reikalavimams
1.	Neatnaujinta dokumentacija	**x**	**x**		**x**	**x**	**x**	**x**
2.	Periodiškai neatliekamas rizikos vertinimas	**x**	**x**	**x**	**x**			**x**
3.	Periodiškai neatliekamas Atitikties vertinimas	**x**	**x**	**x**	**x**	**x**		**x**
4.	Neorganizuojami periodiniai mokymai	**x**				**x**	**x**	**x**
5.	Netinkama paslaugų teikėjų kontrolė		**x**			**x**	**x**	
6.	Periodiškai neatliekamas veiklos tęstinumo valdymo plano išbandymas		**x**			**x**	**x**	

Šaltinis: sudaryta autoriaus pagal informacinių technologijų saugos atitikties vertinimo rezultatus

Rekomenduotini veiksmai pašalinti nustatytas neatitiktis:

1. *Saugos dokumentus persvarstyti (peržiūrėti) ne rečiau kaip kartą per metus arba po esminių pokyčių organizacijoje*. Kiekviena organizacija įsivertina, kibernetinio saugumo ir asmens duomenų apsaugos, vidaus dokumentų poreikį individualiai pagal veiklos pobūdį, išskyrus organizacijas valdančias ir/ar tvarkančias valstybės IS, kurios privalo turėti, su NKSC suderintus, šiuos dokumentus – IS duomenų saugos nuostatus; Saugaus elektroninės informacijos tvarkymo taisykles; IS veiklos tęstinumo valdymo planą; IS naudotojų administravimo taisykles.
2. Kartą per metus atlikti rizikos vertinimą. Atsižvelgus į rizikos įvertinimo ataskaitą, patvirtinti rizikos valdymo priemonių planą. Šie dokumentai ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti ARSIS (taikoma kibernetinio saugumo subjektams valdantiems valstybės informacinius išteklius).
3. Kartą per metus atlikti Atitikties vertinimą. Atlikus Atitikties vertinimą, parengti Atitikties vertinimo ataskaitą ir pastebėtų trūkumų šalinimo planą. Atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo planas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateiktas ARSIS (taikoma kibernetinio saugumo subjektams valdantiems valstybės informacinius išteklius).
4. Organizuoti kibernetinio saugumo ir asmens duomenų apsaugos periodinius mokymus. Mokymų turinį ir formą gali pasirinkti organizacija.
5. Saugos dokumentuose ir sutartyse su paslaugų tiekėjais reglamentuoti sąlygas dėl atitikties kibernetinio saugumo reikalavimams ir vykdyti tiesioginę jų kontrolę, pvz. pateikti audito rezultatus, informuoti apie įvykusius incidentus, laiku reaguoti į paslaugos teikimo sutrikimus.
6. Periodiškai atlikti Veiklos tęstinumo valdymo plano išbandymą praktikoje. Organizacija turėtų sugalvoti kibernetinio incidento scenarijų ir pratybų metu patikrinti, kaip jis valdomas.

3.3. Asmens duomenų tvarkymo teisėtumo nustatymo tyrimo rezultatai

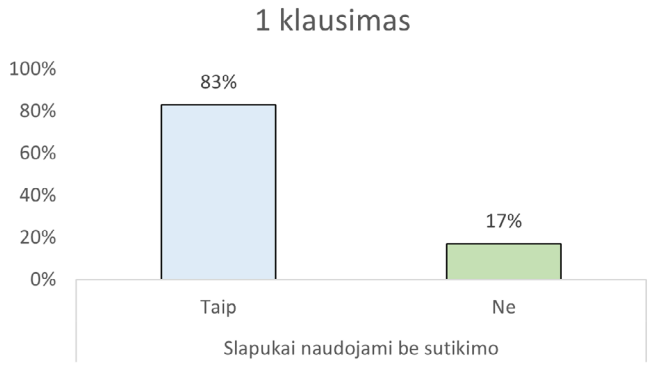
Duomenų valdytojas turi užtikrinti, kad interneto svetainėje būtų pateikta išsami informacija apie slapukų (angl. *Cookies*) tvarkymą, įskaitant slapukų pavadinimą, jų naudojimo tikslą ir saugojimo laikotarpį. Be to, slapukai negali būti naudojami, kol negaunamas vartotojo sutikimas. Slapukų valdymo priemonė turi neturėti jokių savybių ir funkcionalumų, susijusių su „*tamsiuoju dizainu*“, kadangi jis pažeidžia BDAR skaidrumo principą ir neigiamai veikia vartotojo pasirinkimo laisvę išreikšti sutikimą tvarkyti slapukus. Detali šio tyrimo metodika aprašyta disertacijos skyriuje „*2.2.3 Asmens duomenų tvarkymo teisėtumo nustatymo tyrimas*“.

Šio tyrimo metu buvo išanalizuota 100 populiariausių Lietuvos interneto svetainių. Tai naujienų ir skelbimų portalų, mokymo įstaigų, bankų, įvairių elektroninių parduotuvių, kelionių agentūrų, mobiliojo ryšio tiekėjų, valstybinių įmonių interneto

svetainės. Išanalizavus 100 populiariausių Lietuvos interneto svetainių slapukų valdymo ypatumus, siekiant nustatyti organizacijų asmens duomenų tvarkymo teisėtumą BDAR reikalavimams, gauti tokie rezultatai:

1 klausimas. Ar interneto svetainėje naudojami slapukai teisėtai t. y. prieš pradėdamas tvarkyti asmens duomenis (slapukus) duomenų valdytojas ar tvarkytojas gauna vartotojo sutikimą?

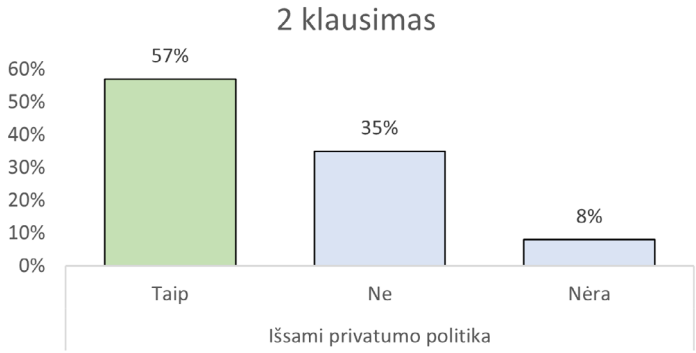
Rezultatas. Interneto svetainės, kuriose nebuvo slapukų valdymo įrankio arba buvo naudojama slapukų informacijos juosta, kuri nesuteikia galimybės atsisakyti slapukų, *de facto* buvo traktuojama slapukų naudojimu negavus vartotojo sutikimo. Buvo vertinamos interneto svetainės, kuriose įdiegtas slapukų valdymo įrankis leidžiantis aktyviai valdyti slapukus, stebint slapukų skaičiaus pasikeitimą prieš ir po vartotojui pareiškiant savo valią tvarkyti slapukus. Nustatyta, kad net 83 proc. interneto svetainių buvo naudojami slapukai be vartotojo sutikimo, pažeidžiant BDAR, ir tik 17 proc. interneto svetainių asmens duomenys buvo naudojami teisėtai t. y. gavus vartotojo sutikimą (žr. 11 pav.).



11 pav. Neteisėtas slapukų naudojimas svetainėse be vartotojo sutikimo
Šaltinis: sudaryta autoriaus

2 klausimas. Ar interneto svetainės privatumo politikoje pateikiama vartotojui išsami informacija apie slapukų naudojimą, t. y. kokie slapukai naudojami, kokiu tikslu, koks jų saugojimo laikotarpis?

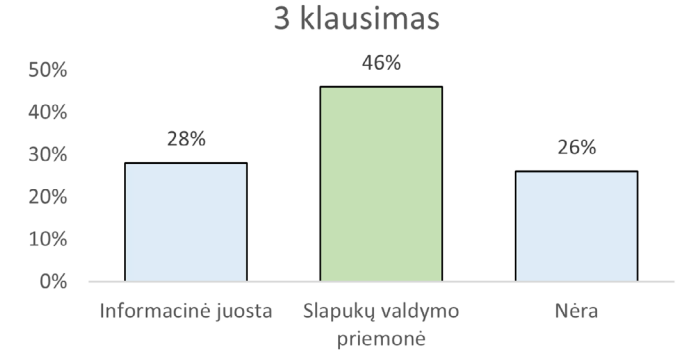
Rezultatas. Interneto svetainėse buvo atliekama privatumo politikos turinio analizė, siekiant nustatyti, kokia informacija pateikta apie slapukų tvarkymą – slapukų pavadinimai, slapukų tvarkymo tikslai ir saugojimo laikotarpis. Nustatyta, kad 57 proc. interneto svetainių turi privatumo politiką, kurioje buvo pateikta išsami informacija apie slapukų tvarkymą, o likusios svetainės nepateikė reikiamos informacijos apie slapukų valdymą: 35 proc. šių interneto svetainių pateikė informaciją, kuri nebuvo pakankamai išsami, o 8 proc. išvis nepateikė jokios informacijos apie slapukų tvarkymą, nes neturėjo privatumo politikos (žr. 12 pav.).



12 pav. Išsami informacija apie slapukų tvarkymą svetainėse
Šaltinis: sudaryta autoriaus

3 klausimas. Koks programinės įrangos sprendimas naudojamas vartotojų sutikimui gauti slapukams interneto svetainėje naudoti?

Rezultatas. Remiantis BDAR, organizacija norėdama naudoti slapukus interneto svetainėje privalo gauti aktyvų vartotojo sutikimą. Nustatyta, kad 28 proc. interneto svetainių buvo naudojama informacinė juosta, kuri nesuteikdavo galimybės vartotojams valdyti slapukų, 26 proc. interneto svetainių nebuvo nei informuojama, nei prašoma išreikšti sutikimą tvarkyti slapukus. Slapukų valdymo priemonė, kuri leido vartotojams aktyviais veiksmais sutikti arba atsisakyti su slapukų tvarkymu buvo naudojama 46 proc. interneto svetainių (žr. 13 pav.).



13 pav. Programinės įrangos sprendimas (priemonė) vartotojų sutikimui gauti
Šaltinis: sudaryta autoriaus

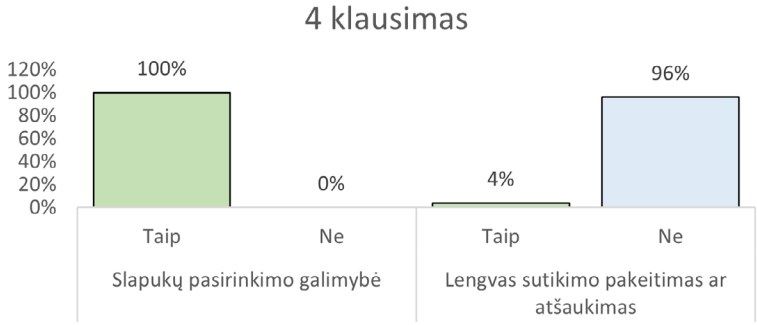
4 klausimas. Ar interneto svetainėje naudojama slapukų valdymo priemonė suteikia vartotojams šias galimybes:

4.1 Pasirinkti konkrečius slapukus, kurie bus naudojami?

4.2 Lengvai atšaukti (pakeisti) sutikimus interneto svetainėje naudoti slapukus?

Rezultatas: Išanalizavus 46 interneto svetaines, kurios turi slapukų valdymo

priemonę suteikiančią vartotojams aktyviais veiksmais valdyti slapukus, nustatyta, kad 100 proc. šių interneto svetainių suteikė galimybę pasirinkti konkrečius slapukus, kurie gali būti tvarkomi. Tik 4 proc. interneto svetainių buvo galimybė lengvai atšaukti (pakeisti) sutikimus naudoti slapukus, o 96 proc. interneto svetainių tokia galimybė vartotojams nebuvo suteikta (žr. 14 pav.).



14 pav. Vartotojų galimybės valdyti slapukus

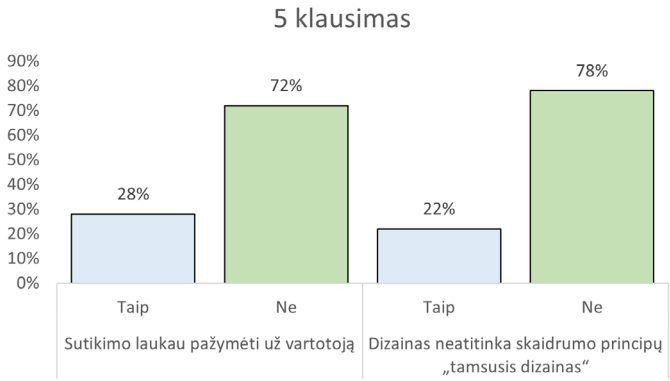
Šaltinis: sudaryta autoriaus

5 klausimas . Ar slapukų valdymo priemonė turi kurią nors iš šių „tamsiojo dizaino" savybių:

5.1. Sutikimo su slapukų tvarkymu skilčių laukeliai yra pažymėti iš anksto už vartotoją?

5.2. Dizainas neatitinka skaidrumo principų t. y. spalvų kontrastas, šrifto dydis, laukų (langelių) išdėstymas ir pan. daro įtaką vartotojo apsisprendimui sutikti naudoti slapukus?

Rezultatas: Išanalizavus 46 interneto svetaines, kurios turi slapukų valdymo priemonę suteikiančią vartotojams aktyviais veiksmais valdyti slapukus, nustatyta, kad 28 proc. interneto svetainių slapukų valdymo priemonių sutikimo su slapukų tvarkymu skilčių laukeliai yra pažymėti iš anksto už vartotoją, o 72 proc. – ne. Interneto svetainių 78 proc. slapukų valdymo priemonių buvo neutralaus dizaino, kuris suteikė galimybę išlaikyti tinkamą pusiausvyrą, t. y. nedarė įtakos vartotojui sutikti su slapukų tvarkymu. „Tamsusis dizainas" buvo naudojamas 22 proc. interneto svetainių, pažeidžiant BDAR skaidrumo principą (žr. 15 pav.).



15 pav. „*Tamsiojo dizaino*“ naudojimas slapukų sutikimams gauti
Šaltinis: sudaryta autoriaus

Tyrimo rezultatų apibendrinimas. Atlikus asmens duomenų tvarkymo teisėtumo nustatymo tyrimą galima teigti:

1. kad didžioji dauguma organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), nesilaiko BDAR reikalavimų, nes 83 proc. interneto svetainių slapukai buvo naudojami be vartotojo sutikimo, tai lėmė dvi priežastys: pirmoji – interneto svetainėse nebuvo naudojamas slapukų valdymo priemonė, kuri būtų galėjusi suteikti galimybę vartotojams valdyti slapukus, t. y. aktyviais veiksmais išreikšti sutikimą leisti arba neleisti tvarkyti slapukus; antroji – interneto svetainėse buvo naudojama slapukų valdymo priemonė, tačiau ji buvo fiktyvi, nes vartotojui nesutikus su slapukų tvarkymu, jie vis tiek buvo naudojami svetainėje.
2. kad daugiau nei pusė organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), laikosi BDAR reikalavimų, nes 57 proc. interneto svetainių buvo pateikiama privatumo politika, kurioje išsamiai aprašytas slapukų tvarkymas – kokie slapukai naudojami, kokiu tikslu, koks jų saugojimo laikotarpis.
3. kad mažiau nei pusė organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), laikosi BDAR reikalavimų, nes 46 proc. interneto svetainių buvo naudojama slapukų valdymo priemonė, kuri leidžia vartotojams aktyviais veiksmais sutikti arba atsisakyti su slapukų tvarkymu.
4. kad beveik absoliuti dauguma organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), nesilaiko BDAR reikalavimų, 96 proc. interneto svetainių buvo naudojama slapukų valdymo priemonė, kuri nesuteikė galimybės lengvai atšaukti (pakeisti) sutikimus naudoti slapukus. Remiantis BDAR reikalavimais, sutikimą turėtų būti taip pat lengva duoti, kaip ir atšaukti.
5. kad didžioji dauguma organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), laikosi BDAR reikalavimų, nes 78 proc. interneto svetainių buvo naudojama slapukų valdymo priemonė, kuri nenaudoja „*tamsiojo dizaino*“, kuriuo siekiama įtakoti vartotojų apsisprendimą sutikti su slapukų tvarkymu, o

72 proc. interneto svetainių buvo naudojama slapukų valdymo priemonė, kurios sutikimo su slapukų tvarkymu skilčių laukeliai nėra pažymėti iš anksto už vartotoją.

Analizuojant organizacijų asmens duomenų tvarkymo teisėtumą naudojant slapukus, pirmasis tyrimas katu su bendraautoriais T. Limba ir K. Driauniu buvo atliktas 2020 m. spalio – lapkričio mėnesiais ir publikuotas 2021 metais „*Web of Science*“ reitingą turinčiame moksliniame žurnale. Žemiau yra pateikiama 2020 metų ir 2022 metų atlikto tyrimo rezultatų suvestinė (žr. 6 lentelę).

6 lentelė. Slapukų tvarkymo 2020 metų ir 2022 metų atlikto tyrimo rezultatų suvestinė

Klausimo Nr.	**Tyrimų rezultatai procentine išraiška**		**Rezultato paaiškinimas**
	2020 metai	**2022 metai**	
1	92	83	Interneto svetainėse buvo naudojami slapukai be vartotojo sutikimo.
	8	17	Interneto svetainėse buvo naudojami slapukai teisėtai t. y. gavus sutikimą prieš juos pradedant naudoti.
2	60	57	Interneto svetainėse buvo privatumo politika, kurioje pateikta išsami informacija apie slapukų naudojimą.
	28	35	Interneto svetainėse buvo privatumo politika, kurioje pateikta informacija apie slapukų tvarkymą nebuvo pakankamai išsami.
	12	8	Interneto svetainėse nebuvo pateikta jokios informacijos apie duomenų tvarkymą, įskaitant slapukų tvarkymą.
3	45	28	Interneto svetainėse buvo naudoja informacinė juosta (angl. Banner), kuri nesuteikė vartotojams galimybės išreikšti savo valią, nesutikti su slapukų tvarkymu.
	27	26	Interneto svetainėse nebuvo naudojamas programinės įrangos sprendimas vartotojų sutikimams gauti, siekiant teisėtai pagal BDAR reikalavimus tvarkyti slapukus.
	28	46	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kuri leido vartotojams aktyviais veiksmais sutikti arba nesutikti su slapukų tvarkymu.

4	96	100	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kuri vartotojams suteikė galimybę pasirinkti konkrečius slapukus, kurie bus tvarkomi.
	4	0	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kuri vartotojams nesuteikė galimybės pasirinkti konkrečių slapukų, kurie bus tvarkomi.
	7	4	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kuri vartotojams suteikė galimybę lengvai atšaukti (pakeisti) sutikimą naudoti slapukus.
	93	96	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kuri vartotojams nesuteikė galimybės lengvai atšaukti (pakeisti) sutikimą naudoti slapukus.
5	36	28	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kurioje sutikimo su slapukų tvarkymu skilčių laukeliai buvo pažymėti iš anksto už vartotoją.
	64	72	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kurioje sutikimo su slapukų tvarkymu skilčių laukeliai nebuvo pažymėti iš anksto už vartotoją.
	72	78	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kurioje buvo neutralus dizainas, kuris suteikė galimybę išlaikyti tinkamą pusiausvyrą, t. y. nedarė įtakos vartotojui sutikti su slapukų tvarkymu.
	28	22	Interneto svetainėse buvo naudojama slapukų valdymo priemonė, kurioje buvo „tamsusis dizainas“, kuris pažeidžia BDAR skaidrumo principą, nes daro įtaką vartotojo apsisprendimui sutikti su slapukų tvarkymu.

Šaltinis: Limba ir kt, 2021; ir autoriaus asmens duomenų tvarkymo teisėtumo nustatymo tyrimo rezultatai

Lyginamosios analizės rezultatų apibendrinimas. Atlikus asmens duomenų tvarkymo teisėtumo nustatymo tyrimą 2020 ir 2022 metais galima teigti:

1. kad įvyko nežymus teigiamas pasikeitimas, nuo 8 proc. iki 17 proc., daugiau organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), interneto svetainėse naudojo slapukus teisėtai t. y. gavus sutikimą prieš juos pradedant naudoti.
2. kad įvyko žymus teigiamas pasikeitimas, nuo 28 proc. iki 46 proc., daugiau organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), interneto svetainėse naudojo slapukų valdymo priemonę, kuri leidžia vartotojams aktyviais veiksmais sutikti arba atsisakyti su slapukų tvarkymu.
3. kad neįvyko kitų esminių teigiamų pasikeitimų, o tik labai nežymūs, organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), interneto svetainėse – pateikiama detali informacija apie slapukų tvarkymą, galimybė lengvai atšaukti (pakeisti) sutikimą naudoti slapukus, nepažymėti slapukų valdymo

priemonėje sutikimo su slapukų tvarkymu skilčių laukeliai, neutralus slapukų valdymo priemonės dizainas.

Apibendrinat galima teigti, kad neskiriamas pakankamas dėmesys interneto svetainių slapukų tvarkymo teisėtumui užtikrinti. Atlikto tyrimo metu nustatyta, kad didžioji dauguma organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), nesilaiko BDAR reikalavimų ir slapukus interneto svetainėse naudoja neteisėtai, t. y. be vartotojų sutikimo. Organizacijos, norėdamos užtikrinti teisėtą duomenų (slapukų) tvarkymą interneto svetainėse, turėtų turėti tinkamą įrankį, kuris vartotojams suteiktų galimybę aktyviais veiksmais sutikti arba nesutikti su atitinkamų slapukų tvarkymu bei bet kada pakeisti apsisprendimą. Šis įrankis turėtų neturėti „*tamsiojo dizaino*" požymių t. y. iš anksto pažymėtų langelių, spalvų ir šrifto, kuris skatintų vartotojus sutikti su slapukų tvarkymu. Visa informacija susijusi su slapukų tvarkymu t. y. kokie slapukai naudojami, kokiu tikslu naudojami, koks jų saugojimo laikotarpis turėtų būti pateikiama vartotojui interneto svetainės privatumo politikoje.

3.4. Ekspertų nuomonės vertinimo tyrimo rezultatai

Atlikus asmens duomenų apsaugos ir kibernetinio saugumą bei jo įgyvendinimo problematikos tyrimą, buvo susisteminti ekspertinio tyrimo metu gauti rezultatai. Ekspertų atsakymai ir pastabos suteikė disertacijos autoriui galimybę sukurti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį ir pateikti tam tikras modelio įgyvendinimo rekomendacijas organizacijoms, kurios nuspręs pasinaudoti šiuo asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modeliu, siekiant sumažinti asmens duomenų apsaugos ir kibernetinio saugumo rizikas.

Žemiau pateikiami ekspertų apibendrinti asmens duomenų apsaugos ir kibernetinio saugumo bei jo įgyvendinimo problematikos empirinio tyrimo rezultatai.

Pusiau struktūruoto klausimyno **I tyrimo dalį – Asmens duomenų apsaugos, kaip reiškinio, teorinis pagrindimas**, sudaro 4 klausimai.

1. Kokią reikšmę asmens duomenų apsaugos įgyvendinimas turi kibernetiniam saugumui? Atsakydami į klausimą 1E ir 5E ekspertai nurodė, kad asmens duomenų apsauga sumažina kibernetinio pažeidžiamumo riziką ir didina kibernetinį atsparumą. 2E, 3E,4E, 6E, 8E ir 9E ekspertai, mano kad tarp asmens duomenų apsaugos ir kibernetinio saugumo yra sinergija. Tiek asmens duomenų apsaugai, tiek kibernetiniam saugumui užtikrinti naudojamos organizacinės ir techninės priemonės (žr. 7 lentelę).

7 lentelė. Asmens duomenų apsaugos reikšmė kibernetinio saugumo įgyvendinimui

Interviu ištrauka	Subkategorija	Kategorija
„*Asmens duomenų apsauga **sumažina kibernetinio pažeidžiamumo riziką** panaudoti netinkamai saugomus duomenis. <...> duomenų pobūdžio specialiųjų apsaugos priemonių tinkamas įgyvendinimas **didina naudotojų sąmoningumą ir kibernetinį atsparumą**.*“ (1E, asmeninis interviu, 2022-06-30).	Sumažinta kibernetinio pažeidžiamumo rizika ir didesnis kibernetinis atsparumas	Asmens duomenų apsaugos reikšmė kibernetinio saugumo įgyvendinimui
„*Tinkamas asmens duomenų tvarkymas gali **mažinti** tvarkomų asmens duomenų kiekius, kurie gali būti kibernetinės atakos objektas.*“ (5E, asmeninis interviu, 2022-11-25).		
„***Kibernetinis saugumas yra neatsiejamas nuo asmens duomenų apsaugos**, nes daugelis priemonių remiasi įvairiomis **organizacinėmis ir techninėmis kibernetinio saugumo rizikų tvarkymo kontrolėmis**.*“ (2E, asmeninis interviu, 2022-07-26).	Asmens duomenų apsaugos ir kibernetinio saugumo sinergija bei taikomos organizacinės ir techninės priemonės	
„*... asmens duomenų valdytojas turi įgyvendinti **organizacines ir technines saugumo priemones**, kitaip tariant, įgyvendinti kibernetinio saugumo priemones. Taigi, **asmens duomenų apsaugos užtikrinimas - kibernetinio saugumo užtikrinimas** toje duomenų apimtyje, kiek jie gali būti vertinami kaip asmens duomenys.*“ (3E, asmeninis interviu, 2022-08-05).		
„*Pagrindinė kibernetinio saugumo funkcija - užkirsti kelią neteisėtai prieigai prie didžiulio kiekio asmeninės informacijos, kurią dabar saugome visur naudojamuose įrenginiuose <...> **Asmens duomenų apsaugos įgyvendinimas yra neatsiejama kibernetinio saugumo dalis**.*“ (4E, asmeninis interviu, 2022-09-14).		
„*... **asmens duomenų ir kibernetinis saugumas yra tarpusavyje susiję procesai**: numatant asmens duomenų **apsaugos priemones** <...>, naudojantis **informacinių technologijų priemonėmis ir įranga**, tuo pačiu gali būti užtikrinamas ir kibernetinis saugumas.*“ (6E, asmeninis interviu, 2022-12-07).		
„*Asmens duomenų apsaugos įgyvendinimas įgalina valdytoją įvertinti ar informacijos saugumo, įskaitant kibernetinį saugumą, **priemonės**, taikomos informacijos, įskaitant asmens duomenis, **saugumui užtikrinti yra pakankamos ir yra proporcingos**.*“ (8E, asmeninis interviu, 2022-12-15).		
*9E ekspertas teigia, kad „**Nėra daroma didelė takoskyra**, iš esmės tarp dviejų reiškinių, informacijos ar kibernetinio saugumo, o **asmens duomenų apsauga neatsiejama nuo kibernetinio saugumo**. Kai duomenų apsauga yra iš esmės yra neatskiriama dalis kibernetinio saugumo, nes viskas, kas vyksta elektroninėje erdvėje, tos elektroninės informacijos apdorojimas ne bet kokios, o būtent tos informacijos, kuri turi vienokių ar kitokių ryšių su duomenų subjektu.*“ (9E, asmeninis interviu, 2023-01-05).		

Šaltinis: sudaryta autoriaus

2. Kokią įtaką asmens duomenų apsauga turi organizacijai? Atsakydami į klausimą 1E, 2E, 3E ir 9E ekspertai nurodė, kad asmens duomenų apsauga yra neatsiejama organizacijos veiklos dalis. Tuo tarpu 4E, 6E ir 7E ekspertai mano, kad organizacijoje asmens duomenų apsauga turi būti reglamentuota. Vienas 8E ekspertas nurodė, kad asmens duomenų apsauga organizacijoje atskleidžia jos brandą (žr. 8 lentelę).

8 lentelė. Asmens duomenų apsaugos įtaka organizacijai

Interviu ištrauka	Subkategorija	Kategorija
„*Jei ta organizacija tvarko ne tik darbuotojų, bet ir kitų asmenų asmens duomenis, tai vienas iš jos* ***būtinųjų teisėtos veiklos poreikių saugant reputaciją****.*“ (1E, asmeninis interviu, 2022-06-30).	Neatsiejama organizacijos veiklos dalis	Asmens duomenų apsaugos įtaka organizacijai
„*... asmens duomenys yra* ***neatsiejama veiklos vykdymo dalis****: klientai, darbuotojai, išorės šalys, verslo partneriai ir visos susijusios atliekamos funkcijos su įvardintomis suinteresuotomis šalimis savyje turės asmens duomenų tvarkymo poreikį.* ***Netinkamai tvarkant ar apsaugant duomenis kyla finansinės rizikos per reputaciją, negautas pajamas, skirtas sankcijas, neišnaudotas galimybes, prarastus klientus ir pan****.*“ (2E, asmeninis interviu, 2022-07-26).		
„*... jai būtina laikytis teisės aktų įpareigojimų.* ***Teisėta veikla reiškia sankcijų išvengimą****. Laimi tiek pati organizacija, tiek valstybė – taip* ***išvengiama papildomų laiko ir finansinių išlaidų****.*“ (3E, asmeninis interviu, 2022-08-05).		
„***Organizacijos veikla negalima, jeigu nėra sutvarkyta asmens duomenų apsauga****. Praktiškai nebėra organizacijų, kurios netvarkytų asmens duomenų. Organizacijos veikloje* ***duomenų apsauga****, ir mechanizmai skirti jai įgyvendinti,* ***yra neatsiejama organizacijos veiklos dalis***“ (9E, asmeninis interviu, 2022-01-05).		
„***BDAR atnešė į asmens duomenų apsaugą tvarką ir dėmesį****. Dabar net ir labai nedidelė įmonė kreipia dėmesį į asmens duomenų apsaugą, dažnai turi paskirtą duomenų apsaugos pareigūną ir* ***stengiasi valdyti kuo mažiau asmens duomenų bei tai daryti skaidriai****...*“ (4E, asmeninis interviu, 2022-09-14).	Reglamentuota asmens duomenų apsauga	
„***Skatina organizacijas <...> reglamentuoti asmens duomenų tvarkymo procesus****,- <...> analizuoti savo veiklos procesus, o analizės proceso metu* ***atsiranda galimybė pamatyti veiklos organizavimo spragas, trūkumus****, keistis, gerinti santykius su kontrahentais, darbuotojų padėtį ir pan.*“ (6E, asmeninis interviu, 2022-12-07).		
„*Asmens duomenų apsauga* ***apibrėžia pagrindines taisykles*** *kaip ir kokiomis priemonėmis asmens duomenys bus tvarkomi organizacijoje.*“ (7E, asmeninis interviu, 2022-12-08).		
„*Indikuoja kokia yra* ***organizacijos branda*** *informacijos saugumo (konfidencialumo, vientisumo, prieinamumo) valdymo srityje*“ (8E, asmeninis interviu, 2022-12-15).	Organizacijos branda	

Šaltinis: sudaryta autoriaus

3. Kaip tobulintumėte duomenų apsaugos pareigūno funkcijas, siekiant užtikrinti asmens duomenų apsaugą organizacijoje? Atsakydami į klausimą 1E, 2E, 3E,4E, 8E ir 9E ekspertai, mano kad duomenų apsaugos pareigūnui reiktų suteikti daugiau įgaliojimų ir leisti naudotis gerąja praktika. 5E ir 7E ekspertai pateikė kitą nuomonę, jog duomenų apsaugos pareigūnai turėtų kelti kvalifikaciją (žr. 9 lentelę).

9 lentelė. Duomenų apsaugos pareigūno funkcijų tobulinimas, siekiant užtikrinti asmens duomenų apsaugą organizacijoje

Interviu ištrauka	Subkategorija	Kategorija
„*Pakanka **suteikti įgaliojimus** numatytus teisės aktuose ir leisti vadovautis **gerąja praktika**.*“ (1E, asmeninis interviu, 2022-06-30).	Didesni įgaliojimai ir geroji praktika	Duomenų apsaugos pareigūno funkcijų tobulinimas, siekiant užtikrinti asmens duomenų apsaugą organizacijoje
„*Šiek tiek rekomenduočiau koreguoti reglamente nurodytas DAP funkcijas, leidžiant **dalyvauti pilnavertiškai organizacijos veikloje** atliekant PDAV, organizuojant duomenų tvarkymo veiklos įrašų priežiūrą ir pan. **Nenusišalinant visiškai nuo procesų ir kultūros**, nes nepriklausomumas mažoms organizacijoms didina kaštus ruošiant papildomai darbuotojus įvairiam BDAR reikalavimų įgyvendinimui...*“ (2E, asmeninis interviu, 2022-07-26).		
„*<...> **aiškiau sureglamentuoti DAP atsakomybes** įgyvendinant duomenų saugą.*“ (3E, asmeninis interviu, 2022-08-05).		
„*<...> BDAR ir jį paaiškinantys dokumentai gana gerai apibrėžia duomenų apsaugos pareigūno funkcijas, tad didelių patobulinimų kaip ir nereikia. <...> Organizacijai reikia **naudoti visuotinai priimtas gerosios praktikos sistemas** sprendimams priimti ir **turėti gerąja praktika sudarytą valdymo ir administravimo struktūrą** - tada tokių barjerų bus išvengta.*“ (4E, asmeninis interviu, 2022-09-14).		
„*Duomenų apsaugos pareigūnas turėtų išmanyti informacijos saugumo valdymo principus, turėti nors minimalių žinių IT, informacijos saugumo srityje <...> **turi aktyviai dalyvauti visuose veiklos procesuose**, susijusiuose su duomenų tvarkymu viso gyvavimo ciklo metu, konsultuoti dėl atitikties BDAR...*“ (8E, asmeninis interviu, 2022-12-15).		
„*<...> Reikia suvokti, kad tai neturi būti formali pareigybė, kaip dažnai labai matoma, kad paprasčiausiai organizacijos formaliai pasirengia dokumentus tokius, kokių reikia. <...> Kartais duomenų apsaugos pareigūnas organizacijoje neturi jokių sprendimo priėmimo galių ir kartais net ir nelabai jo paisoma. <>Turėtų būti priešingai**, jis turėtų tikrai priimti svarbius sprendimus ir būti paskutinis, kuris tars lemiamą žodį duomenų apsaugos srityje**.*“ (9E, asmeninis interviu, 2022-01-05).		
„*rekomenduočiau **kelti kvalifikaciją** informacijos ir kibernetinio saugumo valdymo srityje.*“ (5E, asmeninis interviu, 2022-11-25).	Kvalifikacijos kėlimas	
„*Periodinis duomenų apsaugos pareigūno atestavimas, **kvalifikacijos kėlimo mokymai**...*“ (7E, asmeninis interviu, 2022-12-08).		

Šaltinis: sudaryta autoriaus

4. Kokių veiksmų turėtų imtis organizacija, siekdama patobulinti savo valdymo procesus asmens duomenų apsaugos reiškinio kontekste? Atsakydami į klausimą 1E, 2E, 4E, 8E ir 9E ekspertai nurodė, kad organizacijos valdymo procesus tobulintų duomenų apsaugos reiškinio kontekste vadovaudamiesi gerąja praktika. 5E, 6E ir 7E ekspertai, mano kad svarbu reglamentuoti asmens duomenų apsaugą organizacijoje (žr. 10 lentelę).

10 lentelė. Organizacijos valdymo procesų tobulinimas duomenų apsaugos reiškinio kontekste

Interviu ištrauka	Subkategorija	Kategorija
„*...Bendrai svarbu įsitikinti, kad asmens duomenų apsauga yra **integralus kitų taikomų duomenų apsaugos priemonių valdymo elementas*** už kurį priskirta atsakomybė (vertinti rizikas, nustatyti kontrolės priemones, jas įgyvendinti, stebėti, prireikus koreguoti)...“ (1E, asmeninis interviu, 2022-06-30).	Geroji praktika	Organizacijos valdymo procesų tobulinimas duomenų apsaugos reiškinio kontekste
„*... Pasitelkti ISO27000 ar kitą standarto karkasą procesų sudėliojimui ar ISVS nustatymui. **Ieškoti atitikties kibernetinio saugumo standartams ar gerosioms praktikoms** – NIST, ISO, PCI DSS, CSC20. Bazinių dalykų įgyvendinimas padengia didžiąją dalį techninių reikalaujamų kontrolių, skirtų tinkamam BDAR įgyvendinimui*“ (2E, asmeninis interviu, 2022-07-26).		
„*... Jeigu organizacija naudoja **visuotinai priimtas gerosios praktikos sistemas sprendimams priimti ir turi gerąja praktika sudarytą valdymo ir administravimo struktūrą** – visa tai leis pasirinkti tinkamas pagal tikslus, rizikas ir biudžetą priemones*“ (4E, asmeninis interviu, 2022-09-14).		
„*Taikyti funkcijų atskyrimo principą, taikyti 4 akių principą, **taikyti gerąją praktiką**, vadovautis teisės aktuose nustatytais reikalavimais.*“ (8E, asmeninis interviu, 2022-12-15).		
„*... Tikslai turi būti labai konkretūs ir aiškūs, **betarpiškai susieti su įmonės veikla ir jos teikiamomis paslaugomis**. Įmonės neturi galvoti apie tai, kad daugiau yra geriau. Įmonės neturi galvoti apie tai, kad patogumas yra argumentas. Mes turime suvokti, kad duomenų apsaugoje patogumas negali būti matuojamas kaip argumentas naudoti vienokią ar kitokią technologiją. Patogumas negali būti naudojamas kaip argumentas tvarkant asmens duomenis. Visų pirma, pirmiausia reikėtų galvoti apie duomenų subjekto pažeidžiamumą ir apie būtinumą tokius duomenis tvarkyti.*“ (9E, asmeninis interviu, 2022-01-05).		

*„**detaliai reglamentuoti** su asmens duomenų tvarkymu susijusius organizacijos veiklos procesus...“* (5E, asmeninis interviu, 2022-11-25).	Reglamentuota asmens duomenų apsauga	
*„Visų pirma tiksliai nustatyti tvarkomų asmens duomenų rūšis, tikslus ir pagrindus. Tuomet, pasitelkus profesionalo asmens duomenų apsaugos srityje pagalbą, **pasirengti visus būtinus asmens duomenų tvarkymo dokumentus** ir juos reguliariai peržiūrėti bei atnaujinti. <...> modernizuoti bei padaryti patraukliais ir kaip įmanoma lengviau suvokiamais veiklos procesus, laikantis BDAR reikalavimų.“* (6E, asmeninis interviu, 2022-12-07).		
*„Nustatyti asmens duomenų kategorijas; Apibrėžti duomenų valdytojus ir tvarkytojus; Rengti specializuotus mokymus darbuotojams pagal jų darbo pobūdį; Paskirti asmens duomenų pareigūną; **Suformuoti asmens duomenų tvarkymo taisykles** ir įgyvendinti automatizuotus stebėjimo procesus.“* (7E, asmeninis interviu, 2022-12-08).		

Šaltinis: sudaryta autoriaus

Pusiau struktūruoto klausimyno **II tyrimo dalį – Kibernetinio saugumo, kaip reiškinio, teorinis pagrindimas**, sudaro 3 klausimai.

1. Kokią reikšmę kibernetinio saugumo įgyvendinimas turi asmens duomenų apsaugai? Atsakydami į klausimą 1E, 2E, 3E, 5E, 7E ir 8E ekspertai nurodė, kad kibernetinis saugumas yra neatsiejama asmens duomenų apsaugos dalis, nes jis padeda apsaugoti asmens duomenis ir sumažina incidento tikimybę. 9E ekspertas teigia, kad organizacinės ir techninės priemonės įtakoja asmens duomenų tvarkymo procesus (žr. 11 lentelę).

11 lentelė. Kibernetinio saugumo įgyvendinimo reikšmė asmens duomenų apsaugai

Interviu ištrauka	Subkategorija	Kategorija
*„Be kibernetinio saugumo priemonių įgyvendinimo **neįmanoma užtikrinti el. erdvėje tvarkomų asmens duomenų apsaugos**.“* (1E, asmeninis interviu, 2022-06-30).	Neatsiejama organizacijos veiklos dalis	Kibernetinio saugumo įgyvendinimo reikšmė asmens duomenų apsaugai
*„tinkama kibernetinio saugumo aplinka **leidžia siekti atitikties BDAR ir užtikrinti racionalią asmens duomenų apsaugą**.“* (2E, asmeninis interviu, 2022-07-26)		
*„Kibernetinio saugumo užtikrinimas tiesiogiai **įtakoja saugos užtikrinimą asmens duomenų apimtyje**.“ (3E, asmeninis interviu, 2022-08-05).*		
*„tinkamas kibernetinio saugumo **valdymas sumažina asmens duomenų praradimo, sunaikinimo ir pakeitimo tikimybę**.“ (5E, asmeninis interviu, 2022-11-25).*		

*„Netinkamai įgyvendinus kibernetinio saugumo principus ir sprendimus **asmens duomenim apsaugoti**, internetiniai sukčiai gali panaudot šiuos duomenis kibernetinėms atakoms vykdyti(pvz. socialinė inžinerija).“ (7E, asmeninis interviu, 2022-12-08).*		
*„Kibernetinio saugumo reikalavimų įgyvendinimas **užtikrina informacijos, kuria disponuoja įmonė saugumo užtikrinimą pagal atitinkamą informacijos saugumo lygį**. Skirtingam lygiui – skirtingi reikalavimai. Asmens duomenys taip pat reikalauja skirtingo lygio kibernetinio saugumo reikalavimų įgyvendinimo...“ (8E, asmeninis interviu, 2022-12-15).*		
*„... **Renkantis organizacines technines priemones** organizacijoje, vis dėlto nereikėtų galvoti, kad kaina yra galutinis momentas. Dažnai daroma klaida ne tai, kad per prasti sprendimai pasirenkami, o tiesiog įsigyjama techninė ir programinė įranga, galbūt ta, kurios net nereikia. Ta, kuri turi labai dideles galimybes, technologines galimybes rinkti daugiau nei būtina organizacijai. <...> Organizacija kuri turi daugiau įrangos, kuri leidžia rinkti daugiau duomenų, ir dažnai ji tai darys, rinks daugiau, net jei tai jai nėra būtina. <...> jeigu yra įmanoma nerinkti kažkokios informacijos, tai ir kibernetinio saugumo lygis bus teoriškai ir praktiškai aukštesnis, nes paprasčiausiai bus didesnis dėmesys skiriamas tiesioginių funkcijų atlikimui, o ne nesusijusių duomenų apsaugai.“ (9E, asmeninis interviu, 2022-01-05).*	Organizacinės ir techninės priemonės	

Šaltinis: sudaryta autoriaus

2.1. Kokią įtaką organizacijai turi kibernetinio saugumo teisinis reglamentavimas? Atsakydami į klausimą 1E, 2E, 3E, 4E, 5E, 6E, 8E ir 9E ekspertai nurodė, kad kibernetinio saugumo reglamentavimas padeda organizacijoms suvokti, kokie reikalavimai taikomi, siekiant užtikrinti kibernetinį saugumą. 7E ekspertas įvardino, kad kibernetinio saugumo reglamentavimas apsunkina organizacijų veiklą (žr. 12 lentelę).

12 lentelė. Kibernetinio saugumo teisinio reglamentavimo įtaka organizacijai

Interviu ištrauka	Subkategorija	Kategorija
„***Minimalus reikalavimų rinkinys**, kuris padeda efektyviai naudoti išteklius **parenkant taikomas kibernetinio saugumo priemones** atsižvelgiant į veiklos pobūdį.“* (1E, asmeninis interviu, 2022-06-30).	Kibernetinio saugumo reikalavimų suvokimas ir įgyvendinimas	Kibernetinio saugumo teisinio reglamentavimo įtaka organizacijai
*„... **Atitikties siekis** yra tam tikras brandos laiptelis bei akstinas nenumoti ranka į kibernetinį saugumą, jei organizacijos vis dar abejoja jo nauda...“* (2E, asmeninis interviu, 2022-07-26).		

*„Įstaiga **turi vadovautis teisės aktais, veikti teisėtai**, bendradarbiauti su NKSC (nustatyta prievolė), tokiu būdu prisidedant prie valstybės kibernetinio saugumo įgyvendinimo“ (3E, asmeninis interviu, 2022-08-05).*		
*„... vienas iš pagrindinių gero **kibernetinio saugumo projektavimo aspektų**.“ (4E, asmeninis interviu, 2022-09-14).*		
*„jis **taikomas tik ribotam subjektų ratui** (pagrinde tik valstybės sektoriaus organizacijoms, o BDAR taikomas visoms organizacijoms), todėl turėtų būti tobulintinas;“ (5E, asmeninis interviu, 2022-11-25).*		
*„**Duoda aiškumą** <...> kokius procesus įmonės privalo įdiegti ir organizuoti savo veikloje.“ (6E, asmeninis interviu, 2022-12-07).*		
*„Teisinis reglamentavimas **užtikrina visiems kibernetinio saugumo subjektams aiškius, objektyvius reikalavimus**, nustatomus nacionaliniu mastu, taikomus visiems kibernetinio saugumo subjektams, ne tik viešajam sektoriui ir taikomus skirtingiems saugumo lygiams (pvz. pagal informacijos svarbą, IS kategoriją)“ (8E, asmeninis interviu, 2022-12-15).*		
*„ ... Teisė negali visą laiką iš anksto eiti reguliuoti tam tikrų teisinių santykių, kurie dar nesusiklostė. Bet elektroninėje erdvėje mes žinome, kad viskas kinta labai greitai ir kartais vertinant strateginę plėtrą ar produkto kūrimąsi, dėmesį reikia skirti numanomam arba ateities reguliavimui. Reikia galvoti labai atsargiai, reikia žiūrėti technologijas, kurios ypatingai dabar yra vystomos <> **Teisė vaidina reikšmingą vaidmenį ir gali iš esmės netgi sustabdyti įmonės veiklą**, jeigu bus priimtas vienoks ar kitoks teisinis sprendimas.“ (9E, asmeninis interviu, 2022-01-05).*		
*„**Padidėja organizacijos kaštai, lėtesnis programinės įrangos diegimo ir atnaujinimo procesas**, reikia atsižvelgti į duomenų lokaciją ir teisinį reguliavimą tam tikrame regione bei priklausomai nuo veiklos srities derinti IT saugumo procesus su valstybinėms institucijomis“ (7E, asmeninis interviu, 2022-12-08).*	Kibernetinio saugumo reikalavimų našta	

Šaltinis: sudaryta autoriaus

2.2. Kokią įtaką organizacijai turi kibernetinio saugumo priežiūros institucijos (Nacionalinis kibernetinio saugumo centras) veikla? Atsakydami į klausimą 1E ir 4E ekspertai nurodė, kad Nacionalinis kibernetinio saugumo centras yra labai svarbi institucija, kuri teikia ekspertines žinias ir pagalbą įvykus kibernetiniam incidentui. Visiškai priešingą nuomonę pateikė 2E, 5E, 8E ir 9E ekspertai, kurie teigia, kad NKSC veikla turėtų būti tobulinama, nes šiuo metu ji nepadeda organizacijoms užtikrinti kibernetinio saugumo, o tik skatina formaliai užtikrinti atitiktį kibernetinio saugumo teisės aktų reikalavimams (žr. 13 lentelę).

13 lentelė. Nacionalinio kibernetinio saugumo centro įtaka organizacijai

Interviu ištrauka	Subkategorija	Kategorija
„***Profesionali pagalba ir metodiniai, techniniai patarimai*** *susidūrus su* ***kibernetinio saugumo iššūkiais*** *24x7.*“ (1E, asmeninis interviu, 2022-06-30).	Pagalba užtikrinti kibernetinį saugumą	Nacionalinio kibernetinio saugumo centro įtaka organizacijai
*„... **Tai labai svarbus darinys**, teikiantis **ekspertines žinias** ir **praktinę pagalbą** organizacijoms kovojant su kibernetiniais nusikaltimais.“ (4E, asmeninis interviu, 2022-09-14).*		
*„priežiūros institucijų įtaka kibernetinio saugumo svarbai organizacijose <...> **labai mažareikšmė**... Neturint tinkamų baudimo įrankių – institucijos praranda įtaką, neturint gerų specialistų – jos praranda ir reputaciją, būdamos politiškai paveikiamos – netenka ir nacionalinio svorio.*“ (2E, asmeninis interviu, 2022-07-26).	Pagalba formalizuoti kibernetinį saugumą, bet ne užtikrinti	
„NKSC galėtų būti aktyvesnis savo veikloje, stebėdamas Kibernetinio saugumo įstatymo įgyvendinimo kontrolę ir proaktyviai skatindamas subjektus įgyvendinti jo reikalavimus;“ (5E, asmeninis interviu, 2022-11-25).		
*„Jeigu NKSC vykdytų patikras vietoje, ar akredituotų kibernetinio saugumo subjektų valdomas informacines sistemas, tokiu atveju galima būtų užtikrinti, kad atitiktis yra neformali. Šiai dienai NKSC veikla derinant saugos nuostatus ir saugos politiką įgyvendinančius dokumentus dėl jų atitikties kibernetinio saugumo reikalavimams tik **skatina formalią atitiktį**, nes dažnu atveju tiesiog žiūrima kaip nustatyta teisės aktuose ir jeigu trūksta reikalavimų įgyvendinimo – reikalaujama papildyti dokumentuose trūkstamomis procedūromis ar reikalavimais, tačiau **de facto NKSC netikrina ar tokie reikalavimai/procedūros realiai įgyvendinami, vykdomi**.“ (8E, asmeninis interviu, 2022-12-15).*		
*„ ... **Pas mus viskas yra dokumentų lygiuose tikrinama**. <...> Rezultatas, priklausys nuo pačios organizacijos <...> Ir nuo žmogaus žinių, turimos patirties kiekio, priklausys, ar jis gerai padarys. Tai vis dėlto ta organizacija, priežiūros institucijos pas mus Lietuvoje, kurios turėtų įgyvendinti saugumo politiką, teisės aktų įgyvendinimą, **turėtų pagalvoti apie tai, kad dalis funkcijų, kurios yra formalios, jos turėtų kontrolės mechanizmus, galbūt padidinti galimybes dalyvauti tiesiogiai NKSC**, galbūt kritinės infrastruktūros atveju padaryti savitikros mechanizmą, įvertinti, ar tikrai pateko, ar tikrai turi būti viename ar kitame registre“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

2.3. Kokią įtaką organizacijai turi kibernetinio saugumo valdymo procesai? Atsakydami į klausimą 1E, 2E, 5E, 6E, 8E ir 9E ekspertai nurodė, kibernetinio saugumo valdymo procesai privalo veikti praktikoje ir būti efektyvūs (žr. 14 lentelę).

14 lentelė. Kibernetinio saugumo valdymo procesų įtaka organizacijai

Interviu ištrauka	Subkategorija	Kategorija
„***Greitas reagavimas, sprendimų priėmimas, lankstumas ir integruotas požiūris*** *kaip į sudėtinę organizacijos valdymo procesų dalį, vertinant įtaką pagrindinėms veikloms, bet nesukuriant savitikslių procesų.*“ (1E, asmeninis interviu, 2022-06-30).	Praktinis ir efektyvus kibernetinio saugumo įgyvendinimas	Kibernetinio saugumo valdymo procesų įtaka organizacijai
„*be tinkamų valdymo procesų ir palaikymo kibernetinio saugumo branda organizacijoje gali būti* ***maksimaliai pasiekiama tiek, kiek tame mato prasmę vadovybė****.*“ (2E, asmeninis interviu, 2022-07-26).		
„*kibernetinio saugumo reikalavimų* ***įgyvendinimo procedūros*** *leidžia apsibrėžti būtinas atsakomybes, veiklas ir jų įgyvendinimo procesą, siekiant užtikrinti nepertraukiamą kibernetinio saugumo valdymą*“ *(5E, asmeninis interviu, 2022-11-25).*		
„***Įgalina labiau užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą****.*“ *(6E, asmeninis interviu, 2022-12-07).*		
„***Valdymo procesai de facto yra svarbiau, nei valdymo procesai de jure****. Jeigu de jure sutampa su de facto – tai indikacija, kad valdymo procesai yra realūs, o informacija ir rizikos yra valdomi.*“ *(8E, asmeninis interviu, 2022-12-15).*		
„*Taip, mes žinome, kad yra sertifikatai yra tarptautiniai standartai, kuriuos reikia atitikti.* ***Standartų įgyvendinimas, padeda užtikrinti atitinkamą efektyvų valdymą****.*“ *(9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

2.4. Kokią įtaką organizacijai turi kibernetinio saugumo kultūra? Atsakydami į klausimą 1E, 4E, 5E, 6E ir 8E ekspertai nurodė, kad kibernetinio saugumo kultūra yra naudinga, nes ji formuoja organizacijos elgesį, siekiant užtikrinti kibernetinį saugumą. 2E ir 9E ekspertai išsakė nuomonę, kad kibernetinio saugumo kultūros formavimas prasideda nuo organizacijos vadovybės veiksmų (žr. 15 lentelę).

15 lentelė. Kibernetinio saugumo kultūros įtaka organizacijai

Interviu ištrauka	Subkategorija	Kategorija
„*Organizacinės kultūros dalis, kuri itin svarbi daugeliui organizacijų dirbant nuotoliniu būdu,* ***aptartas elgsenos el. erdvėje modelis*** *ir sudaryta galimybė įvairaus IT raštingumo ...*“ (1E, asmeninis interviu, 2022-06-30).	Nauda kibernetiniam saugumui	Kibernetinio saugumo kultūros įtaka organizacijai
„***Kultūra atsiranda laikui bėgant****. <...> Lietuva keliauja gera kryptimi, nes vis daugiau įmonių supranta (arba priverstos suprasti, kad ir dėl BDAR) kibernetinio saugumo kultūros svarbą.*“ *(4E, asmeninis interviu, 2022-09-14).*		
„*kibernetinio saugumo įgyvendinimą* ***integruoti į kitus organizacijos veiklos procesus***“ *(5E, asmeninis interviu, 2022-11-25).*		
„*... jeigu organizacijoje yra kibernetinio saugumo kultūra, vadinasi,* ***organizacija yra pažangi, moderni, pažengusi, linkusi į naujoves*** *ir žengianti koja kojon drauge su jomis.*“ *(6E, asmeninis interviu, 2022-12-07).*		
„*...****Žema kultūra – žemas kibernetinio saugumo lygis****.*“ *(8E, asmeninis interviu, 2022-12-15).*		
„***Kultūros toną užduoda organizacijoje vadovybė,*** *taigi, čia galioja analogiška situacija, kad formuojant žalingą kultūrą tarp darbuotojų kibernetinio saugumo atžvilgiu, nerodant palaikymo ar neskiriant dėmesio, finansinio taip pat, formuojasi ydingi pavyzdžiai užkertantys kelią tinkamam kibernetinio saugumo brandos lygiui siekti.*“ (2E, asmeninis interviu, 2022-07-26).	Organizacijos vadovų įtaka	
„*Kibernetinė kultūra tiesiogiai siejasi su taip pat skaitmenine higiena.* ***Kibernetinės kultūros organizacijų klausimas tiesiogiai priklauso nuo vadovų****. Jei vadovas pats supras visus procesus, kurie vyksta, jei vadovas betarpiškai tame dalyvaus. Jei darbuotojai nebus įtraukti tik formaliai pasirašant tvarkas, metodologijos ar taisykles, politikas įvairios. Jei darbuotojas nežinos turinio, nesupras tų dokumentų turinio, tai apie kibernetinės kultūros lygį organizacijoje kalbėti negalima.* ***Didžiausia problema Lietuvoje****, kad visos organizacijos formaliai yra priėmusios reikiamus dokumentus. Tačiau jeigu pažiūrėti, kaip yra tas gyvas ryšys su darbuotojais ir dokumentų įgyvendinimas organizacijoje, tai turbūt didžiąja dalimi visiškai formaliai tuos dokumento žiūri. Dėl to ir pats lygis* ***kibernetinės kultūros organizacijos yra tiesiog deklaratyvus****. Jis jokiu būdu neatspindi faktinių aplinkybių ir faktinio veikimo.*“ *(9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

2.5. Kokią įtaką organizacijai turi kibernetinio saugumo komunikacija? Atsakydami į klausimą 1E ir 8E ekspertai nurodė, kad kibernetinio saugumo komunikacija

turi didelę įtaką siekiant suvaldyti incidentus organizacijoje. 2E, 6E, ir 9E ekspertai, mano kad svarbu skirti didelį dėmesį kibernetinio saugumo kasdieninių veiklų iškomunikavimui (žr. 16 lentelę).

16 lentelė. Kibernetinio saugumo komunikacijos įtaka organizacijai

Interviu ištrauka	Subkategorija	Kategorija
„*... **greitas reagavimas**, **aiški komunikavimo strategija** ir seka, žinomi sprendimams priimti reikalingi asmenys užtikrina subalansuotą reagavimą į situaciją, **nekeliant bereikalingos panikos ir laiku suvaldant kilusius iššūkius**.*“ (1E, asmeninis interviu, 2022-06-30).	Incidentų suvaldymas	Kibernetinio saugumo komunikacijos įtaka organizacijai
„*leidžia užtikrinti **kibernetinių incidentų, ypač susijusių su asmens duomenų pažeidimu, tinkamą valdymą**.“ (5E, asmeninis interviu, 2022-11-25).*		
„***Prasta komunikacija gali sukelti krizę** krizėje, pvz. kai įvyksta incidentas / asmens duomenų saugumo pažeidimas.“ (8E, asmeninis interviu, 2022-12-15).*		
„*įgyvendinant kibernetinį saugumą didelę įtaką turi **abipusė komunikacija**. Svarbu išlaikyti tinkamą propagandos lygį iš vadovybės pusės, taip pat būtina girdėti ir darbuotojų žinutes. Kibernetinis saugumas neturi būti kontrolieriaus pozicijoje, tai turi būti **priedas vykdyti kasdienę veiklą saugiai**, taip kuriant pridėtinę vertę organizacijai. Be tinkamos komunikacijos to pasiekti neįmanoma.*“ (2E, asmeninis interviu, 2022-07-26).	Iškomunikuota kasdieninė kibernetinio saugumo veikla	
„*... **Darbuotojai, supažindinti su kibernetinio saugumo priemonėmis**, atsižvelgiant į jų lojalumą darbdaviui ir suinteresuotumą įmonės sėkme, gali būti puikus įrankis, užtikrinant įmonėje kibernetinį saugumą.“ (6E, asmeninis interviu, 2022-12-07).*		
„*... Mes suprantame, kad valstybė negali imperatyviais teisės aktais įtvirtinti vienos vyraujančios technologijos. Valstybė negali priversti įsigyti vienos ar kitos įrangos, tačiau **valstybė gali pasakyti, ką ji ir daro, kad turi atitikti tam tikrą standartą**...“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

3. Kaip tobulintumėte informacijos saugos įgaliotinio funkcijas, siekiant užtikrinti kibernetinį saugumą organizacijoje? Atsakydami į klausimą 1E, 5E ir 4E ekspertai nurodė, kad informacijos saugos įgaliotiniui turėtų būti suteikti tinkami įgaliojimai, o jis vykdydamas savo darbo funkcijas vadovautųsi geroja praktika. 3E ir 7E ekspertai, mano informacijos saugos įgaliotiniui svarbiausia yra kelti kvalifikaciją. 5E ir 9E ekspertai akcentavo, kad didesnis dėmesys turi būti skiriamas komunikacijai vykdant informacijos saugos įgaliotinio funkcijas (žr. 17 lentelę).

17 lentelė. Informacijos saugos įgaliotinio funkcijų tobulinimas, siekiant užtikrinti kibernetinį saugumą organizacijoje

Interviu ištrauka	Subkategorija	Kategorija
„*... pakanka **suteikti įgaliojimus numatytus teisės aktuose** ir leisti **vadovautis gerąja praktika**. Organizacijai svarbu pagal jos veiklos pobūdį ir dydį įvertinti kiek ir kokių asmenų turi būti atsakingų už įvairaus pobūdžio informacijos saugą, esant poreikiui **lanksčiai vertinti ir integruoti tarpusavyje suderinamas atsakomybes**, taip nesukuriant formalių neveiksmingų struktūrų.*“ (1E, asmeninis interviu, 2022-06-30).	Įgaliojimų suteikimas ir geroji praktika	Informacijos saugos įgaliotinio funkcijų tobulinimas, siekiant užtikrinti kibernetinį saugumą organizacijoje
„*informacijos saugos įgaliotinio **pavaldumas tik aukščiausiai vadovybei**, nes kultūra formuojama nuo viršaus žemyn, o ne atvirkščiai...*(2E, asmeninis interviu, 2022-07-26).		
„*Informacijos saugos įgaliotinis, angliškai Chief Information Security Officer (CISO) yra gana gerai apibrėžta funkcija. Problemos prasideda tada, kai organizacija negeba sukurti savo struktūros pagal visuotinai priimtas gerąsias praktikas, o CISO savo ruožtu irgi **nesivadovauja jo funkcijoms skirtomis gerosiomis praktikomis**.*“ *(4E, asmeninis interviu, 2022-09-14).*		
„***Numatyti aiškią kvalifikaciją**.*“ *(3E, asmeninis interviu, 2022-08-05).*	Kvalifikacijos kėlimas	
„*Papildomi **kvalifikacijos kėlimo kursai ir periodinis atestavimas**, <> bei darbo **patirties reikalavimas**.*“ *(7E, asmeninis interviu, 2022-12-08).*		
„***numatyčiau papildomą funkciją – užtikrinti tinkamą komunikavimą su išorinėmis** (paslaugų tiekėjų, klientų, užsakovų, priežiūros institucijų ir pan.) **incidentų valdymo grupėmis**, tikslu keistis informacija apie kibernetinius incidentus*“ *(5E, asmeninis interviu, 2022-11-25).*	Komunikacija	
„*... Problema yra tokia, kad organizacijoms yra sunku pritraukti gerus specialistus, o saugos įgaliotinio poreikiai yra dideli <...> Pagrindinė funkcija**, jis turi būti kaip konsultantas** <...> mažinant jiems tenkančią naštą. <...> Dėl to tas tobulinimas būtų, tikriausiai iš tos pusės, be techninių visų specifikacijų parengimo pagrindo. **Turėtų didelis dėmesys skiriamas ir komunikacijai**, ir žmogiškųjų savybių vystymui, emocinio intelekto vystymui ir taip toliau.*“ *(9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

Pusiau struktūruoto klausimyno **III tyrimo dalį – Asmens duomenų apsaugos ir kibernetinio saugumo įgyvendinimo problematika**, sudaro 5 klausimai.

1. Dėl kokių priežasčių daugelis organizacijų turi formaliai apsibrėžę saugos procesus, gaires? Atsakydami į klausimą 2E, 3E, 6E, 7E ir 9E ekspertai nurodė, kad organizacijos nesuvokia asmens duomenų saugos ir kibernetinio saugumo svarbos, todėl

daugelį procesų ir reikalavimų įgyvendina tik formaliai. 4E, 5E, ir 8E ekspertai, mano, kad organizacijos sąmoningai deklaratyviai užtikrina asmens duomenų apsaugos ir kibernetinio saugumo teisės aktų reikalavimus, nes nenori papildomai investuoti ir supranta, kad priežiūros institucijos nėra pajėgios užtikrinti jų kontrolės. (žr. 18 lentelę).

18 lentelė. Priežastys formalių saugos procesų, gairių organizacijose

Interviu ištrauka	Subkategorija	Kategorija
„***BDAR svarbos suvokimo trūkumas, kompetencijų trūkumas, patarimo iš šalies nepaisymai ir pan***.“ (2E, asmeninis interviu, 2022-07-26).	Nesuvokimas ir kompetencijų trūkumas	Priežastys formalių saugos procesų, gairių organizacijose
„*Formaliai, nes daug kas* ***nežino realių asmens duomenų praradimo pasekmių, valstybėje dar mažai teisminės ir neteisminės praktikos*** *šiuo klausimu.*“ (3E, asmeninis interviu, 2022-08-05).		
„*Vis dar nemato prasmės investuoti į profesionalų asmens duomenų apsaugos srityje paslaugas.* ***Nesuvokia asmens duomenų sąvokos ir svarbos*** *saugoti asmens duomenis, Neinformuoja apie asmens duomenų apsaugos pažeidimų pasekmes. Negerbia žmogaus teisių ir yra neišprususios...“ (6E, asmeninis interviu, 2022-12-07).*		
Dideli informacinės saugos įgyvendinimo kaštai *ir* ***kompetentingų žmonių trūkumas*** *diegiant informacinės saugos sprendimus. Pasitaiko atvejų kai organizacijoje IT saugumo procesai yra priskiriami IT skyriaus veiklai, taip sudarant sąlygas aplaidžiau vertinti IT saugumą ir neužtikrinti reikiamų IT saugumo priemonių“ (7E, asmeninis interviu, 2022-12-08).*		
„*... Dėl to, kad jos* ***nemato didžiausio poreikio stengtis ir daryti****. Jos perkasi ir diegiasi sistemos, kurias diegia ir perka visi. Jos iš esmės nori, kad tie procesai nemaišytų pelno siekimui <...> Jiems visi* ***nauji reguliavimai matomi per stabdymą****, tai yra tai, kad bus nepatogu, reikės kažką keisti ir* ***padidės išlaidos****...“ (9E, asmeninis interviu, 2022-01-05).*		
„***Daugiausia dėka BDAR****. Kiti dėl jiems būtinų reguliavimų ir įstatymų. Dalis dėl visuotinai priimtų gerųjų praktikų naudojimo.“ (4E, asmeninis interviu, 2022-09-14).*	Teisės aktai ir priežiūros institucijų veikla	
„***siekdami įgyvendinti teisės aktų reikalavimus****, tinkamai valdyti informacijos ir kibernetinio saugumo valdymą bei asmens duomenų apsaugą. Kita priežastis, kad* ***NKSC nesiima bausti kibernetinio saugumo subjektų*** *už Lietuvos teisės aktų, reglamentuojančių elektroninės informacijos saugą ir kibernetinį saugumą, reikalavimų“ (5E, asmeninis interviu, 2022-11-25).*		

*„**Aukšti informacijos saugumo reikalavimai**, taikomi I ir aukštesnės kategorijos valstybės informacinėms sistemoms, t.y. reikalavimai užtikrinti gerosios praktikos (ISO 27001, ISO 27002 standartų) reikalavimų įgyvendinimą <...> **1. Skirtingi informacijos saugumo reikalavimai** sąlygoja skirtingą valstybės informacinių valdytojų brandą... 2. kibernetinio saugumo ir informacinių technologijų specialistų **trūkumas** ir (arba) kompetencijų informacijos saugumo (kibernetinio saugumo) srityje trūkumas tiek kibernetinio saugumo subjektų organizacijose tiek **kibernetinio saugumo subjektus kontroliuojančiose institucijose**. 3. efektyvaus informacijos saugumo, kibernetinio saugumo reikalavimų įgyvendinimo kontrolės mechanizmo nebuvimas, kuris pasireiškia **ribotomis kontroliuojančių institucijų (pvz. NKSC) galimybėmis** atlikti valstybės informacinių sistemų nuostatų, saugos dokumentų ir kitų saugos politiką įgyvendinančių dokumentų bei pačių organizacijų atitikties nustatytiems informacijos saugumo (kibernetinio saugumo) reikalavimams vertinimą.“ (8E, asmeninis interviu, 2022-12-15).*		

Šaltinis: sudaryta autoriaus

2. Dėl ko kai kurios organizacijos nesilaiko pagrindinių asmens duomenų tvarkymo principų? Atsakydami į klausimą 1E, 4E, 5E, 6E ir 8E ekspertai nurodė, kad kai kurios organizacijos nesilaiko pagrindinių asmens duomenų tvarkymo principų, nes nežino reikalavimų ir neturi reikiamų išteklių (finansinių, žmogiškųjų, kompetencijos). 2E, 3E ir 9E ekspertai mano, kad organizacijos nesureikšmina asmens duomenų tvarkymo principų nesilaikymo, todėl yra linkusios rizikuoti dėl iš to gaunamos naudos (žr. 19 lentelę).

19 lentelė. Pagrindinės asmens duomenų tvarkymo principų nesilaikymo priežastys

Interviu ištrauka	Subkategorija	Kategorija
*„... priežastys gali būti visos įmanomos: **reikalavimų nežinojimas, finansinė našta, realių sankcijų nebuvimas, kompetencijų trūkumas**.“* (1E, asmeninis interviu, 2022-06-30).	Nežinojimas, išteklių trūkumas	Pagrindinės asmens duomenų tvarkymo principų nesilaikymo priežastys
*„**Dėl nežinojimo, resursų trūkumo**.“ (4E, asmeninis interviu, 2022-09-14)*		
*„**Dėl BDAR nesupratimo**, dėl nesuvokimo kaip tai daryti, **dėl lėšų trūkumo** ir dėl kitų priežasčių“ (5E, asmeninis interviu, 2022-11-25)*		
*„**Neišprusimas. Nesuvokimas**. <> Visuomenės švietimo apie asmens duomenų apsaugą trūkumas priimtina, paprasta, suvokiama forma. **Asmens duomenų tvarkymo sudėtingumas, painumas, neaiškumas, nepatrauklumas**.“ (6E, asmeninis interviu, 2022-12-07).*		

„... žemas informacijos saugumo brandos lygis, ***specialistų, išmanančių asmens duomenų ir kibernetinio saugumo sritis trūkumas****, kontroliuojančių institucijų menka kontrolė.“ (8E, asmeninis interviu, 2022-12-15).*		
„*vadovaujasi rizikos tvarkymo strategija –* ***rizikos prisiėmimas****....“ (2E, asmeninis interviu, 2022-07-26).*	Rizikavimas	
„***Tinkamai neįvertina grėsmių, rizikų, laiko mažareikšmiu dalyku****.“ (3E, asmeninis interviu, 2022-08-05).*		
„... Pramonė ir technologijos vystosi į priekį, jos jau tampa pigesnės, jos tampa patogesnės. O patogumas yra masiškumas, o masiškumas yra greitis, o greitis yra didesnė grąžą. Atsakymas yra paprastas, ***tiesiog galimybės su naujomis technologijomis, kurios galbūt kertasi su principais, privatumo ir duomenų apsaugos, generuoja didesnes pajamas ir pelną****.“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

3. Kas lemia, kad organizacijos norėdamos užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą daugiau investuoja į technines priemones, o ne į organizacines? Atsakydami į klausimą 1E, 5E ir 6E ekspertai nurodė, kad organizacijos daugiau investuoja į technines asmens duomenų apsaugos ir kibernetinio saugumo priemones, nes neteikia prioriteto organizacinėms priemonėms ir nesupranta jų teikiamos naudos. 2E, 4E, 6E, 7E, 8E ir 9E ekspertai mano, kad techninių priemonių pirkimą ir įgyvendinimą organizacijoje lengviau pagrįsti, o į organizacinės priemones dėl išteklių trūkumo ir taupymo neinvestuojama. (žr. 20 lentelę).

20 lentelė. Investavimo į technines priemones, o ne į organizacines priemones priežastys, siekiant užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą

Interviu ištrauka	Subkategorija	Kategorija
„*... tai rodytų* ***nepakankamą organizacijos vadovų*** dėmesį asmens duomenų apsaugai ir kibernetiniam saugumui. Tokius sprendimus galėtų priimti organizacijos kuriose asmens duomenų apsauga ir kibernetinis saugumas priskirtas išskirtinai IT priežiūros padalinių atsakomybei, kurie pirmiausiai siekia tobulinti ir užkardyti galimus pavojus naujausiomis techninėmis priemonėmis, kurių pasiūla nuolat auga ir kinta. Kita vertus, galimai didesnis investicijų į technines priemones poreikis galimas ir pagrįstas, jei organizacija jau turi įdiegtas organizacines priemones ir tiesiog šiuo laikotarpiu atnaujina technines priemones įvertinusi esamas rizikas ir taikomų priemonių netinkamą būklę.“ (1E, asmeninis interviu, 2022-06-30).	Nesupratimas organizacinių priemonių svarbos	Investavimo į technines priemones, o ne į organizacines priemones priežastys, siekiant užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą

*„Kai kurios techninės priemonės yra reikalingos informacinių sistemų veiklos užtikrinimui (pvz. ugniasienės). Kita vertus, organizacijose pirmiau atsiranda IS padaliniai ir IT specialistai, kurie gerai supranta IT apsaugos technines priemones, bet **sunkiai supranta elektroninės informacijos saugos ir kibernetinio saugumo valdymą, ypač šiam valdymui reikiamas organizacines priemones** (tvarkas, darbuotojų mokymą ir socialinė inžineriją).“ (5E, asmeninis interviu, 2022-11-25).*		
*„... **neišprusimas ir nenoras investuoti daug laiko** į asmens duomenų apsaugą ir kibernetinį saugumą. <...> organizacines priemones reikia nuolat analizuoti, vertinti, atgyvenusias keisti, naujas įdiegti ir pan.“ (6E, asmeninis interviu, 2022-12-07).*		
„***techninės priemonės labiau akivaizdžiai matomos**, kaip kontrolės, **nei procesai ar procedūros, kurių, greičiausiai, dėl įgyvendinimo užtikrinimo trūkumo**, ne visada paisoma.“* (2E, asmeninis interviu, 2022-07-26).	Techninių priemonių materialumas ir išteklių trūkumas organizacinėms priemonėms	
*„Žinių trūkumas ir **žmogiškųjų išteklių trūkumas bei jų kaštai**. Vis dar esantis manymas, kad techninės priemonės „užtikrintai“ apsaugo.“ (4E, asmeninis interviu, 2022-09-14).*		
*„Netinkamai įvertintas ir paskirstytas biudžetas, **neaiškiai apibrėžta organizacijos struktūra ir atsakingumo ribos bei taupymas** IT saugumo įgyvendinimo kaštų apjungiant skirtingas roles į vieną.“ (7E, asmeninis interviu, 2022-12-08).*		
*„Todėl kad ugdyti darbuotojų sąmoningumą, įskaitant suvokimą elgtis pagal įmonėje nustatytas procedūras – tai yra **ilgas procesas, reikalaujantis tiek žmogiškųjų išteklių tiek finansinių sąnaudų tiek laiko**“ (8E, asmeninis interviu, 2022-12-15).*		
*„Dėl to, kad **technines priemones galima nupirkti ir parodyti**. Dėl to, kad techninės priemonės aiškiai **atsispindi dokumentuose**. Išlaidose, išlaidų eilutėse, kad juos galima matyti ir apčiuopti, įdiegti, paleisti, veikia. Pačios organizacinės priemonės nesusidaro iš daugelio dalykų. **Mokymai, kultūros lygio kėlimas, personalo kvalifikuoto turėjimas – tai yra sunkiau įgyvendinama**, žinant dėl didelės kaitos ir kitų dalykų, nes nematerialumas yra sunkiai kontroliuojamas.“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

4. Kaip vertinate Valstybinės duomenų apsaugos inspekcijos darbą užtikrinant kontrolę Bendrojo duomenų apsaugos reglamento reikalavimų įgyvendinimo kontekste? Atsakydami į klausimą 2E, 6E ekspertai nurodė, kad VDAI vyrauja pagalbos, o ne baudimo kultūra, siekiama organizacijoms padėti teikiant konsultacijas ir metodinę medžiagą. 5E, 8E ir 9E ekspertai mano, VDAI tinkamai įgyvendinti savo funkcijas trukdo žmogiškųjų išteklių trūkumas (žr. 21 lentelę).

21 lentelė. Valstybinės duomenų apsaugos inspekcijos darbas, siekiant užtikrinti Bendrojo duomenų apsaugos reglamento reikalavimų įgyvendinimo kontrolę

Interviu ištrauka	Subkategorija	Kategorija
„*Atsižvelgiant į tris Baltijos šalis, **Lietuvos VDAI užėmusi patarėjo**, nei, skirtingai kaip Latvijoje, baudėjo poziciją. Tai padeda kurti pasitikėjimo ir bendradarbiavimo kultūrą tarp duomenų tvarkytojų, valdytojų ir kontroliuojančios institucijos, kai, nesant dideliems pažeidimams ar matant duomenų valdytojo/tvarkytojo pastangas, **stengiamasi patarti ir pagelbėti, nei bausti**.*“ (2E, asmeninis interviu, 2022-07-26).	Pagalba įgyvendinant BDAR reikalavimus	VDAI darbo vertinimas, siekiant užtikrinanti Bendrojo duomenų apsaugos reglamento reikalavimų įgyvendinimo kontrolę
„*Kiek teko lankytis jų svetainėje, **vertingos, išsamios, tikslios informacijos apie asmens duomenų apsaugą pakanka**. <...> Valstybinė duomenų apsaugos inspekcija padarė milžinišką darbą, įgyvendinant Bendrojo duomenų apsaugos reglamento reikalavimus Lietuvoje. <...> Kontrolė, kaip įgyvendinami BDAR reikalavimai, priklauso ir nuo finansavimo iš valstybės biudžeto, valstybės tarnautojų ir darbuotojų inspekcijoje kiekio ir jų galimybių.*“ *(6E, asmeninis interviu, 2022-12-07).*		
„*Teisiniu aspektu, nagrinėjant asmens duomenų pažeidimus – tinkamai (gal kiek per mažai principingumo, ypač už asmens duomenų pažeidimus skiriant baudas). **Organizacinių ir techninių duomenų apsaugos priemonių įgyvendinimo monitoringo ir kontrolės vykdymo srityje – visiškai prastai**.*“ (5E, asmeninis interviu, 2022-11-25).	Trūkumas žmogiškųjų resursų	
„*Vidutiniškai. **Trūksta rekomendacijų, gairių, prevencinių priemonių taikymo vietoj baudimo**.*“ *(8E, asmeninis interviu, 2022-12-15).*		
„*Turime suprasti, kad **trūkumas žmonių ir specialistų** toje organizacijoje ir turimų patikrinimų skundų skaičius verčia ją tiesiog be sustojimo dirbti ir kartais kartoti tuos pačius ir tuos pačius darbus. Ir lieka vis mažiau laiko konsultacijoms, lieka vis mažiau laiko savo pozicijos reiškiniui. Aš negaliu vertinti nei neigiamai, nei teigiamai, tačiau žinau, kad jos yra užimtumo prasme ir žmogiškųjų išteklių trūkumo prasme apkrautos labai dideliu darbu, dėl to **negali savalaikiai reaguoti į vykstančius greitus procesus**.*“ *(9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

5. Kaip vertinate Nacionalinio kibernetinio saugumo centro darbą užtikrinant kontrolę kibernetinio saugumo reikalavimų įgyvendinimo kontekste? Atsakydami į klausimą 2E, 4E, 5E ir 8E ekspertai nurodė, kad NKSC trūksta žmogiškųjų resursų, todėl skiriamas per mažas dėmesys tam tikroms veikloms siekiant užtikrinti kibernetinio saugumo reikalavimų įgyvendinimo kontrolę. 3E ir 9E ekspertai mano, kad NKSC bendradarbiauja su organizacijomis ir tobulėja vykdydami kibernetinio saugumo reikalavimų įgyvendinimo kontrolės funkcijas (žr. 22 lentelę).

22 lentelė. NKSC darbo vertinimas, siekiant užtikrinti kibernetinio saugumo reikalavimų įgyvendinimo kontrolę

Interviu ištrauka	Subkategorija	Kategorija
„... ***NKSC trūksta įtaigių įrankių išsireikalauti tinkamos arba bent jau bazinės kibernetinio saugumo aplinkos***, *kas betarpiškai susiję ir su asmens duomenų apsauga, kai ji lieka tik formali, prisidengiant ne visada tobulais dokumentais ir taip suvokiant tinkamą atitiktį BDAR ar kitiems kibernetinį saugumą reglamentuojantiems teisės aktams.*“ (2E, asmeninis interviu, 2022-07-26).	Resursų ir tam tikrų veiklų trūkumas NKSC	NKSC darbo vertinimas, siekiant užtikrinanti kibernetinio saugumo reikalavimų įgyvendinimo kontrolę
„*Teigiamai, nors* ***galėtų būti ir daugiau padaryta, daugiau iškomunikuota, daugiau paruošta metodinių priemonių****. ES lygiu ruošiami nauji įstatymai ir esamų papildymai šiose srityse, tad neišvengiamai šios institucijos turės stiprėti ir duoti daugiau naudos.*“ *(4E, asmeninis interviu, 2022-09-14).*		
„*NKSC galėtų* ***daugiau dėmesio skirti stebėti organizacinių ir techninių elektroninės informacijos saugos ir kibernetinio saugumo priemonių įgyvendinimui****, tobulinti ARSIS sistemą ir pan.*“ *(5E, asmeninis interviu, 2022-11-25).*		
„*Vidutiniškai.* ***NKSC trūksta pajėgų atlikti reikalavimų įgyvendinimo patikrinimą*** *vietoje. Gerai - Mokymų/ KS pratybų organizavimo srityje – pažanga akivaizdi, teigiama ir pozityvi.*“ *(8E, asmeninis interviu, 2022-12-15).*		
„*Manyčiau šių institucijų* ***veikla efektyvi tuomet, jei su jomis geranoriškai bendradarbiauja****. Mano manymu, institucijos veikia gerai.*“ (3E, asmeninis interviu, 2022-08-05).	Bendradarbiavimas ir tobulėjimas	
„*Vertinu teigiamai. Iš pateikiamų ataskaitų ir iš to formalaus dokumentinio lygio, kiek yra pateikiamas, matome, kad jie* ***tobulėja ir tikrai kyla lygis aukštyn****.<> **Žinome bendradarbiavimą tarp privataus ir viešo sektoriaus. Mes matome įvairias iniciatyvas iš Centro****. Mes matome rekomendacijas visuomenės plačiajai daliai, pateiktus audiovizualinius dalykus, įrankius....*“ *(9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

Pusiau struktūruoto klausimyno **IV tyrimo dalį – Kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymo ir imties nustatymas**, sudaro 2 klausimai.

1. Kokių techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos įgyvendinimo priemonių pasigendate nacionaliniuose teisės aktuose? Atsakydami į klausimą 2E, 4E ir 8E ekspertai nurodė, kad trūksta aiškumo teisės aktuose, kaip, kokius ir kam techninius ir organizacinius reikalavimus įgyvendinti. 5E ir 9E ekspertai, mano kad teisės aktai turėtų būti papildyti naujomis techninėmis ir organizacinėmis priemonėmis, pvz. iš 2022 metų standarto ISO 27002. Taip pat svarbu

teisės aktuose akcentuoti, kad techninių ir organizacinių priemonių įsigijimo prioritetas negali būti žema jų kaina (žr. 23 lentelę).

23 lentelė. Techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos įgyvendinimo priemonių trūkumas nacionaliniuose teisės aktuose

Interviu ištrauka	Subkategorija	Kategorija
„*BDAR su laiku tampa vis aiškesnis <...>tuo tarpu **kibernetinio saugumo reglamentavimas dar nėra pakankamai tobulas**: trūksta aiškių atsakomybių nustatymo ir tų atsakomybių įteisinimo kibernetiniuose subjektuose, nepakankami įrankiai kontroliuojančioms institucijoms įgalinti organizacijas diegti nustatytus reikalavimus arba pačių **reikalavimų neadekvatumas pagal ūkio sektorius ar taikomas technologijas**...*“ (2E, asmeninis interviu, 2022-07-26).	Neaiškus techninių ir organizacinių priemonių taikymas	Techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos įgyvendinimo priemonių trūkumas nacionaliniuose teisės aktuose
„*Pagrindinė problema – **daug persidengiančių atskirų įstatymų, aprašų ir reikalavimų** (kai kurie jau neatitinka nūdienos realijų). Reikėtų vieningesnės sistemos, labiau apjungtų, koncentruotų įstatymų (geras pvz. yra BDAR) nustatančių kryptis, politikas.*“ (4E, asmeninis interviu, 2022-09-14).		
„***Minimalių priemonių**, taikomų valstybiniu, nacionaliniu mastu, ne tik valstybės informaciniams ištekliams bet ir **privačiame sektoriuje**. (8E, asmeninis interviu, 2022-12-15).*		
„*Techninės ir organizacinės asmens duomenų apsaugos priemonės nacionalinėse teisės aktuose nenumatytos, jos yra tik VDAI gairėse, kurios nėra privalomos asmens duomenų tvarkytojams ir valdytojams. Techninės ir organizacinės kibernetinio saugumo priemonės nacionalinėse teisės aktuose yra pakankamos, gal kiek mažiau dėmesio yra skiriama debesijos paslaugų apsaugos valdymui bei trečiųjų šalių teikiamų paslaugų kontrolei <...> **Reikėtų į Kibernetinio saugumo įstatymą perkelti kai kurias standarte ISO 27002:2022 naujai pasirodžiusias kontrolės priemones**.*“ *(5E, asmeninis interviu, 2022-11-25).*	Naujų techninių ir organizacinių perkėlimas į teisės aktus bei jų įsigijimo prioritetai	
„*Visi labiau norėtų, kad būtų detalizuota ir apibrėžta, ką konkrečiai naudoti. Mes matome, kad jau yra pasikeitę, kad suteikta galimybė nepirkti ir nesiremti kainos standartu. Aš norėčiau, kad būtų **aiškiau paaiškinta Viešųjų pirkimų tarnybos dokumentuose, kad kaina negali būti lemiamas dalykas**, ir organizacija turėtų suprasti, kad kaina tikrai ne pirmoje vietoje, taip pat ne pirmoje vietoje ir patirtis kitų organizacijų. Kartais organizacijos eina lengviausiu keliu perka viską vienodai, kaip ir kitos, net nesigilindamas į specifiką savo veiklos ir darbo...*“ *(9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

2. Kaip tobulintumėte techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos priemonių įgyvendinimo procesą organizacijoje? Atsakydami į klausimą 2E ir 4E ekspertai nurodė, kad trūksta aiškesnio reglamentavimo apie kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymą pagal organizacijų veiklos specifiką. 5E ir 9E ekspertai mano, kad reikia daugiau kvalifikuotų darbuotojų ir jų švietimo. 6E, 7E ir 8E ekspertai supaprastintų asmens duomenų apsaugos ir kibernetinio saugumo veiklos procesus ir atliktų būtinas konkrečias veiklas (žr. 24 lentelę).

24 lentelė. Techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos priemonių įgyvendinimo proceso organizacijoje tobulinimas

Interviu ištrauka	Subkategorija	Kategorija
„***kibernetinio saugumo techninių priemonių skirstymo pagal organizacijų ūkio sektorius ar vykdomą veiklą***, *aiškesnio YSII identifikavimo metodų ar platesnio identifikavimo profiliavimo.*“ (2E, asmeninis interviu, 2022-07-26).	Kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymas pagal organizacijas	Techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos priemonių įgyvendinimo procesą organizacijoje tobulinimas
„*Teisės aktuose neturėtų būti konkrečių organizacinių ir tuo labiau techninių priemonių. Juose turėtų būti bendro pobūdžio politikos ir kryptys, turėtų būti paminėtos visuotinai priimtos gerosios praktikos.* ***Įmonės pagal savo specifiką ir įstatymų reikalavimus turėtų rinktis ką ir kaip taikyti****. Kibernetinis saugumas greitai vystosi ir keičiasi. Konkretumai verčia pastoviai keisti įstatymus, kas nėra geras dalykas.*“ (4E, asmeninis interviu, 2022-09-14).		
„*reiktų* ***kelti darbuotojų kvalifikaciją*** *kibernetinio saugumo ir asmens duomenų apsaugos srityje, didinti darbuotojų atsparumą socialinei inžinerijai.*“ *(5E, asmeninis interviu, 2022-11-25).*	Kvalifikuoti darbuotojai ir jų švietimas	
„*Iš esmės aš* ***įtraukčiau daugiau darbuotojų****. Kitaip tariant, organizacija turėtų aiškiai deklaruoti. Na, bent jau planus ateičiai <...> Aš tobulinčiau įtraukdamas darbuotojus, aiškindamas tai kas ne tik formaliuose mokymuose, bet naudodamas žaidybinimo principus (angl. Game unification), tai yra daryčiau atraktyviai, skatinčiau juos...*“ *(9E, asmeninis interviu, 2022-01-05).*		
„*Padaryčiau jį* ***labiau suprantamą*** *ir patrauklesnį ir, jeigu įmanoma,* ***paprastesnį****. Apie sudėtingus dalykus paprastai.*“ *(6E, asmeninis interviu, 2022-12-07).*	Procesų paprastinimas ir konkrečios veiklos	
„*stalo pratybų įgyvendinimas,* ***periodinis procesų peržiūrėjimas ir atnaujinimas***“ *(7E, asmeninis interviu, 2022-12-08).*		
„*...****trūksta*** *leistinos programinės įrangos sąrašų, trūksta rekomendacijų dėl laisvai platinamos programinės įrangos, saugumo reikalavimų perkant debesijos ar kt. paslaugas.*“ *(8E, asmeninis interviu, 2022-12-15).*		

Šaltinis: sudaryta autoriaus

Pusiau struktūruoto klausimyno **V tyrimo dalį – Informacinių technologijų saugos atitikties vertinimas**, sudaro 4 klausimai.

1. Kaip užtikrinti nuolatinį kibernetinio saugumo ir asmens duomenų apsaugos dokumentacijos peržiūros ir, esant poreikiui, atnaujinimo procesą? Atsakydami į klausimą 1E ir 8E ekspertai nurodė, kad nuolatinis kibernetinio saugumo ir asmens duomenų apsaugos dokumentacijos peržiūros ir, esant poreikiui, atnaujinimo procesas galėtų būti užtikrinimas atliekant rizikos ir atitikties teisės aktams analizę. 2E, 5E ir 7E ekspertai, mano automatizuotos priemonės palengvintų atitinkamų darbų įgyvendinimą. 3E, 4E ir 9E ekspertai teigia, kad atsakingi asmenys – vadovai, asmens duomenų apsaugos pareigūnas ir informacijos saugos įgaliotinis turėtų užtikrinti reikalavimų įgyvendinimą (žr. 25 lentelę).

25 lentelė. Nuolatinis kibernetinio saugumo ir asmens duomenų apsaugos dokumentacijos peržiūros ir, esant poreikiui, atnaujinimo proceso užtikrinimas

Interviu ištrauka	Subkategorija	Kategorija
„***Susieti su nuolatine organizacijos veiklos rizikos analize.***“ (1E, asmeninis interviu, 2022-06-30).	Rizikos vertinimas ir atitiktis	Nuolatinis kibernetinio saugumo ir asmens duomenų apsaugos dokumentacijos peržiūros ir, esant poreikiui, atnaujinimo proceso užtikrinimas
„***Užtikrinti atitiktį veiklos procesams****. Atitiktis turi būti ne formali. Be to svarbu paskirti saugos įgaliotinį turintį atitinkamas kompetencijas, t. y. ne formaliai atsakingą už šią funkciją (pvz. administratorių ar kt.).“ (8E, asmeninis interviu, 2022-12-15).*		
„***Pokyčių valdymo procedūros bei jų atlikimo kontrolė, kuo daugiau automatizuotų procesų*** *su patvirtinimo reikalavimu apie atliktus rutininius darbus, tame tarpe dokumentacijos peržiūros ir pan.*“ (2E, asmeninis interviu, 2022-07-26).	Automatizacija	
„***įsidegti ISVS ir jį sertifikuotis, nes ISVS turi savikontrolės mechanizmą****, o sertifikavimo procesas užtikrina nepriklausomų auditorių audito procesą.“ (5E, asmeninis interviu, 2022-11-25).*		
„*Pasitelkiant IT technologijas* ***automatizuoti procesą****“ (7E, asmeninis interviu, 2022-12-08).*		
„*Manau, užtikrinti galima tinkama,* ***proaktyvia DAP ir ISĮ veikla****.“ (3E, asmeninis interviu, 2022-08-05).*	Atsakingi asmenys	
„*Reikia,* ***kad aukščiausio lygio vadovai būtų tuo suinteresuoti ir tai nustatytų privalomomis taisyklėmis****.“ (4E, asmeninis interviu, 2022-09-14).*		
„*... dokumentas organizacijoje turi būti gyvas ir tol* ***kol organizacijos vadovui tai nerūpės asmeniškai, tai joks saugos įgaliotinis ar duomenų apsaugos pareigūnas, ar kitas asmuo paskirtas už kibernetinio saugumo politikos įgyvendinimą organizacijoje pats vienas jis to nepadarys, domėtis turi visi****. <...> jisai turi ir aiškinti kitiems būtinybę, kodėl tai reikalinga ir kam“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

2. Kokios priežastys lemia, kad kai kurios organizacijos periodiškai neatlieka rizikos ir atitikties vertinimų, kaip būtų galima tobulinti šias priemones? Atsakydami į klausimą 1E, 2E, 3E, 4E, 5E ir 8E ekspertai nurodė, kad rizikos ir atitikties vertinimų periodinio neatlikimo priežastys kai kuriose organizacijose yra brandos ir kompetencijų trūkumas. 7E ir 9E ekspertai, mano kad organizacijoms trūksta specialistų, kurie atliktų rizikos ir atitikties vertinimą (žr. 26 lentelę).

26 lentelė. Rizikos ir atitikties vertinimų periodinio neatlikimo priežastys kai kuriose organizacijose ir tobulinimo priemonės

Interviu ištrauka	Subkategorija	Kategorija
„*Manau tokį požiūrį lemia **„žema“ organizacijos IT valdymo branda**, tokių vertinimų formalaus atlikimo, neanalizuojant realaus poveikio organizacijai galimybių, ankstesnė patirtis, taip nesukuriant realios naudos organizacijai, **kompetencijų trūkumas**.*“ (1E, asmeninis interviu, 2022-06-30).	Organizacijos brandos ir kompetencijų trūkumas	Rizikos ir atitikties vertinimų periodinio neatlikimo priežastys kai kuriose organizacijose ir tobulinimo priemonės
„***naudos suvokimo, brandos ir kompetencijų šioje srityje trūkumas**, taip pat nepakankama motyvacija iš teisės aktų pusės.*“ (2E, asmeninis interviu, 2022-07-26)		
„***Trūksta ISĮ ir DAP kompetencijos**.“ (3E, asmeninis interviu, 2022-08-05).*		
„*Dažniausiai tokiais atvejais į tuos procesus nebūna **įsitraukę ir jais nesidomi aukščiausio lygio vadovai**. Greičiausiai organizacija nenaudoja visuotinai priimtų gerųjų praktikų sprendimams priimti ir neturi gerąja praktika paruoštos valdymo ir administravimo struktūros.“ (4E, asmeninis interviu, 2022-09-14).*		
„***nežino**, kad tai yra organizacinė priemonė, **leidžianti įsivertinti priemonių pakankamumą ir tinkamai valdyti su tuo susijusias rizikas**. Šių priemonių įgyvendinimui naudoti automatizuotus įrankius (sprendimus, sistemas). VDAI gaires papildyti organizacine priemone – Atlikti informacijos saugumo rizikos vertinimą.“ (5E, asmeninis interviu, 2022-11-25).*		
„***Įdiegti ISVS (Informacijos saugumo valdymo sistemą), užtikrinti procesinį valdymą**.“ (8E, asmeninis interviu, 2022-12-15).*		
„*Įmonės dažniausiai skiria mažą biudžetą IT saugumui užtikrinti, **trūkumas šios srities specialistų** ir/arba pareigų dubliavimas su kitomis IT specialisto funkcijomis“ (7E, asmeninis interviu, 2022-12-08).*	Specialistų trūkumas	
„*Žmogiškasis faktorius, kad tiesiog **neturi specialistų, gebančių tai padaryti** arba jeigu turi specialistą, kuris geba tai padaryti <...>tačiau jis nėra dedikuotas tik tai funkcijai atlikti. Jis dažniausiai užsiima ir kitais darbais...“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

3. Kaip turėtų būti organizuojamas kibernetinio saugumo ir asmens duomenų apsaugos mokymo procesas organizacijoje? Atsakydami į klausimą 1E, 4E, 6E, 7E ir 8E ekspertai nurodė, kad kibernetinio saugumo ir asmens duomenų apsaugos mokymai turėtų vykti periodiškai, įskaitant nuolatinį mokymąsi, atsižvelgiant į darbuotojų funkcijas. 2E, 5E ir 9E ekspertai, mano kad kibernetinio saugumo ir asmens duomenų apsaugos mokymai turėtų būti individualizuoti pagal darbuotojus ir temas (žr. 27 lentelę).

27 lentelė. Kibernetinio saugumo ir asmens duomenų apsaugos mokymo proceso organizavimas organizacijoje

Interviu ištrauka	Subkategorija	Kategorija
„*Turėtų vykti **bent kartą į metus bendro pobūdžio** šių sričių žinių atnaujinimo ir supažindinimo su aktualijomis mokymai, seminarai*“ (1E, asmeninis interviu, 2022-06-30).	Periodinis ir nuolatinis mokymasis	Kibernetinio saugumo ir asmens duomenų apsaugos mokymo proceso organizavimas organizacijoje
„*Tai turėtų būti **nenutrūkstamas procesas**, su už to proceso vyksmą ir sėkmę atsakingais darbuotojais.“ (4E, asmeninis interviu, 2022-09-14).*		
„***Reguliariai**. Sklandžiai. Įdomiai. Apie sudėtingus dalykus paprastai.“ (6E, asmeninis interviu, 2022-12-07).*		
„*Turi būti **nuolatinis mokymo procesas**, atsižvelgiant į darbuotojų atliekamas funkcijas ir pritaikytas jų poreikiams <...>.“ (7E, asmeninis interviu, 2022-12-08).*		
„*Manau turėtų būti vykdomi **tiek nuolatiniai tiek periodiniai mokymai** tiek ad hoc mokymai. Visuose mokymuose turi būti skiriamas dėmesys tiek kibernetiniam saugumui, tiek asmens duomenų apsaugai, tiek fizinei saugai. Mokymai turėtų būti tiek vidiniai, t. y. organizuojami saugos įgaliotinio, atsakingo už kibernetinio saugumo organizavimą asmens, duomenų apsaugos pareigūno, tiek išoriniai, pvz. organizuojami išorinių ekspertų ar kompetentingų institucijų (Pvz. NKSC ir VDAI). Svarbu, kad tokius mokymus kompetentingos institucijos organizuotų ne tik viešajam sektoriui, bet ir privačiam.“ (8E, asmeninis interviu, 2022-12-15).*		
„***profiliuojant pagal mokymo auditoriją** (naujokai, pasikartojantys pažeidėjai ir pan.), automatizuoti (įvairių platformų, kaip Microsoft LMS 365 naudojimas) su galimybe gauti įrodymus apie pasiektą kvalifikaciją, vadovybės palaikymas skiriant mokymams reikalingas lėšas kas metai ir pan.*“ (2E, asmeninis interviu, 2022-07-26).	Individualūs mokymai pagal žinias	
„*geriausia **naudoti nuotolinio mokymų platformas** arba jų pagrindu paslaugas, kurios savyje turėtų kontrolinių klausimų modulį ir (ar) socialinės inžinerijos organizavimo funkcionalumą.“ (5E, asmeninis interviu, 2022-11-25).*		

*„Ne bendrai ir ne formaliai, kad tiesiog temos ir pasakoja, bet galbūt tikriausiai **pagal turimas žinias ir skyrius**, ir atskirus darbuotojus dėl to, kad darbuotojai visi kartu būdami krūvoje, kartais nepatogu ir bijo užduoti klausimus...“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

4. Kaip užtikrinti/kontroliuoti paslaugų teikėjų atitiktį kibernetinio saugumo ir asmens duomenų apsaugos reikalavimams? Atsakydami į klausimą 1E, 2E, 4E, 5E, 7E, 8E ir 9E ekspertai nurodė, kad asmens paslaugų teikėjų kibernetinio saugumo ir asmens duomenų apsaugos atitikties reikalavimų užtikrinimas/kontrolė galima perkėlus reikalavimus į sutartis ir atliekant vertinimas – atitikties ir rizikos bei auditus (žr. 28 lentelę).

28 lentelė. Paslaugų teikėjų kibernetinio saugumo ir asmens duomenų apsaugos atitikties reikalavimų užtikrinimas/kontrolė

Interviu ištrauka	Subkategorija	Kategorija
„***Perkelti būtinus reikalavimus į sutartis** (susitarimus) ir **rizikos analizės**, **auditų metu vertinti** faktinį perduotų trečiosioms šalims paslaugų reikalavimų įgyvendinimą, **vykdyti stebėseną**.“ (1E, asmeninis interviu, 2022-06-30).	Reikalavimų perkėlimas į sutartis ir vertinimas	Paslaugų teikėjų kibernetinio saugumo ir asmens duomenų apsaugos atitikties reikalavimų užtikrinimas/ kontrolė
„***reguliarūs atitikties vertinimų** kontroliuojančioms institucijoms ataskaitų pateikimas, **neplanuoti auditai**, savarankiško vertinimo reikalavimai.“ (2E, asmeninis interviu, 2022-07-26).		
„***Pradinių reikalavimų (politikos) buvimas**, teisingo **kontrakto** su paslaugų teikimo lygio susitarimu **pasirašymas**.“ (4E, asmeninis interviu, 2022-09-14).*		
*„Tinkamai įgyvendinti **standarte ISO 27001:2022 numatytas kontrolės priemones**, susijusias su trečiųjų šalių valdymu.“ (5E, asmeninis interviu, 2022-11-25).*		
„***Periodiškai reikalauti iš teikėjų pateikti ataskaitas**.“ (7E, asmeninis interviu, 2022-12-08).*		
„***Nustatyti juos pirkimo dokumentuose**, asmens duomenų tvarkymo sutartyse ir **kontroliuoti ar nustatyti reikalavimai įgyvendinami**. Pvz. atlikti patikrinimus vietoje.“ (8E, asmeninis interviu, 2022-12-15).*		
*„... bent jau **domėjimasis kompanija**. Na ir prašymas savalaikiai reaguoti į viską turėtų būti prioritetas. Priešingu atveju formalios atitikties vertinimas. Tai yra tik turimų dokumentų apžvalga ir peržiūrėjimas. Na, jis nėra pakankamas, turėtų **remtis ir praktine patirtimi bendravimo su organizacija**“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

Pusiau struktūruoto klausimyno **VI tyrimo dalį – Asmens duomenų tvarkymo teisėtumo nustatymas**, sudaro 2 klausimai.

1. Dėl ko daugelis organizacijų neteisėtai tvarko interneto svetainių slapukus (angl. *Cookies*)? Atsakydami į klausimą 2E, 3E, 4E, 5E, 6E, 7E, 8E ir 9E ekspertai nurodė, kad neteisėtai tvarkomų interneto svetainių slapukų daugelyje organizacijų priežastis yra nežinojimas arba tyčia, taip kontroliuojančių institucijų veiksmų stoka (žr. 29 lentelę).

29 lentelė. Neteisėtai tvarkomų interneto svetainių slapukų daugelyje organizacijų priežastis (angl. *Cookies*)?

Interviu ištrauka	Subkategorija	Kategorija
„***kontroliuojančių ir įgyvendinančių žmogiškųjų išteklių trūkumas, kompetencijos ir kvalifikacijos trūkumas**, netinkamo prioriteto šiais sričiai nustatymas, **nedidelė skundų dėl netinkamo slapukų naudojimo dalis iš duomenų subjektų kontroliuojančioms institucijoms**.*“ (2E, asmeninis interviu, 2022-07-26).	Nežinojimas, tyčia ir kontroliuojančių institucijų veiksmų stoka	Neteisėtai tvarkomų interneto svetainių slapukų daugelyje organizacijų priežastis
„***Manymas, kad cookies užtikrins didesnį pelną** (reklama ir t.t.), gal **nesuvokia realios sankcijų grėsmės**, nes niekad su tuo nesusidūrė ir **nėra praktikos**.*“ (3E, asmeninis interviu, 2022-08-05).		
„***Žinių trūkumas, žmogiškųjų išteklių trūkumas bei jų kaštai, kibernetinės kultūros stoka.**“ (4E, asmeninis interviu, 2022-09-14).*		
„***dėl nežinojimo, dėl nori kaupti perteklinius duomenis**.*“ *(5E, asmeninis interviu, 2022-11-25).*		
„***Prižiūrinčios institucijos kontrolės stokos**. **Nebaudžiamumo. Neišprusimo**. <...> Švietimo stokos. Nors po BDAR priėmimo jau praėjo šeši metai, vis dar yra organizacijų, ypatingai, nedidelių, kurios apie BDAR girdi pirmąkart arba turi apie jį mažai žinių.*“ *(6E, asmeninis interviu, 2022-12-07).*		
„***Neteisėtai tvarko, nes nori surinkti daugiau informacijos apie potencialius tinklapio vartotojus**, pateikt jiems personalinius pasiūlymus ir padidinti pardavimus.*“ *(7E, asmeninis interviu, 2022-12-08).*		
„*Arba **trūksta suvokimo/kompetencijų arba tyčia**, nes analizuojama surinkta informacija.*“ *(8E, asmeninis interviu, 2022-12-15).*		
„*Yra dvi priežastys, tas žodis **neteisėtas**, tai gali būti dėl tam tikro paprasčiausiai nematomumo ar net latentiškumo gali būti jisai dirbtinis. Tai yra, kai tiesiog nepatogu, tiesiog **norima surinkti**, bet nenorima rodyti, nes didelis vartotojų nesutiks. Tai galima sakyti tyčia, o **didžiąja dalimi tai daroma nesuprantant** kartais dėl to, kad kompanijos užsakydamos svetaines ar puslapius, ar prižiūrėdamas jas net nežino, kokie techniniai slapukai techninio lygio slapukai sudėti.*“ *(9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

2. Kaip paskatinti organizacijas tvarkyti interneto svetainių slapukus teisėtai? Atsakydami į klausimą 1E, 3E, 4E, 5E, 6E ir 8E ekspertai nurodė, kad turėtų būti parengta daugiau medžiagos, kaip tinkamai rinkti slapukus organizacijoje ir viešinti esamą situaciją apie netinką slapukų naudojimą. 2E, 7E ir 9E ekspertai, mano svarbu turėti tinkamus įrankius, kurių pagalba būtų galima teisėtai tvarkyti slapukus interneto svetainėse (žr. 30 lentelę).

30 lentelė. Paskatinimas organizacijas tvarkyti interneto svetainių slapukus teisėtai

Interviu ištrauka	Subkategorija	Kategorija
„***Prevencinė, švietėjiška veikla, viešinami informacijos apie tinkamą slapukų naudojimą pavyzdžiai....***“ (1E, asmeninis interviu, 2022-06-30)	Švietimas ir informacijos viešinimas apie netinkamą slapukų naudojimą	Paskatinimas organizacijas tvarkyti interneto svetainių slapukus teisėtai
„***Daugiau šviečiamosios veiklos****....*“ (3E, asmeninis interviu, 2022-08-05)		
„*Mano nuomone, reikėtų **daugiau šviesti ir pačias organizacijas** (duomenų **valdytojus) ir naudotojus**. Neteisėtas asmeninės informacijos tvarkymas gali sukelti daug problemų duomenų valdytojui, jeigu naudotojas supras kas vyksta ir kreipsis į atitinkamas instancijas.“ (4E, asmeninis interviu, 2022-09-14).*		
„***edukuoti** ir bausti.“ (5E, asmeninis interviu, 2022-11-25).*		
„***Viešinti atvejus apie už neteisėtą interneto svetainių slapukų tvarkymą nubaustus asmenis**. Kalbėti apie privalumus, pliusus tvarkant interneto svetainių slapukus teisėtai.“ (6E, asmeninis interviu, 2022-12-07).*		
„***Parengti aiškias gaires**, pvz. pavyzdines tipines informavimo apie slapukus rekomendacijas.“ (8E, asmeninis interviu, 2022-12-15).*		
„*... **sprendimų interneto svetainių platformoms dėl slapukų tinkamo naudojimo populiarinimas**, trečių šalių (Google ir pan.) paslaugų kontrolė iš kontroliuojančių asmens duomenų apsauga ir reglamento įgyvendinimą institucijų.“ (2E, asmeninis interviu, 2022-07-26).*	Tinkamų įrankių naudojimas	
„*Interneto svetainių slapukų reguliavimas turi būti valdomas valstybės lygmenyje, taikant <...> nuobaudas už nusižengimus ir bendradarbiaujant su stambiais **IT rinkos dalyviais, įpareigojant jas kurti saugias ir reikalavimus atitinkančias sistemas**.“ (7E, asmeninis interviu, 2022-12-08).*		
„***Tikriausiai naudotis įrankiais**, vertinti juos, galbūt automatizuoti procesus. <...> organizacijos matydamos patirtį kitų organizacijų, pačios norės tvarkytis iš esmės. Baudimu mes nieko nepasieksime, nes vienoks ar kitoks slapukas, koks yra tas priežastinis ryšys tarp rinkimo ir potencialios žalos sunkiai įrodomas...“ (9E, asmeninis interviu, 2022-01-05).*		

Šaltinis: sudaryta autoriaus

Apibendrinant galima teigti, kad asmens duomenų apsauga sumažina kibernetinio pažeidžiamumo riziką panaudoti netinkamai saugomus duomenis. Asmens duomenys yra neatsiejama organizacijos veiklos vykdymo dalis, todėl organizacijos norėdamos užtikrinti saugų asmens duomenų tvarkymą privalo taikyti kibernetinio saugumo priemones. Organizacijoje užtikrindamas Reglamento reikalavimų įgyvendinimą, siekiant teisėto ir saugaus asmens duomenų tvarkymo, duomenų apsaugos pareigūnas galėtų turėtų didesnius įgaliojimus, lemiančius galutinį spendimą dėl asmens duomenų apsaugos. Organizacija tobulindama veiklos procesus asmens duomenų apsaugos kontekste turėtų mąstyti ne apie patogumą, bet apie saugumą vadovaudamasi teisės aktais ir visuotinai pripažinta gerąją praktika nustatyta tarptautiniuose standartuose. Pastebėtina, kad kibernetinio saugumo priemonės yra nurodytos disertacijos 2 priede atlikus pirmąjį tyrimą. Teisinį reglamentavimą nuolatos reikia tobulinti, kad jis atitiktų besikeičiančias technologijas ir organizacijų vykdomos veiklos ypatumus. Tuo tarpu NKSC turėtų plėsti organizacijų imtį, kurias galėtų kontroliuoti, stebėti ir įpareigoti užtikrinti kibernetinio saugumo priemonių įgyvendinimą. Valdymo procesai atskleidžia organizacijos brandą, jų užtikrinimas turėtų būti kontroliuojamas nustačius tinkamas procedūras. Organizacijoje kibernetinio saugumo kultūrą formuoja vadovybė, viskas prasideda nuo jos suvokimo ir skatinimo, pvz. rengiant periodinius mokymus. Atlikus antrąjį disertacijos tyrimą – Atitikties vertinimą 3 organizacijose buvo nustatyta, kad jos periodiškai neatlieka kibernetinio saugumo mokymų. Komunikacija užtikrina informacijos sklaidą, kas tai nebūtų ar reagavimas į incidentus, ar kibernetinio saugumo priemonių įgyvendinimas, suteikdama galimybę greičiau ir tinkamai reaguoti esamoje situacijoje. Saugos įgaliotinis turėtų turėti platų matymą įvairių kibernetinio saugumo aspektų apimančių įvairias sritis, todėl organizacijai reikia nuolatos kelti jo kvalifikaciją ir užtikrinti kompetenciją atitinkantį atlygį, kadangi rinkoje jaučiamas šių specialistų trūkumas. Formalus BDAR ir kibernetinio saugumo teisės aktų atitikties įgyvendinimas atskleidžia organizacijos žemą brandą ir nepagarbą žmogaus teisėms bei nesuvokimą dėl to kylančių, asmens duomenų saugumo pažeidimų ir kibernetinių incidentų, rizikų. Tai gali lemti įvairios aplinkybės – reikalavimų nežinojimas, finansinė našta, realių sankcijų nebuvimas, kompetencijų trūkumas. Atlikus disertacijos trečiąjį tyrimą pastebėta, kad dauguma organizacijų interneto svetainėse neteisėtai tvarko asmens duomenis – slapukus, tai gali lemtis šiame tyrime aukščiau išvardintos apilnkybės. Ši padėtis galėtų būti spendžiama VDAI ir NKSC didesniu įsitraukimu užtikrinant organizacijų stebėseną ir kontrolę, švietimu ir mokymų organizavimu bei teisės aktuose atsakomybės įtvirtinimu. Organizacijos prioritetą dažnu atveju teikia techninėms, o ne organizacinėms priemonėms, nes technines priemones galima nupirkti ir parodyti, o organizacinės sunkiau įgyvendinamos ir kontroliuojamos. Tačiau turėtų būti randamas balansas tarp abiejų priemonių įgyvendinimo, nes techninės priemonės tinkamai neveiks be organizacinių priemonių, pvz. tinkamai apibrėžto proceso ir nustatytų procedūrų jam įgyvendinti, taip pat galimos žmogiškosios klaidos.

4. ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE SISTEMOS MODELIO KŪRIMAS

Šioje disertacinio darbo dalyje bus atliekama koncepcinio asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio, skirto sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas organizacijoje, pateikiant rekomendacijas ir pasiūlymus, kokios saugaus valdymo priemonės turi būti naudojamos, atsižvelgiant į mokslinių tyrimų metu gautus duomenis. Svarbu pabrėžti, kad, aptariant asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio struktūrą disertaciniame darbe, nėra nagrinėjami konkretūs technologiniai sprendimai, techninė ir programinė įranga ir priemonės, kurios yra naudojamos kibernetinio saugumo ir asmens duomenų apsaugos užtikrinimo procese, bei šių priemonių taikymo efektyvumas.

Analizuojamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis yra technologiškai neutralus, o technologinių priemonių panaudojimas ir kibernetinio saugumo bei asmens duomenų apsaugos technologinių procesų realizavimas nėra nagrinėjamas šiame disertaciniame darbe.

Nagrinėjant asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio struktūrą ir jo pritaikomumą įgyvendinti organizacijoje, valdančiose ir/ ar tvarkančiose asmens duomenis, yra pateikiamos tam tikros priemonės, kuriomis galima sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas organizacijoje. Konceptualus asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis yra pateikiamas 16 paveiksle. Modelio konstravimas buvo vykdomas vadovaujantis T. Parsonso struktūrinio funkcionalizmo principais. Anot T. Parsonso kiekviena visuomenė susideda iš posistemių, kurios skiriasi pagal savo struktūrą ir funkcinę reikšmę platesnei bendruomenei. Socialinis gyvenimas kaip sistema reikalauja jos elementų priklausomybės, o tai lemia socialinį stabilumą. Todėl bet kuri sistema, siekdama išlaikyti ir sustiprinti savo struktūrines ribas, privalo atliepti keturis funkcinius principus, kurios turi būti įvykdytos, kad sistema tinkamai veiktų:

- Prisitaikymas (angl. *Adaptation*) – Sistema turi prisitaikyti prie aplinkos ir jos pokyčių, įskaitant tai, kaip individų elgesys sistemoje gali būti pritaikytas prie aplinkos.
- Tikslo siekimas (angl. *Goal Attainment*) – Sistema turi apibrėžti tikslus ir sutelkti sistemos komponentus pagrindiniams tikslams pasiekti. Būtina išsikelti prioritetinius tikslus.
- Integracija (angl. *Integration*) – Sistema turi reguliuoti santykius tarp elementų, kad visi komponentai veiktų subalansuotai.
- Latentinės struktūros priežiūra (angl. *Latency*) – Sistema turi papildyti, palaikyti ir tobulinti individualią motyvaciją ir kultūrinius modelius, kurie sukuria ir palaiko tą motyvaciją. Jei elgesys yra nukrypęs, jis išsprendžiamas susitarimais, kurie nuolat atnaujinami. Ši funkcija yra susijusi su normomis ir modelių palaikymu (Parsons ir Gerald, 1973; Ritzer, 2004; Mensah, 2019; Čižikienė, 2020; Rusydiyah ir Rohman, 2020; Agafonov, 2021).

Detaliai asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos ir kibernetinio saugumo dimensijos yra išanalizuotos sekančiuose disertacijos poskyriuose.

Atsižvelgiant į asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių empirinių tyrimų metu gautus rezultatus, galima teigti, kad asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio įgyvendinimą organizacijoje yra tikslinga vykdyti etapais. Kuriamo konceptualaus asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio įgyvendinimas organizacijoje yra daug resursų reikalaujantis procesas. Siekiant supaprastinti šio asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio įdiegimą organizacijoje, yra numatomas modelio priemonių įgyvendinimas pakopomis, išskiriant keturis asmens duomenų apsaugos ir kibernetinio saugumo valdymo modelio lygius:

1. Supratimo (I lygis).
2. Įgyvendinimo (II lygis).
3. Užtikrinimo/ tobulinimo (III lygis).
4. Integruotąjį (IV lygis).

Supratimo (I), įgyvendinimo (II) ir užtikrinimo/ tobulinimo (III) lygių įgyvendinimas suteikia organizacijai galimybę stebėti asmens duomenų apsaugos ir kibernetinio saugumo įgyvendinimo pokyčius pagal priemonių laipsnišką įgyvendinimą lygiais konkrečiose dimensijose, kiekviena asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio priemonė gali būti įgyvendinama, neatsižvelgiant į kitas priemones. Vėliau, asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos ir kibernetinio saugumo dimensijose organizacijai pasiekus užtikrinimo/ tobulinimo (III) lygį (įgyvendinus visas priemones), organizacija pereina į integruotąjį asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio įgyvendinimo etapą, kuomet kiekvienos priemonės svyravimas iš tam tikros stabilios būsenos automatiškai sukelia kitų priemonių įgyvendinimo pokyčius.

Pažymėtina, kad asmens duomenų apsaugos ir kibernetinio saugumo siūlomo konceptualaus asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio dimensijų supratimo (I) lygmuo yra siejamas su organizacijos gebėjimais aiškiai nustatyti, kokius asmens duomenų apsaugos ir kibernetinio saugumo veiksmus privalu atlikti organizacijoje. Įgyvendinimo (II) lygmuo asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelyje yra orientuotas į konkrečių organizacijos pokyčiams būtinų priemonių įgyvendinimą, kurie suteikia organizacijai galimybę pagerinti savo asmens duomenų apsaugą ir kibernetinį saugumą asmens duomenų apsaugos ir kibernetinio saugumo dimensijų ribose. Užtikrinimo/ tobulinimo (III) lygmuo yra skirta užtikrinti II lygio priemonės taikymą ir/ar jį patobulinti. Integravimo (IV) lygmuo yra skirtas visų asmens duomenų apsaugos ir kibernetinio saugumo dimensijose priemonių įgyvendinimui harmonizuoti, siekiant užtikrinti visapusišką asmens duomenų apsaugą ir kibernetinį saugumą bei jo valdymą organizacijoje.

Kaip jau buvo minėta anksčiau, supratimo (I), įgyvendinimo (II) ir užtikrinimo/ tobulinimo (III) lygių įgyvendinimas asmens duomenų saugaus valdymo elektroninėje

erdvėje sistemos modelyje gali būti diegiamas atskiruose asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio dimensijose nepriklausomai, tačiau, tik asmens duomenų apsaugos ir kibernetinio saugumo dimensijose pasiekus užtikrinimo/ tobulinimo (III) lygį, atsiranda galimybė pereiti į integruotąjį (IV) lygį.

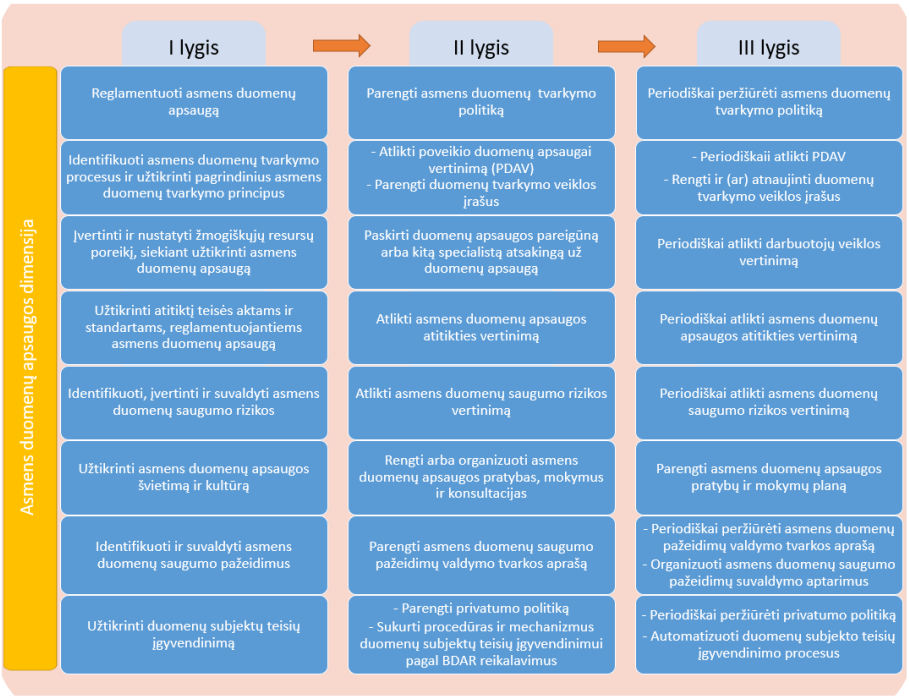
Šioje disertacinio darbo dalyje yra pateikiamas konceptualus asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis (žr. 16 paveikslas), skirtas sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas organizacijoje, pateikiant rekomendacijas ir pasiūlymus, kokios saugaus valdymo priemonės turi būti naudojamos, atsižvelgiant į mokslinių tyrimų metu gautus duomenis. Svarbu pabrėžti, kad, aptariant asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio struktūrą disertaciniame darbe, nėra nagrinėjami konkretūs technologiniai sprendimai – techninė ar programinė įranga, kurie yra naudojami užtikrinti kibernetinio saugumo ir asmens duomenų apsaugos įgyvendinimą organizacijoje.

16 pav. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis
Šaltinis: sudaryta autoriaus

Detaliai asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos ir kibernetinio saugumo dimensijose nurodytų priemonių lygio įgyvendinimas yra išanalizuotas sekančiuose disertacijos poskyriuose.

4.1. Asmens duomenų apsaugos dimensijos analizė

Asmens duomenų apsaugos dimensija asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kontekste yra svarbi asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio dalis. Būtent ši sritis atsakinga už teisėtą asmens duomenų tvarkymą ir atitinkamas technines ir organizacines priemones, siekiant apsaugoti pagrindines duomenų subjekto teises ir laisves, visų pirma jų teisė į asmens duomenų apsaugą. Asmens duomenų apsaugos dimensija yra grafiškai pavaizduota žemiau esančiame paveiksle (žr. 17 pav.).



17 pav. Asmens duomenų apsaugos dimensija

Šaltinis: sudaryta autoriaus

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos 1 priemonės detalizavimas (žr. 31 lentelę).

31 lentelė. Asmens duomenų apsaugos dimensijos 1 priemonė

1 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Reglamentuoti asmens duomenų apsaugą.	Parengti asmens duomenų tvarkymo politiką.	Periodiškai peržiūrėti asmens duomenų tvarkymo politiką.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 1 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Reglamentuoti asmens duomenų apsaugą. Organizacija privalo žinoti kokie teisės aktai reglamentuojantys asmens duomenų apsaugą yra taikomi, siekiant įgyvendinti jų reikalavimus. Pagrindinis iššūkis, susijęs su BDAR įgyvendinimu, yra tai, kad organizacijos nežino ir nesuvokia būsimų pokyčių ir reikalavimų, kuriuos BDAR nustato. Šie reikalavimai turi įvairių praktinių pasekmių organizacijos procesams ir praktikai, technologinių sistemų projektavimui, taip pat personalo mokymui ir naujų pareigų skyrimui organizacijose. Tokie reikalavimai iškelia būtinybę peržiūrėti esamą duomenų tvarkymo praktiką ir technologines duomenų apsaugos priemones, taip pat galbūt planuoti naujas, kad būtų užtikrinta BDAR atitiktis (Tikkinen-Piri ir kt., 2018).
2. **II lygis**.
   Parengti asmens duomenų tvarkymo politiką. Organizacija siekdama įgyvendinti teisės aktų reglamentuojančių asmens duomenų apsaugą reikalavimus jų nuostatus perkelia į vidaus dokumentus. Asmens duomenų politika turėtų reglamentuoti asmens duomenų tvarkymą pagal BDAR reikalavimus. Šią politiką galima reglamentuoti viename vidaus teisės akte arba atskiruose vidaus teisės aktuose, priklausomai nuo organizacijos apsisprendimo. Asmens duomenų politikos turinys, priklauso nuo organizacijos veiklos pobūdžio ir asmens duomenų tvarkymo procesų ir procedūrų bei taikomų techninių ir organizacinių priemonių. Asmens duomenų politikos turinį gali sudaryti, įskaitant bet neapsiribojant: Asmens duomenų valdytojo ir tvarkytojų pareigos; Asmens duomenų tvarkymo tikslai; Asmens duomenų gavimo šaltiniai; Asmens duomenų gavėjai; Asmens duomenų saugojimo terminai; Konfidencialumo ir saugumo nuostatos organizacijos darbuotojams; Asmens duomenų tvarkymas; Duomenų subjektų teisės; Asmens duomenų saugumo pažeidimų valdymas; Duomenų tvarkytojų ir kitų asmenų pasitelkimas; Poveikio duomenų apsaugai vertinimas; Duomenų perdavimas į trečiąsias valstybes arba tarptautinėms organizacijoms; Privatumo politika; ir t.t.

3. **III lygis**.
   Periodiškai peržiūrėti asmens duomenų tvarkymo politiką. Rekomenduojama kartą per pusmetį peržiūrėti, esant poreikiui, atnaujinti vidaus tvarkas reglamentuojančias asmens duomenų apsaugą. Gali būti sudarytas asmens duomenų politikos peržiūros grafikas, pvz. 4 kartus per metus kas 3 mėnesius. Šiame grafike būtų žymima asmens politikos peržiūros data ir esant poreikiui korekcijų data bei atsakingas asmuo. Asmens duomenų tvarkymo politika turi atspindėti realią padėtį asmens duomenų tvarkymo kontekste t. y. asmens duomenų politika privalo būti atnaujinta, jeigu pakito asmens duomenų apsaugos priemonės arba asmens duomenų tvarkymo procesai, buvo nustatyta neatitiktis BDAR reikalavimams arba atsirado rizikos dėl kurių galėtų kilti asmens duomenų saugumo pažeidimas ir t.t.

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos 2 priemonės detalizavimas (žr. 32 lentelę).

32 lentelė. Asmens duomenų apsaugos dimensijos 2 priemonė

2 priemonė		
I lygis **(ką privalu atlikti organizacijoje?)**	**II lygis** **(kaip įgyvendinti?)**	**III lygis** **(kaip patobulinti arba užtikrinti įgyvendinimą?)**
Identifikuoti asmens duomenų tvarkymo procesus ir užtikrinti pagrindinius asmens duomenų tvarkymo principus.	- Atlikti poveikio duomenų apsaugai vertinimą (PDAV); - Parengti duomenų tvarkymo veiklos įrašus.	- Periodiškai atlikti PDAV; - Rengti ir (ar) atnaujinti duomenų tvarkymo veiklos įrašus.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 2 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Identifikuoti asmens duomenų tvarkymo procesus ir užtikrinti pagrindinius asmens duomenų tvarkymo principus. Organizacija privalo identifikuoti duomenis, kuriuos tvarko vykdydama veiklą ir įgyvendinti BDAR pagrindinius asmens duomenų tvarkymo principus – teisėtumo, sąžiningumo ir skaidrumo; tikslo apribojimo; duomenų kiekio mažinimo; tikslumo; saugojimo trukmės apribojimo; vientisumo ir konfidencialumo; atskaitomybės. Detalūs šių principų aprašymai pateikti šios disertacijos 1 lentelėje „*Pagrindiniai asmens duomenų tvarkymo principai*“. Duomenų valdytojas ir duomenų tvarkytojas privalo užtikrinti, kad visų septynių pagrindinių asmens duomenų tvarkymo principų būtų laikomasi (Štarchoň, Pikulík, 2019). Organizacija visas su asmens duomenimis susijusias tvarkymo operacijas privalo dokumentuoti ir

stebėti (Blanco-Lainé ir kt., 2019). Ši informacija dokumentuojama dokumentų tvarkymo veiklos įrašuose. Kai dėl duomenų tvarkymo rūšies, ypač naudojant inovatyvias technologijas, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, organizacijos privalo atlikti poveikio duomenų apsaugai vertinimą (toliau – PDAV). Ankstyvas problemos nustatymas paprastai reiškia paprastesnį ir pigesnį sprendimą, taip pat galimos žalos reputacijai išvengimą vėliau.

2. **II lygis**.

- *Atlikti poveikio duomenų apsaugai vertinimą.* PDAV – tai procesas, skirtas duomenų tvarkymui aprašyti ir tokio tvarkymo reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo, jį įvertinant ir nustatant šio pavojaus pašalinimo priemones. PDAV yra svarbi atskaitomybės priemonė, nes padeda duomenų valdytojams ne tik laikytis BDAR, bet ir įrodyti, kad, siekiant užtikrinti atitiktį BDAR, buvo imtasi tinkamų priemonių (ES 29 straipsnio darbo grupė, 2017; Grütter ir Schneider, 2019). PDAV yra struktūrizuota duomenų tvarkymo rizikos analizė, sudaryta prieš pradedant darbą, kuri nustato ir įvertina galimus padarinius pagrindinėms teisėms (Bock ir kt., 2021). PDAV padeda nustatyti konkretaus projekto pažangą ir apsispręsti dėl duomenų apsaugos priemonių, taip pat planuoti ir pasiūlyti esminius žingsnius, užtikrinančius įstatymų laikymąsi (Chassang, 2017). Tinkamai atlikus PDAV bus sumažinta privatumo, saugumo ir reputacijos rizika, bus laikomasi duomenų apsaugos teisės aktų ir padidės duomenų subjektų ir suinteresuotųjų šalių pasitikėjimas (Georgiou ir Lambrinoudakis, 2021). PDAV metu pateikiamas duomenų tvarkymo operacijų ir jų tikslo aprašymas, vidinis duomenų tvarkymo būtinumo ir proporcingumo įvertinimas, atsižvelgiant į tikslą, rizikos asmenims vertinimas ir susijusios rizikos mažinimo priemonės (Crockett, 2018). VDAI patvirtino tiek įmonių ir valstybės institucijų, tiek su asmens duomenų apsauga dirbančios teisinės bendruomenės nekantriai lauktą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašą.
- *Parengti duomenų tvarkymo veiklos įrašus*. Apdorojimo veiklos įrašai arba vadinamieji procedūrų žurnalai dažnai yra svarbus duomenų srautų ir rizikos supratimo pagrindas. VDAI parengė gaires, kuriose nurodo, kad veiklos įrašai yra privalomi – valdžios institucijoms ir įstaigoms; įmonėms, įstaigoms ar organizacijos, kuriose dirba daugiau kaip 250 darbuotojų; įmonėms, įstaigoms ar organizacijoms, dėl kurių vykdomo duomenų tvarkymo gali kilti pavojus duomenų subjektų teisėms ir laisvėms; įmonėms, įstaigoms ar organizacijoms, kurių duomenų tvarkymas yra reguliarus; įmonėms, įstaigoms ar organizacijoms, kurių duomenų tvarkymas apima specialių kategorijų asmens duomenis; įmonėms, įstaigoms ar organizacijoms, kurios tvarko asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas. BDAR sudaro įspūdį, kad duomenų tvarkymo veiklos įrašai yra kuriami dokumentiniais sumetimais, kad juos būtų galima pateikti priežiūros institucijoms (Samardžić,2021).

Privalomas duomenų tvarkymo veiklos įrašo turinys nustatytas BDAR 30 straipsnio 1 dalyje. Procesai kinta ir vystosi bėgant laikui – pvz., gali pasikeisti paskirtis, arba tas pats procesas naudojamas kitiems papildomiems tikslams, arba keičiasi priskirtas procesorius. Kad būtų laikomasi BDAR, kiekvienas toks pakeitimas turi būti dokumentuojamas kaip laikinas apdorojimo įrašas, kad būtų parodytas apdorojimo veiklos laikymasis tuo laikotarpiu (Pandit ir kt., 2019).

3. **III lygis**.
   - *Periodiškai atlikti PDAV.* Pakitę duomenų tvarkymo procesai, gali turėti įtakos asmens duomenų saugumui, todėl turi būti atliktas pakartotinis PDAV.
   - *Rengti ir (ar) atnaujinti duomenų tvarkymo veiklos įrašus*. Kai pasikeičia asmens duomenų tvarkymo veiksmai ar kita informacija, susijusi su asmens duomenų tvarkymu, duomenų tvarkymo veiklos įrašuose esanti informacija turi būti atnaujinama. Duomenų tvarkymo įrašai taip pat yra svarbi priemonė rengiant duomenų apsaugos informaciją/pranešimus (pvz., darbuotojams ar pareiškėjams) ir įgyvendinant duomenų subjektų prašymus susipažinti su duomenimis (Helbing, 2022; Hilberg, 2022).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos 3 priemonės detalizavimas (žr. 33 lentelę).

33 lentelė. Asmens duomenų apsaugos dimensijos 3 priemonė

3 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Įvertinti ir nustatyti žmogiškųjų resursų poreikį, siekiant užtikrinti asmens duomenų apsaugą.	Paskirti duomenų apsaugos pareigūną arba kitą specialistą atsakingą už duomenų apsaugą.	Periodiškai atlikti darbuotojų veiklos vertinimą.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 3 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Įvertinti ir nustatyti žmogiškųjų resursų poreikį, siekiant užtikrinti asmens duomenų apsaugą. Organizacija norėdama užtikrinti asmens duomenų apsaugą turi turėti atitinkamus darbuotojus su priskirtomis funkcijomis, kurie įgyvendintų BDAR reikalavimus ir užtikrintų jų kontrolę. VDAI 2019 metų ataskaitoje teigiama, kad susiduriama su asmens duomenų apsaugos specialistų trūkumu rinkoje, kai, pradėjus taikyti Reglamentą, nemažai organizacijų turi paskirti ne tik Pareigūną, tačiau samdo ir kitus asmens duomenų apsaugos profesionalus,

siekdami organizacijose užtikrinti atitiktį Reglamento reikalavimams. Pareigūnu gali būti organizacijos darbuotojas arba asmuo iš išorės.

2. **II lygis**.
   Paskirti duomenų apsaugos pareigūną arba kitą specialistą atsakingą už duomenų apsaugą. Detalizuotos Duomenų apsaugos pareigūno skyrimo organizacijoje sąlygos yra pateiktos disertacijos 1.1.3. skyriuje „*Duomenų apsaugos pareigūno organizacijoje ir duomenų apsaugos priežiūros institucijos vaidmenų analizė*". Jeigu organizacijai pagal BDAR nėra privaloma paskirti Duomenų apsaugos pareigūną, ji gali paskirti asmenį, kuriam būtų pavestos su asmens duomenų apsauga susijusios užduotys. Bamberger ir Mulligan (2015) Pareigūno vaidmenį apibūdina kaip svarbiausią reguliavimo pasirinkimą institucionalizuojant duomenų apsaugą. Praktikoje Pareigūnas yra išankstinis įspėjimo apie nepageidaujamus įvykius indikatorius organizacijoje tvarkant asmens duomenis (Drewer, 2018). Pareigūnas yra atsakingas už visos bendrovės (įmonės ar įstaigos) duomenų tvarkymo procesų priežiūrą. Jis turi stebėti, kaip laikomasi BDAR ir kitų asmens duomenų apsaugos aktų nuostatų reikalavimų bendrovės veikloje, teikti rekomendacijas dėl procesų keitimo, susijusių su duomenų tvarkymu ar informuoti apie bet kokias neatitiktis duomenų apsaugos reikalavimams. Be kita ko, duomenų apsaugos pareigūnas teikia įvairias konsultacijas duomenų apsaugos klausimais (tiek bendrovei, tiek darbuotojams), vykdo darbuotojų mokymus, veda duomenų tvarkymo veiklos įrašus, komunikuoja su priežiūros institucijomis bei padeda laikytis reikalavimų įgyvendinant įvairias atskaitomybės priemones, asistuoja atliekant poveikio duomenų apsaugai vertinimus (Jurkonis, 2021).
3. **III lygis**.
   Periodiškai atlikti darbuotojų veiklos vertinimą. Viešojo administravimo sistema gali būti valdoma dviem pagrindiniais būdais: 1) remiantis taisyklėmis, kai darbuotojų gera veikla iš esmės sutapatinama su nepriekaištingu taisyklių laikymusi; 2) remiantis veiklos rezultatų vertinimu, kuomet darbuotojų gera veikla iš esmės sutapatinama su pasiektais, dažniausiai kiekybiškai įvertinamais rezultatais. Stebėti trumpalaikių ir ilgalaikių tikslų įgyvendinimą (Vanagas ir Tumėnas, 2008). Veiklos vertinimas apibrėžiamas kaip formalus, sistemingai vykdomas procesas, kurio metu yra nustatomos, stebimos, matuojamos, fiksuojamos bei ugdomos su darbu susijusios asmens stipriosios bei silpnosios pusės ir skiriamas įvairaus pobūdžio atlygis (Fletcher, 2001).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos 4 priemonės detalizavimas (žr. 34 lentelę).

34 lentelė. Asmens duomenų apsaugos dimensijos 4 priemonė

4 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Užtikrinti atitiktį teisės aktams ir standartams, reglamentuojantiems asmens duomenų apsaugą.	Atlikti asmens duomenų apsaugos atitikties vertinimą.	Periodiškai atlikti asmens duomenų apsaugos atitikties vertinimą.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 4 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Užtikrinti atitiktį teisės aktams ir standartams, reglamentuojantiems asmens duomenų apsaugą. Organizacija norėdama įgyvendinti asmens duomenų apsaugą turi užtikrinti BDAR reikalavimus ir užtikrintų jų kontrolę. Atitiktis BDAR šiuo metu yra pagrindinė problema organizacijoms visame pasaulyje. Problema priklauso nuo teisinių reikalavimų supratimo, kuris paprastai užima daug laiko ir yra sudėtingas (Ayala-Rivera ir Pasquale, 2018). Tinkamas jų aiškinimas yra sudėtingas procesas, kuriame dažnai pasitaiko klaidų (Otto ir Anton, 2007). Pagal BDAR atskaitomybės principą reikalaujama, kad duomenų valdytojas galėtų įrodyti, kad laikosi Reglamento (BDAR 74 konstatuojamoji dalis). Tam reikia, kad organizacija veiktų atsakingai, vykdytų tinkamus veiksmus, paaiškintų ir pateisintų veiksmus, suteiktų patikinimą ir pasitikėjimą vidinėmis ir išorinėmis suinteresuotosiomis šalimis, kad organizacija elgiasi teisingai, ir ištaisyti netinkamus veiksmus (Felici, 2013). Tai gana sudėtinga užduotis duomenų valdytojui, nes trūksta supratimo apie savo įsipareigojimus ir pareigas, susijusias su asmens duomenų apsauga, skubiai reikia apibrėžti metodiką, kad būtų galima laikytis BDAR (Freitas ir Silva, 2018). Todėl organizacijoms reikia įrankių ir metodų, galinčių padėti joms pasiekti visišką BDAR atitiktį. Tai reiškia, pavyzdžiui, paramą, skirtą: 1) analizuoti ir suprasti dabartinį organizacijos BDAR atitikties lygį; 2) parinkti, kuriuos BDAR aspektus turi atitikti organizacija t. y. ne visus BDAR aspektus turi tenkinti visos organizacijos; iš tikrųjų tai priklauso nuo konkrečios organizacijos esamos situacijos, verslo ir poreikių; 3) suprasti, kokių veiksmų reikia imtis, kad būtų laikomasi BDAR, parengti tam skirtą planą ir turėti paruoštų naudoti gairių, kaip atlikti šį sudėtingą procesą; 4) suteikti vartotojui funkcijas, skirtas naudotis savo teisėmis; 5) būti pasirengusiam pateikti institucijoms reikiamus dokumentus ir su jomis bendrauti (Mouratidis ir kt., 2016).
2. **II lygis**.
   Atlikti asmens duomenų apsaugos atitikties vertinimą. VDAI parengė gaires

„*Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*“. Šios gairės parengtos remiantis ENISA rekomendacijomis ir trimis ISO standartais – 27001, 27002 ir 27701. Gairės padeda įvertinti aktualius pavojus asmens duomenų saugumui ir įgyvendinti tinkamas saugumo priemones. Svarbu atkreipti dėmesį, kad ISO standartai paremti organizacijos rizikų valdymu, o asmens duomenų apsauga vertinama kaip organizacijos saugumo dalis, tuo tarpu Reglamente duomenų saugumas yra tik vienas iš asmens duomenų apsaugos komponentų, o rizika vertinama atsižvelgiant į poveikį žmogaus teisėms ir laisvėms. Vertinant atitiktį, teisės aktams, reglamentuojantiems asmens duomenų apsaugą organizacijoje turėtų būti atliktos šios veiklos: inventorizuoti tvarkomi asmens duomenis; peržiūrėtos asmens duomenų tvarkymui naudojamos procedūros ir procesai; įvertinta, kokia apimtimi taikomi BDAR reikalavimai; pateiktos rekomendacijas nustatytoms neatitiktims pašalinti. Pirmasis žingsnis siekiant atitikties yra tinkamų BDAR sąlygų atrinkimas ir pavertimas apčiuopiamais reikalavimais. Tam naudingi ištekliai yra duomenų apsaugos institucijų ir profesinių institutų teikiama informacija ir gairės. Informacija, susijusi su šių reikalavimų įvykdymu, reikalinga atitikties dokumentams. Kitas žingsnis – nustatyti informaciją, kurios reikia norint įvertinti, ar buvo įvykdyti reikalavimai, ir sukurti apribojimus, kurie patikrina tos informacijos buvimą ir jos teisingumą (Pandit ir kt., 2019; Blanco-Lainé ir kt., 2019).

3. **III lygis**.
   Periodiškai atlikti asmens duomenų apsaugos atitikties vertinimą. Nuolatinis verslo pokyčių tempas, susijęs su besikeičiančiomis teisinėmis interpretacijomis, reikalauja nuolatinio Pareigūno budrumo ir sukuria papildomų atskaitomybės iššūkių. Iš esmės organizacija, o ne Pareigūnas, turi sugebėti įrodyti, kad ji atitinka atskaitomybės principo ribą (Ryan, ir kt., 2020). Atsižvelgdama į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, organizacija turi įgyvendinti tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis BDAR. Pažymėtina, siekiant, kad būtų išvengta BDAR neatitikties grėsmės, fizinių asmenų apsauga turėtų būti neutrali technologijų atžvilgiu ir turėtų nepriklausyti nuo taikomų metodų.

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos 5 priemonės detalizavimas (žr. 35 lentelę).

35 lentelė. Asmens duomenų apsaugos dimensijos 5 priemonė

5 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Identifikuotos, įvertintos ir suvaldytos asmens duomenų saugumo rizikos.	Atlikti asmens duomenų saugumo rizikos vertinimą.	Periodiškai atlikti asmens duomenų saugumo rizikos vertinimą.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 5 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Identifikuoti, įvertinti ir suvaldyti asmens duomenų saugumo rizikos. Nesugebėjimas apsaugoti duomenų, gali kelti pavojų organizacijai, kuo tikslesnis rizikos įvertinimas, tuo geriau valdomi duomenys (Haes ir kt., 2013). BDAR preambulės 75 ir 76 punktuose rašoma, kad įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms gali kilti dėl tokio asmens duomenų tvarkymo, kurio metu galėtų būti padarytas kūno sužalojimas, materialinė ar nematerialinė žala, visų pirma kai dėl tvarkymo gali kilti diskriminacija, būti pavogta ar suklastota tapatybė, būti padaryta finansinių nuostolių, pakenkta reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas, neleistinai panaikinti pseudonimai arba padaryta kita didelė ekonominė ar socialinė žala; kai duomenų subjektai gali netekti galimybės naudotis savo teisėmis ir laisvėmis ar jiems užkertamas kelias kontroliuoti savo asmens duomenis; kai tvarkomi asmens duomenys, kurie atskleidžia rasinę arba etninę kilmę, politines pažiūras, religiją ar filosofinius įsitikinimus, priklausymą profesinėms sąjungoms, taip pat tvarkant genetinius duomenis, sveikatos duomenis ar duomenis apie lytinį gyvenimą, arba apkaltinamuosius nuosprendžius ir nusikalstamas veikas, arba susijusias saugumo priemones; kai siekiant sukurti arba naudoti asmens profilį vertinami asmeniniai aspektai, visų pirma nagrinėjami arba numatomi su asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu susiję aspektai; kai tvarkomi pažeidžiamų fizinių asmenų, visų pirma vaikų, asmens duomenys; arba kai duomenų tvarkymas apima didelį kiekį asmens duomenų ir daro poveikį daugeliui duomenų subjektų. Pavojaus duomenų subjekto teisėms ir laisvėms tikimybė ir rimtumas turėtų būti nustatomi atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus. Pavojus turėtų būti vertinamas remiantis objektyviu įvertinimu, kurio metu nustatoma, ar duomenų tvarkymo operacijos yra susijusios su pavojumi arba dideliu pavojumi.

2. **II lygis**.
   Atlikti asmens duomenų saugumo rizikos vertinimą. Ghazouani ir kt. (2014), teigia kad rizikos valdymo metodai leidžia organizacijai maksimaliai padidinti savo galimybes kontroliuoti galimų grėsmių poveikį pagrįsta. Rizika formuoja teisinius įsipareigojimus ta prasme, kad ji tapo vienu iš kriterijų, į kurį duomenų valdytojas turėtų atsižvelgti priimdamas sprendimą dėl tinkamiausių techninių ir organizacinių priemonių. Rizika sukelia teisinę prievolę ta prasme, kad jei rizikos nėra, įsipareigojimo vykdyti nereikia (Demetzou, 2018). ES 29 straipsnio duomenų apsaugos darbo grupė nurodo, kad rizika yra scenarijus, apibūdinantis įvykį ir jo pasekmes, kuris įvertinamas pagal sunkumą ir tikimybę. Organizacija, įvertinusi rizikos lygį, gali pasirinkti tinkamas saugumo priemones asmens duomenų saugumui užtikrinti.
3. **III lygis**.
   Periodiškai atlikti asmens duomenų saugumo rizikos vertinimą. Rizikos vertinimas padeda apsispręsti renkantis alternatyvas, kokias riziką mažinančias priemones įgyvendinti. Pasirinkimas dažnai priklauso nuo kaštų ir naudos analizės (Aven, 2016). Įsigaliojus Reglamentui organizacijų vadovams vis dažniau kyla atsakomybė už netinkamą kibernetinio saugumo rizikų valdymą (Rahul ir kt., 2020).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos 6 priemonės detalizavimas (žr. 36 lentelę).

36 lentelė. Asmens duomenų apsaugos dimensijos 6 priemonė

6 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Užtikrinti asmens duomenų apsaugos švietimą ir kultūrą.	Rengti arba organizuoti asmens duomenų apsaugos pratybas, mokymus ir konsultacijas.	Parengti asmens duomenų apsaugos pratybų ir mokymų planą.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 6 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Užtikrinti asmens duomenų apsaugos švietimą ir kultūrą. BDAR įgyvendinimo pradžia yra žinių apie reglamentą įgijimas, todėl labai svarbu, kad visi, susiję su duomenų tvarkymu, suprastų asmens duomenų apsaugos svarbą. Kiekvienai organizacijai reikia tam tikro tipo BDAR informuotumo didinimo ir mokymų, siekiant užtikrinti, kad visi laikytųsi viduje nustatytų taisyklių ir nekeltų

pavojaus duomenų *saugumui*. Organizacija, kuri atitinka BDAR reikalavimus, periodiškai rengia arba organizuoja asmens duomenų apsaugos pratybas ir mokymus. ENISA ataskaitoje „*Grėsmių peizažas 2022*“ rašoma, kad kibernetinės atakos sudėtingėja ir tampa vis labiau rafinuotos. Vis daugiau kibernetinių incidentų paremti manipuliavimu žmonėmis, jų silpnybėmis, siekiama apeiti informacijos apsaugos sistemas bei pavogti ir užvaldyti konfidencialią informaciją. Pastebimas socialinės inžinerijos metodais paremtų kibernetinių incidentų skaičiaus didėjimas (Šidlauskas ir Ungurytė-Ragauskienė, 2020). Socialinė inžinerija siejama su žmonių klaidinimu ir manipuliavimu, o ne technologijomis ar kitais mechanizmais (Shimonski, 2016). Anot D. Gibson (2014), jei darbuotojai ir vartotojai nesupranta saugumo praktikos vertės, jie mažiau linkę imtis konkrečių veiksmų. Organizacijų mokymai yra ne tik svarbi bet kurios organizacijos dalis, bet ir labai naudinga, nors mokymų kaina kartais gali atrodyti brangi, bendra investicijų grąža iš darbuotojų mokymų ir tobulėjimo yra reikšminga. Vienas iš pagrindinių sėkmės faktorių efektyviam organizacijos politikos ir procedūrų taikymui yra darbuotojų bendravimas, informavimas ir mokymas (Dounis, 2017).

2. **II lygis**.
   Rengti arba organizuoti asmens duomenų apsaugos pratybas, mokymus ir konsultacijas. Mokymas apibrėžiamas kaip suplanuotos, sistemingos pastangos keisti arba plėtoti žinias, įgūdžius ar požiūrį per mokymosi patirtį, siekiant efektyvaus veiklos ar veiklos rezultatų. Šios veiklos tikslas profesinėse situacijose yra sudaryti sąlygas apmokytam asmeniui įgyti gebėjimų tinkamai atlikti tam tikrą užduotį ar darbą (Buckley ir Caple, 2009). Mokymo medžiaga – tai pagalbiniai tekstai, pristatymai, vadovėliai ir kita fizinė bei skaitmeninė medžiaga, kuri naudojama tose sistemingose pastangose (Barnard-Wills ir kt., 2019), todėl visi darbuotojai turi būti informuoti apie duomenų apsaugos mokymus tiek akis į akį, tiek per nuotolinius internetinius kursus, kad išlaikytų tinkamą reikalavimų laikymosi lygį (Perry, 2019). Duomenų apsaugos mokymų tikslas – pateikti duomenų apsaugos apžvalgą per gana trumpą laiką, paprastai per vieną ar dvi dienas. Privačios institucijos prisideda siūlydamos seminarus vietoje arba internetu (Huth ir Matthes, 2020). Remiantis kompetencijų valdymo ir žmonių ugdymo gairių standartu ISO 10015, mokymas pasirenkamas kaip sprendimas kompetencijų spragai užpildyti, mokymo reikalavimai turėtų būti nurodyti ir dokumentuoti. Procesai ir privatumo apsaugos priemonės taip pat turi būti skaidrūs, kad darbuotojas turėtų pakankamai žinių apie apsaugos priemones visoje organizacijoje (Werner ir kt., 2020).
3. **III lygis**.
   Parengti asmens duomenų apsaugos pratybų ir mokymų planą. Nors BDAR nenustatytas terminas, kuriuo remiantis turėtų būti rengiami duomenų apsaugos mokymai, patartina rengti metinius duomenų apsaugos mokymus. Gali prireikti dažnesnių duomenų apsaugos mokymų, susijusių su didelės rizikos tvarkymu arba kai dažnai iškyla reikalavimų nesilaikymo problemos. Be to,

jei pažeidžiamas duomenų saugumas arba nesilaikoma BDAR, rekomenduojama kuo greičiau su pažeidimu ar incidentu susijusiems asmenims surengti papildomus duomenų apsaugos mokymus (Carey, 2019). Mokymai turi būti ne vienkartinė veikla, o pasikartojantis ir reguliarus procesas, atspindintis identifikuotas rizikas ir grėsmes įmonėje. Didesnė erudicija gali padėti darbuotojams suvokti rizikas darbo procese ir gebėjimą atkreipti į jas dėmesį bei tuo pačiu geriau ginti savo teises asmeniniame gyvenime (Zanker ir kt., 2021). Siekiant sumažinti ir užkirsti kelią darbuotojų keliamai rizikai, organizacijoje būtina periodiškai organizuoti mokymus, kurių metu darbuotojams primenama, kokių taisyklių reikia laikytis įmonėje, kokios yra jų teisės ir pareigos, o taip pat saugumo reikalavimai, praeityje įvykę incidentai ir jų priežastys (Tiliute, 2019).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos 7 priemonės detalizavimas (žr. 37 lentelę).

37 lentelė. Asmens duomenų apsaugos dimensijos 7 priemonė

7 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Identifikuoti ir suvaldyti asmens duomenų saugumo pažeidimus.	Parengti asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą.	- Periodiškai peržiūrėti asmens duomenų pažeidimų valdymo tvarkos aprašą; - Organizuoti asmens duomenų saugumo pažeidimų suvaldymo aptarimus.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 7 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Identifikuoti ir suvaldyti asmens duomenų saugumo pažeidimus. BDAR 4 straipsnio 12 dalyje asmens duomenų saugumo pažeidimas apibrėžtas taip: „*saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga*“. Anot Stravinskaitės (2022) asmens duomenų saugumo pažeidimo apibrėžimo atskiros dalys gali būti suprantamos taip:
   - Sunaikinimas – kai duomenų nebelieka arba jų nebelieka tokia forma, kad duomenų valdytojas juos galėtų naudoti.
   - Sugadinimas – asmens duomenys pakeičiami, iškraipomi arba dalis duomenų dingsta.

- Praradimas – kai duomenys galbūt tebėra, tačiau duomenų valdytojas jų nebevaldo, netenka prieigos prie jų arba nebegali jais disponuoti.
- Duomenų tvarkymas be leidimo arba neteisėtas duomenų tvarkymas - kai asmens duomenys atskleidžiami (arba prieigos prie duomenų suteikimas) duomenų gavėjams, kurie neturi leidimo gauti (arba prieiti prie) duomenų arba duomenų tvarkymą bet kokia kita forma, kuria pažeidžiamas BDAR.

Atsižvelgiant į aplinkybes, pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu prie asmens duomenų, taip pat su bet kokiu šių savybių deriniu. Gautus pranešimus apie asmens duomenų saugumo pažeidimus VDAI įvertina ir, jei reikia, atlieka tyrimą. Visi darbuotojai turi suprasti pagrindinį BDAR lygį ir su tuo susijusią riziką organizacijai dėl bet kokių duomenų pažeidimų, padarytų per klaidą ar kitaip (Reeves, 2020). Tiesą sakant, dauguma duomenų pažeidimų yra vidiniai, o ne dėl išorinių įsilaužimų (Addis ir Kutar, 2018). Negalima nuvertinti organizacijoms keliamos finansinės ir reputacijos rizikos: nežinojimas nėra gynyba (Mackie ir kt., 2017).

2. **II lygis**.
   Parengti asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą. Parengti ir pasitvirtinti asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą, reglamentuojantį asmens duomenų saugumo pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie juos tvarką. Įvykus asmens duomenų saugumo pažeidimui, organizacijos turi imtis visų įmanomų veiksmų pažeidimui sustabdyti. Mažesnių ar didesnių pažeidimų vyksta nuolatos. Visais atvejais organizacijos turi tokius pažeidimus dokumentuoti ir laikytis kitų BDAR nustatytų procedūrų. Nustačius, kad dėl įvykusio pažeidimo kyla rizika fizinių asmenų teisėms ir laisvėms, privaloma apie tai pranešti VDAI be reikalo neatidėliojant, bet ne vėliau kaip per 72 valandas, ir asmenims, kurių duomenys galėjo nukentėti (VDAI, 2022).
3. **III lygis**.
   - Periodiškai peržiūrėti asmens duomenų pažeidimų valdymo tvarkos aprašą. Vidaus tvarkos organizacijoje turėtų būti reguliariai peržiūrimos ir esant poreikiui atnaujinamos, kadangi vyksta nuolatiniai pokyčiai. Pokyčiai gali būti vidiniai t. y. vykstantys organizacijos viduje, pvz. kinta procedūros, asmens duomenų apsaugos priemonės ir t. t. Taip pat pokyčiai gali būti išoriniai, pvz. kinta teisės aktai reglamentuojantys asmens duomenų apsaugą, atitinkamų institucijų pateikiamos asmens duomenų apsaugos gairės ir t.t. Organizacija nepriklausomai nuo pokyčių visada turi užtikrinti asmens duomenų apsaugą įgyvendinant BDAR atitiktį.
   - Organizuoti asmens duomenų pažeidimų suvaldymo aptarimus. Atsakingi asmenys turėtų analizuoti asmens duomenų pažeidimus ir statistiką bei inicijuoti asmens duomenų pažeidimų suvaldymo aptarimus. Asmens duomenų pažeidimų suvaldymo aptarimai gali būti rengiami periodiškai, aptariant išmoktas pamokas, siekiant sumažinti asmens duomenų pažeidimų įvykio tikimybę.

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos 8 priemonės detalizavimas (žr. 38 lentelę).

38 lentelė. Asmens duomenų apsaugos dimensijos 8 priemonė

8 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Užtikrinti duomenų subjektų teisių įgyvendinimą.	- Parengti privatumo politiką; - Sukurti procedūras ir mechanizmus duomenų subjektų teisių įgyvendinimui pagal BDAR reikalavimus.	- Periodiškai peržiūrėti privatumo politiką; - Automatizuoti duomenų subjekto teisių įgyvendinimo procesus.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 8 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Užtikrinti duomenų subjektų teisių įgyvendinimą. Detalūs duomenų subjekto teisių įgyvendinimo ypatumai pateikiami šio darbo poskyryje „*1.1.2. Duomenų subjektų teisių įgyvendinimas organizacijoje*".
2. **II lygis**.
   - *Parengti privatumo politiką.* Privatumo politika reglamentuoja organizacijos ar subjekto asmens duomenų tvarkymo praktiką, taip pat apie konkrečias duomenų subjektų teises (Siegel, 2016; Harkous el al., 2018). Privatumo politika yra viešas organizacijos dokumentas, kuriame paaiškinama, kaip organizacija tvarko asmens duomenis ir kaip taiko duomenų apsaugos principus. BDAR 12, 13 ir 14 straipsniuose pateikiamos išsamios instrukcijos, kaip sukurti privatumo politiką, pabrėžiant, kad ji būtų lengvai suprantama ir prieinama. Privatumo politikoje atskleidžiami visi būdai, kuriais organizacija renka, naudoja, atskleidžia ir tvarko duomenis (Flavián, Guinalíu, 2006). BDAR 12 straipsnyje nustatomas skaidrumo pagrindas – vienas iš šešių pagrindinių BDAR principų. Jame teigiama, kad bet kokia informacija ar komunikacija vartotojams turi būti glausta, skaidri, suprantama ir lengvai prieinama, naudojant aiškią ir paprastą kalbą. Organizacijos turi nedelsdamas informuoti vartotojus apie jų privatumo praktikos atnaujinimus (Linden ir kt., 2018). Anot Wolford (2022) jei organizacija informaciją renka tiesiogiai iš asmens, ji savo privatumo politikoje turi nurodyti šią informaciją:

- Organizacijos, jos atstovo ir duomenų apsaugos pareigūno tapatybę bei kontaktiniai duomenis.
- Organizacijos tikslą tvarkyti asmens duomenis ir jo teisinis pagrindą.
- Organizacijos (arba trečiosios šalies, jei taikoma) teisėtus interesus.
- Asmens duomenų gavėjus arba gavėjų kategorijas.
- Išsamią informaciją apie bet kokį asmens duomenų perdavimą trečiajai šaliai ir apsaugos priemones, kurių buvo imtasi.
- Asmens duomenų saugojimo laikotarpį arba kriterijus, naudojamus asmens duomenų saugojimo laikotarpiui nustatyti.
- Duomenų subjekto teises.
- Teisę pateikti skundą priežiūros institucijai.
- Teisę atšaukti sutikimą.
- Prievolę pateikti asmens duomenis, pvz. remiantis įstatymu ar sutartimi, ir galimas pasekmes, jei asmens duomenys nepateikti.
- Automatizuoto sprendimų priėmimo, įskaitant profiliavimą, svarbą ir pasekmes (jeigu tai naudojama).

Organizacijos privatumo politikoje yra visa informacija, kurios vartotojams reikia, kad žinotų apie organizacijos duomenų tvarkymo praktiką ir priimtų pagrįstus sprendimus, kurioms organizacijoms patikėti savo asmens duomenis (Gluck, 2016).

- Sukurti procedūras ir mechanizmus duomenų subjektų teisių įgyvendinimui pagal BDAR reikalavimus. Svarbu užtikrinti Reglamento reikalavimus, kuriant procedūras ir mechanizmus, kurių specifika priklauso nuo organizacijos vykdomos veiklos specifikos.

3. **III lygis**.

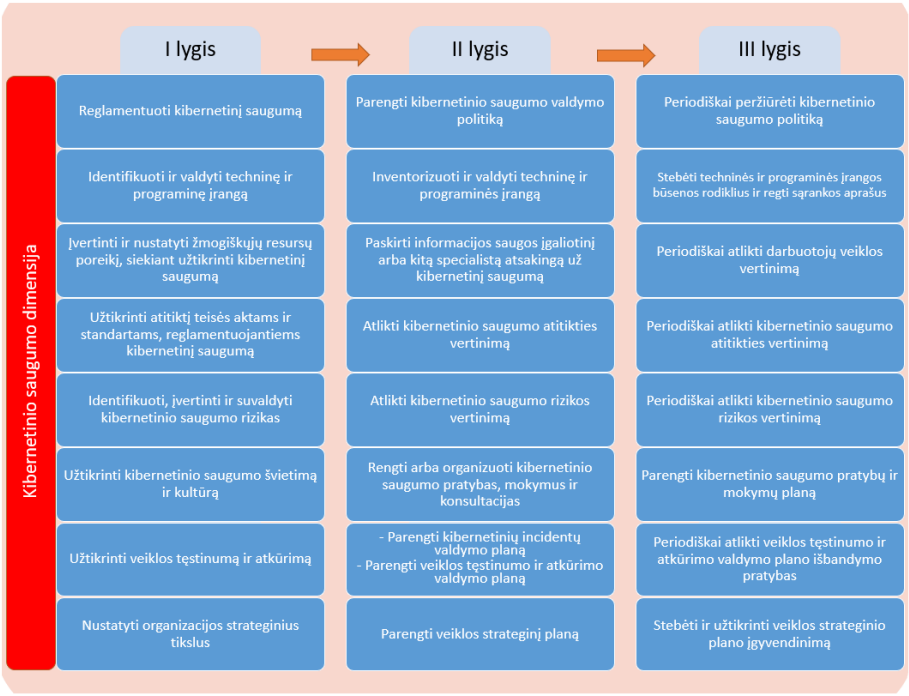
- Periodiškai peržiūrėti asmens duomenų tvarkymo politiką. Asmens duomenų tvarkymo politiką, turi atspindėti realią duomenų tvarkymo situaciją organizacijoje, todėl nuolatos turi būti peržiūrima ir, esant poreikiui, atnaujinama.

- Automatizuoti duomenų subjekto teisių įgyvendinimo procesus. Organizacijos ne tik gali keisti asmens duomenų tvarkymo būdą, bet ir skaidriai atskleisti, kaip jos tvarko asmens duomenis, jų duomenų tvarkymo teisinius pagrindus ir turi pasiūlyti savo vartotojams individualaus sutikimo, prieigos prie duomenų, duomenų ištrynimo ir duomenų perkeliamumo mechanizmus (Degeling ir kt., 2018). Organizacijos, kurios investuoja į programinę ir techninę įrangą, turi galimybes automatizuoti duomenų subjektų teisių įgyvendinimą panaudojant atitinkamus mechanizmus, pvz. vartotojų autentifikavimo, vartotojų profiliavimo ir t.t. Organizacijos savo interneto svetainėse naudoja slapukus. Slapukas yra nedidelis failas, atsiųstas į įrenginį, naudotojui besilankant atitinkamoje interneto svetainėje. Per pastaruosius kelis dešimtmečius kuklus slapukas tapo neatsiejama naršymo žiniatinklyje dalimi, todėl vartotojams jis tapo greitesnis ir patogesnis, o dizaineriams padeda tobulinti savo svetaines (Gunawardena, 2018). Interneto naršyklės slapukai, naudojami autentifikavimui ir seanso valdymui, taip pat naudotojų stebėjimui ir reklamos taikymui (Dabrowski ir kt.,

2019). Slapukai gali būti naudojami įvairiems tikslams, pradedant nuo būtinų slapukų, be kurių paslauga tinkamai neveikia, tokiems slapukams rinkti sutikimas nereikalingas, iki sekimo ir rinkodaros slapukų, kurie stebi klientų elgesį (Basin, 2020). Koch (2020) teigia, kad apskritai yra trys skirtingi slapukų klasifikavimo būdai - kokiam tikslui jie naudojami, kiek laiko jie galioja ir kokia jų kilmė. *Šiandien interneto lankytojai beveik kiekvieną kartą prisijungę prie interneto sutinka slapukus.* BDAR numato, kad duomenų valdytojai turi turėti teisinį pagrindą rinkti ir tvarkyti asmens duomenis. Vienas teisinis pagrindas yra sutikimas: duomenų subjektai (vartotojai) sutinka, kad duomenys būtų tvarkomi konkrečiais tikslais. Nors šie reikalavimai nėra nauji, BDAR grėsmė sankcijomis ir veiksmingesnis vykdymas paskatino daugelį svetainių operatorių permąstyti savo slapukų praktiką arba bent jau užtikrinti atitiktį gavus sutikimą prieš naudojant slapukus kitais teisiniais pagrindais nenumatytiems tikslams (Eijk ir kt., 2019). Teisėtam slapukų tvarkymui buvo sukurtos ir pristatytos naujos sutikimo valdymo platformos, kurios suteikė galimybę naudotojams sužinoti aktualią informaciją apie slapukus ir aktyviais veiksmais valdyti slapukų tvarkymą (Nouwens ir kt., 2020). Naudotojas turi aiškiai suprasti, kad jis duoda sutikimą dėl slapukų naudojimo, be to, jam turi būti sudaryta galimybė šį sutikimą bet kada atšaukti.

4.2. Kibernetinio saugumo dimensijos analizė

Kibernetinio saugumo dimensija asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kontekste yra svarbi asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio dalis. Būtent ši dimensija užtikrina kibernetinį saugumą ir atitinkamas technines ir organizacines priemones, siekiant apsaugoti asmens duomenis elektroninėje erdvėje. Kibernetinio saugumo dimensija yra grafiškai pavaizduota žemiau esančiame paveiksle (žr. 18 pav.).



18 pav. Kibernetinio saugumo dimensija
Šaltinis: sudaryta autoriaus

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kibernetinio saugumo dimensijos 1 priemonės detalizavimas (žr. 39 lentelę).

39 lentelė. Kibernetinio saugumo dimensijos 1 priemonė

1 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Reglamentuoti kibernetinį saugumą.	Parengti kibernetinio saugumo valdymo politiką.	Periodiškai peržiūrėti kibernetinio saugumo valdymo politiką.

Šaltinis: sudaryta autoriaus

Kibernetinio saugumo dimensijos 1 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Reglamentuoti kibernetinį saugumą. Kibernetinio saugumo reikalavimai yra suformuluoti teisės aktuose, kuriuose nurodytos tam tikros techninės ir organizacinės priemonės, kurias organizacijos turi taikyti. Taip pat kibernetinio saugumo geroji praktika pateikiama įvairiuose tarptautiniuose standartuose – ISO, SANS, NIST ir t.t., kuriais organizacijos gali remtis siekiant reglamentuoti kibernetinio saugumo valdymą.
2. **II lygis**.
   Parengti kibernetinio saugumo valdymo politiką. Terminas „*kibernetinio saugumo politika*“ reiškia nuostatas, skirtas užtikrinti kibernetinį saugumą (Bayuk ir kt., 2012). Organizacijose įprasta, kad bus laikomasi kibernetinio saugumo politikos, o už jos nesilaikymą gresia sankcijos. Privataus sektoriaus organizacijos nėra taip suvaržytos kaip organizacijos valdančios ir tvarkančios valstybės informacines sistemas, kurios pagal patvirtintą LRV 2013 m. liepos 24 d. Nr. 716 nutarimą „*Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo*“ arba LRV 2018 m. rugpjūčio 13 d. Nr. 818 nutarimą „*Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo*“ privalo parengti, suderinti su NKSC ir patvirtinti šiuos kibernetinio saugumo dokumentus:
   – Duomenų saugos nuostatus.
   – Saugaus elektroninės informacijos tvarkymo taisykles.
   – Informacinės sistemos veiklos tęstinumo valdymo planą.
   – Informacinės sistemos naudotojų administravimo taisykles.

   Alqahtani (2017 m.) teigimu, prieš pradedant taikyti kibernetinę politiką, ją turi patvirtinti organizacijos vadovas. Kibernetinio saugumo politikos taikymas skiriasi priklausomai nuo jos taikymo spektro (Cheng ir kt., 2020). Organizacijų kibernetinis saugumas taikomas tik jos darbuotojams, todėl reguliuoti savo elgesį organizacijos atžvilgiu. Netgi negalima tikėtis, kad paslaugų tiekėjai laikysis užsakovo kibernetinio saugumo politikos, nebent būtų sudaryta oficiali sutartis įpareigojanti tai daryti (Alghamdi, 2021). Vertinant kibernetinio saugumo politiką iš vien prevencinės perspektyvos, reiškia kad organizacija turi minimalią toleranciją bet kokiam poveikiui, pvz., neteisėtai prieigai prie informacijos, jos pakeitimo, sunaikinimo ar atskleidimo, todėl turi būti taikomos atsakomosios priemonės, kad būtų užkirstas kelias bet kokiam organizacijos puolimui (Ghelani, 2022). Kibernetinio saugumo politiką gali sudaryti įvairios temos, įskaitant bet nepasiribojant, - taikymo sritis, vaidmenys ir atsakomybės, informacijos klasifikavimas, prieigos kontrolė ir slaptažodžių sudarymo reikalavimai, tinklo apsauga ir nuotolinis prisijungimas, mobiliųjų įrenginių valdymas, fizinė sauga, incidentų valdymas, veiklos tęstinumo užtikrinimas, programinės įrangos valdymas, naudotojų veiksmų stebėsena ir analizė, IS pokyčių valdymas, atsarginių kopijų darymo reikalavimai, rizikos vertinimas ir

t.t. Sąrašas nėra baigtinis, nes organizacijos kibernetinio saugomo politika priklauso nuo daug veiksnių, tokių kaip infrastruktūra, veiklos pobūdis, naudojamos techninės ir organizacinės priemonės, darbuotojų suvokimo ir kultūros ir t.t. Viena iš sričių, į kurią reikia atkreipti dėmesį, yra tinkamas vaidmenų ir atsakomybės paskirstymas tarp informacinės sistemos vartotojų (Kahyaoglu ir Caliyurt, 2018). Atskiri vaidmenys derinami su pareigomis, siekiant užkirsti kelią netinkamai naudotojų veiklai. Atitinkamai, kibernetinio saugumo politika turi būti skirta mobiliųjų įrenginių, tokių kaip nešiojamieji kompiuteriai, planšetiniai kompiuteriai, išmanieji telefonai ir įvairūs kompiuterių išoriniai įrenginiai, naudojimui (Kahyaoglu ir Caliyurt, 2018; Lu ir kt., 2015). Nuotolinio darbo negalima ignoruoti, nes kibernetiniai nusikaltėliai gali mėgdžioti teisėtus vartotojus ir sukompromituoti sistemą (Lu, Zhao, Zhao, Li ir Zhang, 2015). Anot Lubua ir Pretorius (2019) veiksniai, prisidedantys prie visapusės kibernetinio saugumo politikos trūkumo yra žinių apie politikos formavimo procedūras trūkumas, pagrindinių suinteresuotųjų šalių neįtraukimas, formalizuotų gairių trūkumas ir politikos peržiūros trūkumas.

3. **III lygis**.
   Periodiškai peržiūrėti kibernetinio saugumo valdymo politiką. Tobulėjant kibernetinei erdvei ir atitinkamoms kibernetinio saugumo priemonėms, vystosi kibernetinio saugumo politikos klausimų taksonomija (Bayuk ir kt., 2012). Kibernetinė politika reikalauja periodinės peržiūros, kad būtų atsižvelgta į naujas grėsmes. Nors kibernetinio sąmoningumo lygis įvairiose organizacijose auga, daugelis organizacijų vis dar investuoja į kibernetinės saugumo politikos tobulinimą. Pavyzdžiui, kibernetinio saugumo politika, kuri yra neišsami ir ignoruojama organizacijos aukščiausios vadovybės, gali kelti saugumo problemų (Lubua ir Pretorius, 2019). Kai kurios organizacijos peržiūri politiką, kai tik pastebi išorinius pokyčius. Pakeitimai gali atsirasti pasikeitus nacionaliniams arba tarptautiniams teisės aktams ir reguliavimo institucijoms pateikus atitinkamas rekomendacines gaires arba net keičiantis technologijoms (Heeks ir Stanforth, 2015). Kitos organizacijos nustato atitinkamą laikotarpį kada kibernetinio saugumo politika bus išsamiai peržiūrėta (Lubua ir Maharaj, 2012). Turi būti griežtai laikomasi kibernetinio saugumo politikos, kad organizacija galėtų atpažinti ir pasirengti įvairioms ateityje augančių kibernetinio saugumo grėsmių formoms (Aliyeva ir Hwang, 2019). Teigiamas požiūris į kibernetinio saugumo politiką yra susijęs su saugesniu elgesiu (Choong ir Theofanos, 2015). Li ir kt. (2019) atlikti tyrimo rezultatai rodo, kad kai darbuotojai žino savo organizacijos kibernetinio saugumo politiką ir joje nustatytas procedūras, jie yra kompetentingesni atlikti kibernetinį saugumą užtikrinančias užduotis nei tie, kurie nežino savo organizacijos kibernetinio saugumo politikos. Tinkamas planavimas ir nuolatinė kibernetinio saugumo peržiūra yra labai svarbu organizacijų tvarumui (Patterson, 2017).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kibernetinio saugumo dimensijos 2 priemonės

detalizavimas (žr. 40 lentelę).

40 lentelė. Kibernetinio saugumo dimensijos 2 priemonė

2 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Identifikuoti ir valdyti techninę ir programinę įrangą.	Inventorizuoti ir valdyti techninę ir programinės įrangą.	Stebėti techninės ir programinės įrangos būsenos rodiklius ir rengti sąrankos aprašus.

Šaltinis: sudaryta autoriaus

Asmens duomenų apsaugos dimensijos 2 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Identifikuoti ir valdyti techninę ir programinę įrangą. Šios priemonės tikslas - aktyviai valdyti (inventorizuoti, sekti ir koreguoti) visus įrenginius, kurie jungiasi prie tinklo ir visą programinę, kuri naudojama organizacijos tinkle. Tik autorizuotiems įrenginiams turi būti suteikta prieiga, o neautorizuoti privalo būti laiku aptikti bei užkardyta jų prieiga. Tik patvirtinta įranga turi būtų leistina diegti ir naudotis, o neautorizuota privalo būti laiku aptikta bei užkardytas jos naudojimas. Todėl yra būtina tiksli, išsami ir nuolatos atnaujinama techninės ir programinės įrangos, kuri naudojama organizacijos veiklai, inventorizacija, kuri būtų prieinama bei tinkama naudoti visiems suinteresuotiems organizacijos padaliniams. Standarte ISO 27002 rašoma, kad atsakomybė už turtą turėtų būti priskiriama tada, kai turtas sukuriamas arba kai turtas perduodamas organizacijai. Turto valdytojas turėtų būti atsakingas už tinkamą turto valdymą per visą turto gyvavimo ciklą. Turto valdytojas turėtų užtikrinti, kad turtas būtų inventorizuotas, tinkamai klasifikuotas ir apsaugotas bei nustatyti ir reguliariai peržiūrėti prieigos prie svarbaus turto apribojimus. Taip pat užtikrinti tinkamą tvarkymą, kai turtas pašalinamas ar sunaikinamas.
2. **II lygis**.
   Inventorizuoti ir valdyti techninę ir programinės įrangą. Inventorizacija - turto ir įsipareigojimų patikrinimas ir jų faktiškai rastų likučių palyginimas su buhalterinės apskaitos duomenimis. Ji atliekama norint užtikrinti turto saugumą ir sumažinti turto grobstymo galimybes, po stichinių nelaimių ar vagysčių, siekiant tiksliai nustatyti nuostolių dydį bei pačios pagrindinės priežasties - įvertinti faktinį turto buvimą. Inventorizacija gali būti dalinė, atrankinė, tam tikrų vertybių, tik pas įtariamus nesąžiningumu materialiai atsakingus asmenis ar kitais atvejais (Siaurusevičiūtė ir Vasiliauskienė, 2015). Žvelgiant per kibernetinio saugumo prizmę organizacijai yra svarbu inventorizuoti techninę ir programinę įrangą, siekiant nustatyti ne tik trūkstamą techninę įrangą bet taip pat

nesankcionuotą techninę ir programinę įrangą. SANS instituto parengtoje „*CIS Critical Security Controls Version 8*“ prioritetinių apsaugos priemonių rinkinyje rašoma, kad būtina sudaryti ir tvarkyti tikslią, išsamią ir atnaujintą viso įmonės turto, galinčio saugoti arba apdoroti duomenis, inventorių, tane tarpe ir galutinio vartotojo įrenginius (įskaitant nešiojamuosius ir mobiliuosius), tinklo įrenginius, ne kompiuterinius / daiktų interneto įrenginius ir tarnybines stotis. Į šį inventorių įeina turtas, prijungtas prie infrastruktūros fiziškai, virtualiai, nuotoliniu būdu ir debesies aplinkoje. Be to, jis apima turtą, kuris reguliariai prijungiamas prie įmonės tinklo infrastruktūros, net jei jo organizacija nekontroliuoja. Rekomenduojama peržiūrėti ir atnaujinti visą organizacijos turto inventorių bent du kartus per metus arba dažniau. Taip pat privalo būti sudarytas leistinos naudoti programinės įrangos sąrašas. Neleistina programinė įranga būtų pašalinta arba jai turi būtų taikoma dokumentuota išimtis.

3. **III lygis**.
   Stebėti techninės ir programinės įrangos būsenos rodiklius ir rengti sąrankos aprašus. Organizacijos turi pasirengti sąrankos valdymo tvarkos aprašą, kuriame būtų aprašyti procesai (pvz., sąrankos registravimas, atnaujinimas ir kontrolė) ir patvirtinti formos (pvz., sąrankos klasifikavimo forma, sąrankos vertinimo forma). Sąranka gali būti klasifikuojama:
   - Dokumentai (saugomi visų tipų elektroniniai dokumentai, kurie susiejami su įvairiais sąrankos vienetais (technine bei programine įranga, sutartimis ir kt.)), pvz. sutartys, paslaugų lygio susitarimai (angl. *SLA*), techninės ir programinės įrangos techninės specifikacijos ir t.t.
   - Techninė įranga, pvz. tarnybinė stotis (serveris - fizinis, virtualus), tinklo įrenginys, ugniasienė, atsarginio kopijavimo įrenginys, duomenų saugykla, spausdintuvas, nepertraukiamo maitinimo šaltinis, oro kondicionavimo sistema ir t.t.
   - Programinė įranga, pvz., sisteminė programinė įranga, operacinės sistemos; duomenų bazių valdymo sistemos; tarnybinių stočių virtualizavimo programinė įranga; kontrolės ir diagnostikos sistemos ir t.t.
   - Kompiuterių tinklai, pvz., LAN, WAN, VPN ir t.t.
   - Programinės įrangos licencijos.
   - IT Paslaugos (informacinių technologijų išteklių palaikymas ir priežiūra, informacinių technologijų priemonių, reikalingų organizacijos darbuotojui vykdyti savo funkcijas, teikimas ir priežiūra) - IT paslaugos aprašymas ir IT paslaugų katalogas.

   Sąranka ir būsenos rodikliai yra vertinami, rašomos pastabos ir pasiūlymai, viskas dokumentuojama. Nustačius neatitiktis registruojami kreipiniai. Konfigūracijos valdymo sistema turėtų kontroliuoti turto konfigūraciją ir pakeitimus. Taip pat gali būti naudojama konfigūracijos valdymo programinė įranga – CMDB (angl *Configuration Management Database*). Daugumos organizacijų sąranka (IT sistemos ir jos komponentų suderinamumas) nėra dokumentuotas, todėl CMDB sistemos įdiegimas yra būtinas saugai (Koskelo, 2020). CMDB yra

duomenų bazė arba duomenų bazių rinkinys, kuriame yra viena vartotojo sąsaja. CMDB saugoma visa svarbi informacija apie konkrečiame perimetre naudojamus techninės ir programinės įrangos komponentus. CMDB gali palyginti saugos konfigūracijas su esamais konfigūracijos failais ir stebėti pakeitimus (de Moura ir kt., 2020; Kolev ir Ivanov, 2009; Madduri ir kt., 2007). Kalbant apie kibernetinį saugumą, CMDB dažnai naudojamos poveikio analizei atlikti ir pagrindinės gedimo priežasties paieškai. Varela-Vaca, 2020).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kibernetinio saugumo dimensijos 3 priemonės detalizavimas (žr. 41 lentelę).

41 lentelė. Kibernetinio saugumo dimensijos 3 priemonė

3 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Įvertinti ir nustatyti žmogiškųjų resursų poreikį, siekiant užtikrinti kibernetinį saugumą.	Paskirti informacijos saugos įgaliotinį arba kitą specialistą atsakingą už kibernetinį saugumą.	Periodiškai atlikti darbuotojų veiklos vertinimą.

Šaltinis: sudaryta autoriaus

Kibernetinio saugumo dimensijos 3 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Paskirti informacijos saugos įgaliotinį arba kitą specialistą atsakingą už kibernetinį saugumą. Jaučiama vis didesnė kibernetinio saugumo specialistų paklausa (Wang, 2018), kuri tiesiog užvaldo pasiūlą kibernetinio saugumo darbo rinkoje. Niekada nebuvo toks didelis spaudimas kibernetinio saugumo srityje sukurti kuo daugiau kvalifikuotos darbo jėgos (Daimi ir Francia, 2020). Kvalifikuotų kibernetinio saugumo specialistų skaičiaus trūkumas yra iššūkis, turintis ilgalaikę įtaką saugumui. Organizacijoms svarbu samdyti kvalifikuotus kibernetinio saugumo specialistus, kurie užtikrintų kibernetinio saugumo politikos taikymą. Organizacijos paprastai orientuojasi į techninę infrastruktūrą, tačiau dažniausiai nepaisoma socialinių ir etinių saugumo aspektų (Cabaj ir kt., 2018). Organizacijos, norinčios suburti kibernetinio saugumo specialistus, turėtų skirti daugiau dėmesio kandidatams, kurie yra patikimi ir gali sąžiningai tvarkyti informaciją, o ne tiems, kurie yra labai geri specialistai technologijų srityje, tačiau jais negalima pasitikėti. Patikimumą, kaip aukščiausią kibernetinės saugumo specialistų kvalifikaciją, galima įvertinti tarpasmeninio bendravimo, taip pat grupinės sąveikos metu (Ho, 2020). Svarbi organizacijų problema yra kompetentingų specialistų trūkumas ir neužtikrinama kvalifikacijos kėlimo

bei nuolatinių mokymų sistema. Net turint tinkamą saugumo užtikrinimo infrastruktūrą, suformuotą reguliavimo politiką ar naujausias analitikai taikomas technologijas, saugumo rizikos nustatymui reikalingi specializuoti įmonės darbuotojai (Meištaitė, 2021). Williams ir kt. (2017) teigia, kad esant dideliam darbo krūviui (pvz., dėl didelio kognityvinio krūvio, laiko trūkumo ir pan.) žmonės jaučia, kad neturi išteklių elgtis saugiai, siekiant išvengti kibernetinio incidento rizikos, todėl jos nepaiso ir toliau siekia užsibrėžto tikslo, pavyzdžiui, laikytis nustatyto termino. Maurer ir kt. (2021) teigimu, organizacijos sako, kad kibernetinis saugumas yra vienas iš jų didžiausių rūpesčių, jos linkusios padaryti daugiau. Tačiau vis dar nenoriai samdo Saugos įgaliotinį ar prioretizuoja kibernetinį saugumą. Siūlomi galimi šios situacijos priežasčių spėjimai:

- Kibernetinio saugumo biudžetą yra labai sunku pagrįsti, nes nėra žinoma investicijų grąža.
- Gali būti, kad organizacijos vadovo tolerancija rizikai didėja, bijoma, kad saugos reikalavimai slopins produktyvumą ir naujoves.
- Gali būti, kad organizacijose vyrauja požiūris, kad kibernetinio saugumo grėsmės niekur nedings ir net gerai pasirengusios organizacijos patirs incidentų.

2. **II lygis**.
Paskirti informacijos saugos įgaliotinį arba kitą specialistą atsakingą už kibernetinį saugumą. Saugos įgaliotinis yra strateginio lygio pareigybė, atsakinga už tai, kad informacinis turtas ir IT sistemos būtų apsaugoti ir saugūs ir kad tokia apsauga atitiktų organizacijos strateginę kryptį. Saugos įgaliotinio vaidmuo yra paaiškinti saugumo sąvokas suprantamais terminais (naudojant analogiją), įvertinus rizikas informuoti apie esamą saugumo būklę, įtikinti organizacijos vadovus investuoti į saugumą (Hooper ir McKissack, 2016). Saugos įgaliotinis turi būti lyderis ir pokyčių katalizatorius organizacijoje (Subramanian, 2020). Anot Fitzgerald (2018), Saugos įgaliotinio vaidmuo per pastaruosius kelerius metus tapo sudėtingesnis dėl daugybės išorinių ir vidinių organizaciją veikiančių jėgų. Šios jėgos daro įtaką Saugos įgaliotinio veiklos krypčiai, o vėliau ir darbo krūvio prioritetams. Nurodytos išorinės ir vidinės jėgos pasireiškia aukštesniu lygiu nei administracinė, techninė ir veiklos kontrolė, reikalinga užtikrinti sistemų ir informacijos konfidencialumą, vientisumą ir prieinamumą: nauji teisės aktai, asmens duomenų apsauga, technologijų pažanga, nauji produktai / paslaugos, trečiųjų šalių paslaugos, išorės / vidaus auditai, socialinės ir kultūrinės tendencijos, organizacinė kultūra. Karanja, ir Rosso, (2017) tyrimo išvados rodo, kad vis daugiau organizacijų samdo Saugos įgaliotinį, dažniausiai jis būna atskaitingas tiesiogiai organizacijos vadovui. „*Ponemono instituto*“ (2017) ataskaitoje pažymėta, kad organizacijų vadovai dabar labiau nei bet kada supranta, kad vienas rimtas kibernetinio saugumo incidentas ar duomenų saugumo pažeidimas gali nulemti jų organizacijos augimą ir pelningumą dėl poveikio prekės ženklui ir reputacijos atstatymo išlaidų, baudų, klientų nuostolių ir teisinių išlaidų. Todėl Saugos įgaliotinio vaidmuo tampa vis svarbesnis, atsirandant

poreikiui turėti organizacijos IT saugumo strategiją, kuri remtų įmonės misiją ir tikslus (Ritchey, 2020). Kai organizacijos vadovas nežino ar nėra informuotas apie vyraujančią IT saugumo situaciją, gali būti skiriamos mažesnės investicijos į IT saugumo išteklius organizacijoje. Galiausiai dėl mažesnių investicijų gali atsirasti IT saugumo pažeidimų arba netinkamos IT saugumo apsaugos paslaugos, dėl kurių gali kilti duomenų pažeidimų ir pažeidžiamumų (Karanja, 2017).

3. **III lygis**.
   Periodiškai atlikti darbuotojų veiklos vertinimą. Organizacijos, kaip visumos, patikimumas daugiausia priklauso nuo teisingo užduočių paskirstymo tarp pavaldinių (Gnatyuk ir kt., 2019). Veiklos vertinimas užtikrina, kad tiek darbuotojai tiek vadovai skirtų laiko praėjusiems pasiekimams įvertinti ir ateinančioms veiklos kryptims aptarti bei bendriems tikslams nustatyti. Klupšas, F. (2006). Veiklos vertinimas pagal rezultatus yra sudėtingiausias ir pats subjektyviausias veiklos vertinimo būdas. Sėkmingas jo taikymas priklauso nuo daugelio veiksnių, bet pirmiausia nuo pasitikėjimu ir bendradarbiavimu tarp vadovų ir pavaldinių grįstos organizacinės kultūros (Kaselis ir Pivoras, 2012). Nuo organizacijoje dirbančių darbuotojų priklauso jos konkurencinis pranašumas, todėl siekiant prisitaikyti prie greitai kintančios aplinkos organizacijoms svarbu sekti, įvertinti bei gerinti darbuotojų atliekamą veiklą (Judge ir Ferris, 1993). Šiam tikslui pasiekti organizacijose atliekamas darbo vertinimas, leidžiantis priimti sprendimus, susijusius su darbuotojų veikla ir jos rezultatais (Daukšytė ir Lazauskaitė-Zabielskė, 2016).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kibernetinio saugumo dimensijos 4 priemonės detalizavimas (žr. 42 lentelę).

42 lentelė. Kibernetinio saugumo dimensijos 4 priemonė

4 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Užtikrinti atitiktį teisės aktams ir standartams, reglamentuojantiems kibernetinį saugumą.	Atlikti kibernetinio saugumo atitikties vertinimą.	Periodiškai atlikti kibernetinio saugumo atitikties vertinimą.

Šaltinis: sudaryta autoriaus

Kibernetinio saugumo dimensijos 4 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Užtikrinti atitiktį teisės aktams ir standartams, reglamentuojantiems kibernetinį saugumą. Valstybės kontrolė 2022 m. spalio 27 d. valstybinio audito ataskaitoje

„*Kibernetinio saugumo užtikrinimas*“ teigia, kad 2019–2021 m. beveik pusė (45 proc., 80 iš 176) valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų nė karto neatliko informacinių technologijų saugos atitikties vertinimo ir taip neįsitikino savo informacijos saugumo valdymo sistemos būkle, kad, prireikus, laiku galėtų imtis veiksmų ją tobulinti. Nors kibernetinio saugumo klausimai yra gana aiškiai koordinuojami ES lygmeniu, nacionalinių kibernetinio saugumo strategijų reglamentavimas vis dar yra minimalus. Nacionalinės kibernetinio saugumo sistemos turėtų būti suvienodintos, atsižvelgiant į tai, kad kibernetinio saugumo grėsmės dažnai peržengia nacionalinių sienų ribas ir paprastai yra globalios, keliančios iš esmės panašius iššūkius visoms nacionalinėms valstybėms (Štitilis ir kt., 2020). Kibernetinio saugumo vertinimai yra labai svarbūs siekiant užtikrinti, kad gyvybiškai svarbūs kibernetiniai turtai būtų apsaugoti nuo grėsmių (Leszczyna, 2021).

2. **II lygis**.
   Atlikti kibernetinio saugumo atitikties vertinimą. Organizacijoje kibernetinio saugumo programa privalo užtikrinti taikomų teisės aktų laikymąsi. Atitikties vertinimas yra kontrolė, siekiant apsaugoti informaciją ir kitą turtą, nustatytą norminiuose ir kituose teisės aktuose (Schreider 2017). Atitikties įvertinimas – tai procesas, kurio metu nustatoma esama informacinės sistemos kibernetinio saugumo padėtis (Dalalana Bertoglio ir Zorzo, 2017; Qassim ir kt., 2019 ir įvertinamas saugumo tikslų įgyvendinimas (Scarfone ir kt., 2021). Jei atliekama metodologiškai, tai užtikrina, kad kritinis kibernetinis turtas yra apsaugotas nuo grėsmių (Alshamrani ir kt., 2019; Kaloudi ir Li, 2020; Liu ir kt., 2018). Taigi atitikties vertinimas yra labai svarbi veikla, kuri suteikia organizacinių, teisinių, veiklos ir finansinių pranašumų. Atitikties vertinimo trūkumas gali sukelti tiesiogines ir netiesiogines išlaidas, susijusias su praleistomis normatyvinėmis nuostatomis, sertifikatų praradimo rizika, padidėjusia saugumo incidentų tikimybe ir poveikiu (Buccafurri, 2015).
3. **III lygis**.
   Periodiškai atlikti kibernetinio saugumo atitikties vertinimą. Valstybės įmonės privalo ne rečiau kaip kartą per metus organizuoti ir atlikti Atitikties vertinimą, t. y. valstybės informacinių išteklių atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimą. Pagal Kibernetinio saugumo įstatymą, NKSC atlieka valstybės įmonių atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną. Taip pat NKSC teikia konsultacijas ir rekomendacijas kibernetinio saugumo klausimais bei vykdo informacijos sklaidą kibernetinio saugumo klausimais. Taigi organizacijos atlikdamos Atitikties vertinimą ir iškilus neaiškumams dėl vieno ar kito kibernetinio saugumo reikalavimo įgyvendinimo visada gali susisiekti su NKSC ir pasikonsultuoti. Taigi Atitikties vertinimas yra ciklišKas procesas, kurio metu turtas susiduria su kibernetinio saugumo reikalavimais, atsižvelgiant į galimą riziką, grėsmių pasekmes ir susijusias išlaidas. Naudojant sistemoje nustatytas apsaugos priemones, kibernetinio saugumo vertinimu siekiama įvertinti

teisingą kibernetinio saugumo priemonių įgyvendinimą ir veikimą bei jų adekvatumą, atsižvelgiant į sistemos saugumo reikalavimų tenkinimą (Chapple et al., 2018).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kibernetinio saugumo dimensijos 5 priemonės detalizavimas (žr. 43 lentelę).

43 lentelė. Kibernetinio saugumo dimensijos 5 priemonė

5 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Identifikuoti, įvertinti ir suvaldyti kibernetinio saugumo rizikas.	Atlikti kibernetinio saugumo rizikos vertinimą.	Periodiškai atlikti kibernetinio saugumo rizikos vertinimą.

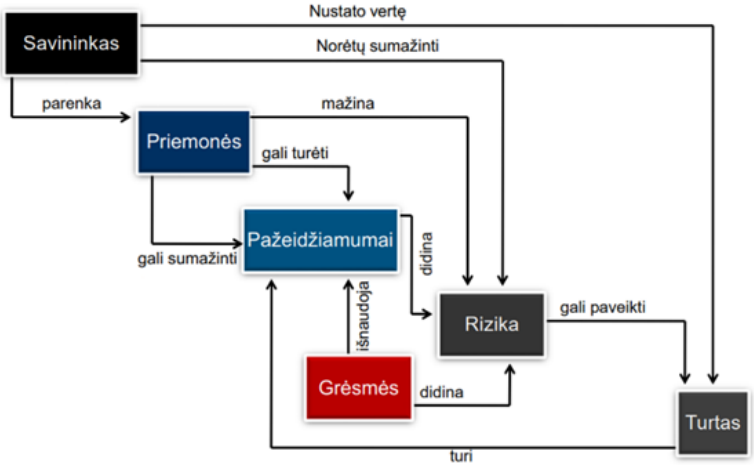
Šaltinis: sudaryta autoriaus

Kibernetinio saugumo dimensijos 5 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Identifikuoti, įvertinti ir suvaldyti kibernetinio saugumo rizikas. Kartu su IT pažanga kibernetinio saugumo sritys nuolat susiduria su naujais grėsmės metodais, kuriais siekiama pasinaudoti IT ir žmogaus pažeidžiamumu (Lee, 2021). Rizika (angl. *Risk*) yra neapibrėžtumo poveikis tikslams, o rizikos valdymas (angl. *Risk management*) atsižvelgiant į riziką suderinti veiksmai, skirti organizacijos veiklai nukreipti ir kontroliuoti. Norint nustatyti organizacinius poreikius, susijusius su IS reikalavimais, būtina vykdyti sistemingą rizikos valdymą. Priemonės saugumui užtikrinti turi padėti suvaldyti riziką veiksmingai ir laiku, t. y. kur ir kada reikia. Kibernetinio saugumo rizikos vertinimo metodai pagrįsti grėsmių vertinimu įtraukiant realios grėsmės informaciją (Gollmann ir kt., 2015). Be to, kaip Menard ir kt. (2017) pripažįsta, kad bet koks kibernetinio saugumo atsakomųjų priemonių taikymas tiesiogiai arba netiesiogiai grindžiamas tam tikra grėsme. Norint sumažinti ar net užkirsti kelią rizikai, reikalingas kibernetinio saugumo rizikos vertinimas, nes jis gali padėti rizikos valdytojams nustatyti rizikos prioritetus, skirti ribotus išteklius joms sumažinti ir priimti tolesnius gynybos sprendimus (Peltier, 2005). Valstybės kontrolė 2022 m. spalio 27 d. valstybinio audito ataskaitoje „*Kibernetinio saugumo užtikrinimas*“ teigiama, kad informacija apie kibernetinio saugumo subjektų identifikuotas kibernetinio saugumo rizikas nekaupiama bei nacionaliniu lygiu nevaldoma. Daugiau kaip trečdalis (38 proc., 81 iš 212) apklaustų kibernetinio saugumo subjektų neatlieka kibernetinio saugumo rizikos vertinimo, dėl to gali būti nepastebėtos naujos ar besikartojančios grėsmės, darančios įtaką subjektų

saugos būklei ir jų veiklai. Kuo labiau pasitikime kibernetinės erdvės teikiamos kibernetinės galimybės, tuo labiau turime apsvarstyti naujus tipus grėsmių, kurios gali labai paveikti mūsų kasdienės veiklos, kritinės veiklos infrastruktūrą ir prieigą prie įvairių paslaugos (Kovács, 2018).

2. **II lygis**.
Atlikti kibernetinio saugumo rizikos vertinimą. Struktūrizuotas rizikos vertinimo atlikimas padeda nustatyti galimas grėsmes, analizuoti jų priežastis ir pasekmes ir aprašyti riziką, paprastai kiekybiškai ir tinkamai atspindint neapibrėžtumus (Zio, 2018). Adolfas Vala (2015) pateikia rizikos vertinimo metu vartojamų sąvokų ryšius (žr. 19 pav.). Terminologijos standartizavimas palengvina efektyvų bendravimą. Tarp disciplinų egzistuoja komunikacijos atotrūkis, kurį galima iš dalies įveikti kuriant ir taikant standartizuotą kalbą (Cains ir kt., 2022).



19 pav. Rizikos vertinimo metu vartojamų sąvokų ryšiai
Šaltinis: Adolfas Vala, 2015

Holistinis požiūris yra toks, kuriame dėmesys sutelkiamas ne tik į komponentus, bet ir į tų komponentų sąveiką, sistemos architektūrą, kūrėjus, vartotojus, tuos, kurie nori pakenkti sistemai, taip pat į tai, kaip sąveika tarp šių objektų sukuria papildomų pažeidžiamumų. Standarte ISO 31000 rašoma, kad Rizikos vertinimas turi būti atliekamas sistemingai, periodiškai ir bendradarbiaujant, atsižvelgiant į suinteresuotųjų šalių žinias ir nuomonę. Reikia naudotis geriausia prieinama informacija, jei reikia, papildant ją tolesniais tyrimais (Scala ir kt., 2019). Rizikos vertinimą sudaro trys dalys:

- *Rizikos identifikavimas*. Rizikos identifikavimo tikslas yra rasti, atpažinti ir apibūdinti riziką, kuri gali pagelbėti ar užkirsti kelią organizacijai pasiekti savo tikslus. Norint nustatyti kibernetinę riziką, reikia suprasti, kokius

metodus pasirenka įsibrovėliai ir įsilaužėliai. Kibernetinės rizikos taksonomijos reiškia išankstines žinias, kurias organizacija turi apie saugotino turto tipus, taip pat pažeidžiamumą ir grėsmes (Rea-Guaman ir kt., 2020).

- *Rizikos analizė*. Rizikos analizės tikslas yra perprasti rizikos pobūdį ir jos charakteristikas. Rizikos analizė apima išsamų neapibrėžtumo, rizikos šaltinių, pasekmių, tikimybės, įvykių, scenarijų, kontrolės priemonių ir jų rezultatyvumo nagrinėjimą.
- *Rizikos įvertinimas*. Rizikos įvertinimo tikslas yra padėti priimti sprendimus. Rizikos įvertinimas apima rizikos analizės rezultatų ir nustatytų rizikos kriterijų palyginimą, kad būtų galima nuspręsti, kada reikalingi papildomi veiksmai. Veiksmų su rizika parinktys gali apimti vieną arba daugiau iš šių dalykų: rizikos vengimą nusprendus nepradėti arba netęsti veiklos, dėl kurios rizika didėja; rizikos prisiėmimą arba didinimą galimybei siekti; rizikos šaltinio pašalinimą; tikimybės keitimą; pasekmių keitimą; rizikos pasidalijimą (pvz., sudarant sutartis, įsigyjant draudimą); rizikos išlaikymą žinojimu pagrįstu sprendimu.

ISO 27005 rašoma, kad rizikos valdymas turėtų padėti: identifikuoti rizikas; įvertinti rizikas atsižvelgiant į jų pasekmes veiklai ir atsiradimo tikimybę; užtikrinti pranešimo apie tokias rizikas ir jų suvokimo tikimybę ir pasekmes; nustatyti prioritetinę rizikos priežiūros tvarką; teikti pirmenybę atsiradusių rizikų mažinimo veiksmams; įtraukti suinteresuotąsias šalis priimant rizikos valdymo sprendimus ir informuoti jas apie rizikos valdymo būklę; veiksmingai stebėti rizikos priežiūrą; stebėti ir reguliariai peržiūrėti rizikas ir rizikos valdymo procesą; rinkti informaciją siekiant pagerinti rizikos valdymo metodą; šviesti vadovus ir darbuotojus apie rizikas ir veiksmus, kurių imtasi siekiant jas sumažinti. Tai, ką organizacijos vertina, yra unikalu ir gali priklausyti nuo jos kibernetinio saugumo brandos lygio, pvz., įmonės dydžio, pramonės sektoriaus, ankstesnės atakų istorijos ir kt. (Black ir kt., 2018). Svarbu suprasti, kad kiekviena organizacija yra individuli, skiriasi joje valdomas turtas, procesai ir procedūros siekiant užtikrinti kibernetinį saugumą, todėl grėsmių sąrašas gali būti didinamas. Nuolatinis grėsmių sąrašo tobulinimas leidžia organizacijoms peržiūrėti būsimas kibernetines investicijas joms suvaldyti. Anot Garrett (2018) kibernetinių grėsmių pobūdis nuolat kinta. ISO 31000 standarte rašoma, kad visų tipų ir dydžių organizacijos susiduria su išoriniais ir vidiniais veiksniais bei įtakomis, dėl kurių tampa neaišku, ar joms pavyks pasiekti savo tikslus.

3. **III lygis**.

Periodiškai atlikti kibernetinio saugumo rizikos vertinimą. Rizikos valdymas yra kartotinis procesas, padedantis organizacijoms nustatyti strategiją, siekti tikslų ir priimti žinojimu pagrįstus sprendimus. Kibernetinio saugumo srityje aplinka nuolat keičiasi, o atsiradus naujoms grėsmėms ir technologijoms pasikeis arba duomenų, naudojamų atliekant pirminį rizikos vertinimą, pritaikymas, arba paties rizikos vertinimo pagrįstumas. Taip pat yra didelių psichologinių kliūčių, pavyzdžiui, tai, kad kibernetinio saugumo išlaidos, skirtingai nei kitos

išlaidos, nesukelia lengvai atpažįstamos investicijų grąžos. Vietoj to, tai gryna esamų investicijų apsauga, o ne būdas gauti pajamų (Fielder ir kt., 2018). Kibernetinės rizikos valdymui skiriamos didelės pinigų sumos, dažnai mažai žinoma informacijos apie priimtų priemonių efektyvumą ir prioritetus tarp jų (Paté-Cornell ir kt., 2018).Pasaulyje, kuris yra tankiai sujungtas, labai priklausomas nuo informacijos ir komunikacijos, savalaikiai ir aktualūs duomenys gali padėti priimti informatyvesnius sprendimus bet kurioje srityje, ypač kibernetinio saugumo srityje (Roldán-Molina ir kt., 2017). Kadangi pažeidžiamumų skaičius didėja, o grėsmių sudėtingumas ir toliau tobulėja, poreikis tinkamai suprasti santykinę kibernetinę riziką yra svarbus siekiant veiksmingai nustatyti rizikos mažinimo priemonių prioritetus ir užtikrinti tvirtą saugumo poziciją (Claroty, 2021; Eggers ir Le Blanc, 2021).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kibernetinio saugumo dimensijos 6 priemonės detalizavimas (žr. 44 lentelę).

44 lentelė. Kibernetinio saugumo dimensijos 6 priemonė

6 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Užtikrinti kibernetinio saugumo švietimą ir kultūrą.	Rengti arba organizuoti kibernetinio saugumo pratybas, mokymus ir konsultacijas.	Parengti kibernetinio saugumo pratybų ir mokymų planą.

Šaltinis: sudaryta autoriaus

Kibernetinio saugumo dimensijos 6 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Užtikrinti kibernetinio saugumo švietimą ir kultūrą. Zimmermann ir Renaud (2019) pristatė ir aptarė keletą veiksnių, kurie gali lemti daugelį žmonių pažeidžiamumų organizacijose, pavyzdžiui: neoptimalus saugumo rizikos suvokimas; kai kurių organizacijų informuotumas apie saugumą ir kultūrą; per didelis pasitikėjimas ydingomis euristinėmis problemomis ir sprendimų priėmimo šališkumas; individualūs skirtumai, susiję su tokiais veiksniais kaip rizikos užduotys, impulsyvumas, pasitikėjimas ir savimonė; netinkamas elgesys dėl tokių veiksnių kaip laiko spaudimas, didelė kognityvinė apkrova, didelis stresas ir darbas tokiomis sąlygomis, kai vyrauja pertraukimai ir trukdžiai. Laiko trūkumas gali turėti neigiamą poveikį užduočių vykdymui, teigiama, kad žmogaus kibernetinio saugumo klausimai nėra išimtis (Chowdhury ir kt., 2019). Saugesnis kibernetinio saugumo elgesys pastebimas tarp asmenų, kurie vertina

grėsmę kaip didelę, suvokia, kad turi reikiamų įgūdžių apsisaugoti, mato šios apsaugos vertę ir supranta savo vietą kibernetinio saugumo grandinėje (Bishop ir kt., 2020). Pastebėta, kad organizacijos pasitelkia technologinius sprendimus ir politiką sprendžiant kibernetinio saugumo problemas, tačiau darbuotojų mokymai ir kibernetinio saugumo sąmoningumo ugdymas nėra prioretizuojami (Rauf, 2019). Nėra vienareikšmės kibernetinio saugumo kultūros apibrėžties, kuri galėtų būti laikoma pagrindu kibernetinio saugumo kultūros teoriniuose ir empiriniuose tyrimuose. Tačiau, visuose atliktuose tyrimuose pateikiami kibernetinio saugumo kultūrą įtakojantys išoriniai ir vidiniai faktoriai yra orientuoti į žmogaus elgesį. Tai suponuoja kibernetinio saugumo kultūros plėtojimą informuotumo didinimo, mokymo ir švietimo programomis. Išskirti du esminiai faktoriai į kuriuos turi būti atsižvelgta kuriant informavimo kampanijas: pateikimo formato dalyviams patrauklumas ir dalyvio įsitraukimo didinimas (Chochlova, 2022). Makrolygmeniu kibernetinio saugumo užtikrinimą verslo procesuose lemia valstybės dalyvavimo intensyvumas formuojant kibernetinio saugumo politiką, ES priimtos direktyvos ir reglamentai. 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 kibernetinį saugumą (Paulius Pelenis, 2015). Kibernetinio saugumo kultūros vystymas yra didelis žingsnis link saugesnės kibernetinės erdvės (Aiken, 2019). Tačiau Coventry ir kt., (2020) teigia, kad darbuotojai, nors ir žino apie gresiančias išorines grėsmes organizacijoje, tačiau jų elgesys nebūtinai šias grėsmes sumažina. Įvardijamos trys pagrindinės to priežastys: saugumas, suvokiamas kaip našumo kliūtis, blogas elgesio pasekmių suvokimas, Saugaus elgesio kultūros stiprinimo trūkumas. ENISA 2018 metų ataskaitoje „*Kibernetinio saugumo kultūra organizacijoje*“ rašoma, kad organizacijų kibernetinio saugumo kultūra reiškia žmonių žinias, įsitikinimus, suvokimą, požiūrį, prielaidas, normas ir vertybes apie kibernetinį saugumą ir tai, kaip jie pasireiškia žmonių elgesiu su informacinėmis technologijomis. Kibernetinio saugumo kultūra nukreipta į evoliuciją ir plėtrą, prisitaikant prie naujų informacinių technologijų ir naujausių skatinimo būdų. Kibernetinio saugumo kultūrai būdingas lankstumas ir pritaikomumas, kintantis kartu su visuomenės, ypač skaitmeninės visuomenės, raida (Pătrașcu, 2019).

2. **II lygis**.
   Rengti arba organizuoti kibernetinio saugumo pratybas, mokymus ir konsultacijas. ENISA ataskaitoje „*Grėsmių peizažas 2022*“ rašoma, kad organizacijos personalas turi būti mokomas atlikti su kibernetiniu saugumu susijusias pareigas ir įsipareigojimus, atitinkančius organizacijos kibernetinio saugumo politiką. Organizacijos turėtų rengti pratybas, pvz. socialinės inžinerijos, kurių metu yra stebimas darbuotojų gebėjimas atpažinti socialinės inžinerijos atakas. Kibernetinio saugumo srityje socialinė inžinerija vilioja vartotojus atidaryti

dokumentus, failus ar el. laiškus, lankytis svetainėse arba suteikti pašaliniams asmenims prieigą prie sistemų ar paslaugų. Atliekant kibernetinio saugumo pratybas gali būti pasitelkiamas reguliarių žaidimų ir simuliacijų kūrimas, siekiant mokyti žmones, kaip reaguoti į skirtingas galimas grėsmes (Dean ir McDermott, 2017). Siekdami sumažinti socialinės inžinerijos išpuolių galimų padarinių tikimybę, organizacijos turėtų ne tik stengtis stiprinti darbuotojų žinias apie saugumą, bet ir investuoti į darbuotojų supratimo apie socialinę inžineriją didinimą (Aldawood ir kt., 2020). Longley (2019) savo tyrime aprašė darbuotojų žinių trūkumų pasekmes, kai daugelyje šalių trūksta tinkamos kvalifikacijos kibernetinio saugumo specialistų, tačiau atkreipiamas dėmesys, kad tai neturi būti pasiteisinimas neinvestuoti į reikalingus išteklius kibernetinei rizikai suvaldyti (Lin ir kt., 2019; Meištaitė, 2021). Kai saugumo valdymas yra gerai apibrėžtas, Saugos įgaliotinis turi tinkamą valdžios ir atsakomybės pusiausvyrą (Blum, 2020). Kadangi vadovybė vaidina svarbų vaidmenį organizacijos saugumo kultūroje, būtina užtikrinti, kad saugumo procesai atitiktų vadovo tikslus ir organizacijos strateginę kryptį (Reeves ir kt., 2020).

3. **III lygis**.
   Parengti kibernetinio saugumo mokymų ir pratybų planą. KAM Nacionalinio kibernetinio saugumo būklės ataskaitoje už 2021 metus rašoma, kad nepriklausomai nuo to, kas vykdo kibernetinio saugumo mokymus: pati organizacija ar samdo mokymų specialistus, patariama organizuoti apie 11 kibernetinio saugumo mokymų darbuotojams per metus. Norint sustiprinti supratimą apie kibernetinį saugumą, nepakanka vien surengti kelis mokymo kursus savo darbuotojams. Reguliarus mokymo kursų vedimas yra gyvybiškai svarbus norint įgyti ir išlaikyti sąmoningumą (ID Agent, 2021). Mokymo kursai, kuriuose daugiausia dėmesio skiriama naujų technologijų naudojimui, virtualių komandų kūrimui ir valdymui bei elektroninių nusikaltimų prevencijos priemonėms, turi tapti didesne šiuolaikinių verslo struktūrų dalimi (Lois ir kt., 2020). Švietimo, informuotumo didinimo ir mokymo programos turi būti pastoviai vystomos ir atnaujinamos, atsižvelgiant į besikeičiančią kibernetinio saugumo situaciją ir besikeičiančias kibernetines grėsmes. Turėtų būti kuriamos bei palaikomos ir naujos studijų programos. Tiek Lietuvoje, tiek aplinkinėse valstybėse šiuo metu rengiama daug techninio profilio specialistų, tačiau trūksta specialistų, turinčių vadybines, teisines žinias, sugebančių valdyti kibernetinio saugumo procesus (Štitilis ir kt., 2017).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kibernetinio saugumo dimensijos 7 priemonės detalizavimas (žr. 45 lentelę).

45 lentelė. Kibernetinio saugumo dimensijos 7 priemonė

7 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Užtikrinti veiklos tęstinumą ir atkūrimą.	- Parengti ir patvirtinti kibernetinių incidentų valdymo planą; - Parengti veiklos tęstinumo ir atkūrimo valdymo planą.	Periodiškai atlikti veiklos tęstinumo ir atkūrimo valdymo plano išbandymo pratybas.

Šaltinis: sudaryta autoriaus

Kibernetinio saugumo dimensijos 7 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Užtikrinti veiklos tęstinumą ir atkūrimą. Veiklos tęstinumas yra gyvybiškai svarbus daugelio organizacijų reikalavimas, nes staigus paslaugų teikimo sutrikimas gali tiesiogiai paveikti organizacijos tikslus ir sukelti didelių pajamų, reputacijos ir rinkos dalies praradimus. Kai kalbame apie organizacijos tvarumą, pirmiausia turime omenyje techninės ir programinės įrangos, kaip informacinių sistemų pagrindo, veikimą (Nikolovski ir Mitrevski, 2022). Kiekviena organizacija, kurios veikla paremta informacinėmis technologijomis, turi reaguoti į poreikį sukurti veiklos tęstinumo ir atkūrimo planą, kad būtų užtikrintas greitas atsigavimas įvykus incidentui (Fernando, 2017). Organizacijos turi nustatyti tikėtinus įvykius, galinčius sukelti nelaimes, ir įvertinti jų poveikį. Rengiant veiklos tęstinumo ir atkūrimo planą reikia atsižvelgti nelaimės atveju atsižvelgti į organizacijos duomenų poreikius ir jų atkūrimo po nelaimės tikslus. Norint įvertinti riziką, reikia nustatyti nelaimių tipus (gamtinės ar žmogaus sukeltos) ir nustatyti tikimybę kartu su atitinkamų gedimų išlaidomis (Alhazmi ir Malaiya, 2013). Veiklos tęstinumo ir atkūrimo valdymo planas yra procedūrinės gairės, kurios užkerta kelią bet kokiam sutrikimui, parengia, reaguoja, valdo ir atkuria organizacijos veiklą. Daugelis organizacijų nesuvokia, kad veiklos tęstinumo ir atkūrimo valdymo planas yra būtinas jų veiklos tęstinumui, nes joms labiau rūpi jų pagrindinis tikslas - pelningumas ir rinkos augimas, o ne veiklos tęstinumas (Fani ir Subriadi, 2019).
2. **II lygis**.
   - Parengti kibernetinių incidentų valdymo planą. Kibernetinių incidentų valdymui naudojamas techninės įrangos, programinės įrangos ir žmogaus vykdomo tyrimo bei analizės derinys. Kibernetinių incidentų valdymo procesas paprastai prasideda įspėjimu, kad įvyko incidentas, ir reagavimo į incidentą atsakingų asmenų įtraukimu. Atsakingi asmenys analizuos incidentą, kad nustatytų jo mastą, įvertintų žalą ir parengs priemonių planą jam užkardyti (Lord, 2018). Kibernetinio saugumo incidentų valdymo tikslas – sumažinti šių incidentų

poveikį organizacijoms ir užkirsti kelią jų pasikartojimui. Jame išsamiai aprašomi procesai, reikalingi kibernetiniams incidentams spręsti, ištekliai, atsakingų asmenų vaidmenys ir komunikacijos kanalai. Turi *būti* taikomos tinkamos procedūros, kad incidentai nepasikartotų (Bisson, 2021). Incidentų valdymo plano įgyvendinimas turi daug privalumų - sumažintas prastovos laikas, ateities incidentų prevencija, patobulintas komunikavimas. Pvz. ISO 27035-1 standarte yra pateikiami informacijos saugos incidentų valdymo principai kurie suskirstyti į penkias sritis: planavimas ir pasiruošimas, aptikimas ir ataskaitų teikimas, įvertinimas ir sprendimas, reagavimas į incidentus, išmoktos pamokos. NIST „*Kompiuterių saugos incidentų valdymo vadove*" nurodyti keturi reagavimo į incidentus žingsniai: paruošimas, aptikimas ir analizė, sulaikymas, naikinimas ir atkūrimas, veikla po incidento. Organizacijos vadovaujantis gerąja praktika pačios sprendžia, kaip detaliai apsirašys kibernetinių incidentų valdymo planą ir kokias organizacines ir technines priemones naudos. Organizacijos valdančios valstybės informacines sistemas t. y. Kibernetinio saugumo subjektai įvykus kibernetiniam incidentui privalo reaguoti pagal nacionalinį kibernetinių incidentų valdymo planą patvirtintą LRV 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „*Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo*". Taigi kibernetinio saugumo subjektai remdamiesi šiuo aukščiau paminėtu teisės aktu pasirengti vidaus tvarką, kurioje būtų reglamentuotas kibernetinių incidentų valdymas. Organizacija turi paskirti atsakingą asmenį už kibernetinių incidentų valdymą, kuris informuos atitinkamas institucijas apie įvykusį kibernetinį incidentą (nustatęs jo poveikio kategoriją) per atitinkamą laiką. Kibernetinio saugumo subjektai apie incidentą NKSC gali pranešti telefonu, e. paštu arba užpildę specialią formą jų internetiniame puslapyje. Pranešime informuojant apie didelio ar vidutinio poveikio kibernetinius incidentus pateikiama informacija koks ir kada kibernetinis incidentas įvyko arba buvo nustatytas bei kaip jis bus šalinamas. Asmenys, kuriems teisės aktuose nėra nustatytos pareigos apie kibernetinius incidentus pranešti NKSC, turi teisę tai padaryti savanoriškai. Tinkamas reagavimas į kibernetinius incidentus sumažina galimą patirti žalą, siekiant užtikrinti kibernetinį saugumą. Organizacijoms svarbu išlaikyti veiklos tęstinumą net ir kibernetinės atakos metu, o tai reikalauja didelio organizacijų atsparumo, gebėjimas pasiruošti ir prisitaikyti prie besikeičiančių sąlygų bei greitai atlaikyti ir atsigauti po kibernetinių incidentų (Aoyama ir kt., 2015). Kibernetinių incidentų valdymas gali būti ne toks sudėtingas procesas, jei iš anksto suprantate sprendimų priėmimo iššūkius (Aoyama ir kt., 2015).

- *Parengti veiklos tęstinumo ir atkūrimo valdymo planą.* Veiklos tęstinumo ir atkūrimo valdymo plano tikslas - pasirengti organizacijai greitai ir ryžtingai reaguoti kritinėje situacijoje, užtikrinti darbuotojų saugumą ir atnaujinti organizacijos veiklą su minimaliais trikdžiais (Alvero, 2021). Organizacija norėdama parengti veiklos tęstinumo valdymo planą pirmiausiai turėtų sudaryti organizacijos informacinių išteklių sąrašą ir priskirti atsakingus asmenis už tinkamą jų veikimą, atlikti informacinių išteklių poveikio informacijos konfidencialumui,

vientisumui ir prieinamumui įvertinimą, siekiant nustatyti kritinę infrastruktūrą. Nustatyti ir įvertinti informacinių išteklių RPO (angl. *Recovery Point Objective*) – toleruotinus duomenų praradimo dydžius ir RTO (angl. *Recovery Time Objective*) – minimalius paslaugų atstatymo laiko intervalus (Baig, 2022). Pvz., jei RTO yra 2 valandos, tai reiškia, kad norite atnaujinti veiklos vykdymą po 2 valandų. RPO ir RTO vertės įvairiose įmonėse gali skirtis, tačiau visada bus kompromisas tarp verslo poreikių dėl prieinamumo ir reikalingų IT investicijų. Jų įvertinimas turėtų būti organizacijos ir IT ekspertų svarstymo rezultatas. Šių tikslų pasiekti neįmanoma neįsigijus atsarginių kopijų/duomenų atkūrimo programinės įrangos arba debesies paslaugų. (Zgureanu, 2022). Kosutic (2017) teigia, kad RTO yra orientuotas į paslaugų, programų ir procesų prastovą, padedantis apibrėžti veiklos tęstinumui paskirstytinus išteklius, o RPO yra orientuotas į duomenų kiekį, vienintelis tikslas yra apibrėžti atsarginių kopijų dažnį. Kitas svarbus skirtumas, kad, atsižvelgiant į incidento momentą, RTO žiūri į priekį (t. y. laikas, kurio reikia veiklai atnaujinti), o RPO žiūri atgal (t. y. kiek laiko ar duomenų esate pasirengęs prarasti). Svarbu atkreipti dėmesį, kad RTO naudojamas norint nustatyti, kokių pasirengimo priemonių reikia incidento atveju, kalbant apie pinigus, patalpas, telekomunikacijas, automatizuotas sistemas, personalą ir kt. Kuo trumpesnis RTO, tuo daugiau išteklių reikia. RPO naudojamas duomenų atsarginių kopijų kūrimo dažnumui nustatyti, kad būtų galima atkurti reikalingus duomenis įvykus nelaimei. Pvz. jeigu RPO yra 4 valandos, atsarginę kopiją turite atlikti bent kas 4 valandas.

3. **III lygis**.
   - Periodiškai atlikti veiklos tęstinumo ir atkūrimo valdymo plano išbandymo pratybas. Testavimas yra pagrindinis veiklos tęstinumo ir atkūrimo plano komponentas, siekiant nustatyti, ar veiklos tęstinumo ir atkūrimo planas yra tinkamas kritinei rizikai pašalinti. Be to, kad būtų užtikrinta, kad atkūrimo komandos nariai – tiek pirminiai, tiek pakaitiniai – žinotų, ką daryti, testavimas vis realesnėmis sąlygomis padeda ugdyti pasitikėjimą ir išvengti panikos nelaimės metu. Daugelis organizacijų neatlieka veiklos tęstinumo ir atkūrimo plano bandymų, tačiau bandymai yra labai svarbūs, nes jų metu yra imituojami incidentai, siekiant patikrinti veiklos tęstinumo ir atkūrimo plano realų įgyvendinimą (Cerullo ir Cerullo, 2004).

Toliau esančioje lentelėje yra pateikiamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kibernetinio saugumo dimensijos 8 priemonės detalizavimas (žr. 46 lentelę).

46 lentelė. Kibernetinio saugumo dimensijos 8 priemonė

8 priemonė		
I lygis (ką privalu atlikti organizacijoje?)	**II lygis (kaip įgyvendinti?)**	**III lygis (kaip patobulinti arba užtikrinti įgyvendinimą?)**
Nustatyti organizacijos strateginiai tikslai.	Parengti veiklos strateginį planą.	Stebėti ir užtikrinti veiklos strateginio plano įgyvendinimą.

Šaltinis: sudaryta autoriaus

Kibernetinio saugumo dimensijos 8 priemonės pirmame, antrame ir trečiame lygiuose organizacija turi įgyvendinti:

1. **I lygis**.
   Nustatyti organizacijos strateginius tikslus. Organizacija privalo identifikuoti savo veiklą ir apibrėžti trumpalaikius ir ilgalaikius tikslus bei šių tikslų įgyvendinimo procesą. Nuoseklus trumpalaikių tikslų įgyvendinimas laiku suteiktų organizacijai galimybę pasiekti užsibrėžtą ilgalaikį tikslą. Pagrindinis ilgalaikis organizacijos tikslas, be jokios abejonės, yra siejamas su teisėtu ir saugiu asmens duomenų tvarkymu, o trumpalaikiai organizacijos siekiami tikslai gali būti tapatinami su tam tikrų organizacinių ir techninių priemonių įgyvendinimu. Jei plano nėra, darbas vis tiek atliekamas kasdien, tačiau dažnai trūksta tikslo ir prioriteto (Mccarthy, 2018).
2. **II lygis**.
   - Parengti veiklos strateginį planą. Strateginis veiklos planas – veiklos planavimo dokumentas, kuriame, atsižvelgiant į ilgos ir vidutinės trukmės planavimo dokumentų nuostatas, aplinkos analizės išvadas, yra suformuluota organizacijos misija, strateginiai tikslai, aprašomos vykdomos programos, siekiami rezultatai ir numatomi asignavimai. Anot Allison ir Kaye (2011) strateginis planavimas padeda organizacijai susitelkti, įvertinti viziją ir prioritetus atsižvelgiant į besikeičiančią aplinką ir užtikrinti, kad organizacijos nariai siektų tų pačių tikslų. Strateginių planų turinys priklauso nuo surinktos informacijos kokybės ir strateginio planavimo metu atliekamos analizės (George, 2021). Tyrimai atskleidė, kad bent pusę visų strateginių sprendimų žlunga jų priėmimo procese. Strateginis valdymo procesas yra integruoto valdymo sritis, kuri jungia analizę, tikslų formulavimą ir įgyvendinimą ir kuri gali lemti konkurencinį pranašumą (Rothaermel, 2012). Strateginis planavimas padeda, kadangi jis leidžia susikoncentruoti į svarbiausius klausimus ir iššūkius, padeda išsiaiškinti kokių priemonių reikia imtis, norint įveikti iššūkius (Bryson, 2018). Bet kurio strateginio plano rengimo būtina sąlyga yra aukšto lygio prioritetų, kuriais vadovaujamasi kuriant tą planą, supratimas (Parker, 2018). Valstybės įmonės turi parengti informacinių ir ryšių technologijų plėtros planą. Informacinių ir ryšių technologijų (IRT) plėtros plane, kaip to reikalauja LR valstybės Informacinių išteklių valdymo įstatymas, turi būti nustatyti informacinių technologijų priemonių, skirtų

informacijai, duomenims, dokumentams ir (arba) jų kopijoms tvarkyti, kūrimo ir naudojimo tikslai, uždaviniai, nurodomos planuojamos kurti ar modernizuoti valstybės informacinės sistemos ir registrai, jų steigimo, modernizavimo prioritetai, planuojamos diegti elektroninės paslaugos, reikalingi finansiniai ir žmogiškieji ištekliai, organizacinės ir teisinės priemonės, kvalifikaciniai reikalavimai darbuotojams, darbuotojų mokymų poreikis, jų veiklos organizavimas ir kontrolė. Strateginis kibernetinio saugumo valdymas atsirado per evoliucinę plėtrą iš strateginio organizacijos informacinės aplinkos kibernetinio saugumo būklės planavimo, kuris yra esminis jos pagrindas. Pokyčių, įvykusių organizacijos informacinėje aplinkoje iš kibernetinio saugumo pozicijų, esmė sumažinama iki jos kibernetinio saugumo strateginio planavimo proceso išskaidymo į tris tarpusavyje susijusias, bet kartu ir savarankiškas veiklas, atitinkančias pagrindinės kibernetinio saugumo valdymo funkcijas: kibernetinio saugumo strategijos kūrimas remiantis organizacijos informacinės aplinkos išorinės ir vidinės aplinkos analize, galimų alternatyvų svarstymu; strategijos organizavimas pagal maksimalaus kibernetinio saugumo ir minimalių išlaidų kriterijų; kibernetinio saugumo rezultatų stebėjimas ir vertinimas prieš ir po įvykių įgyvendinimo (Mandritsa, 2018).

3. **III lygis**.
   Stebėti ir užtikrinti veiklos strateginio plano įgyvendinimą. Įgyvendinat strategiją būtina užtikrinti proceso kontrolę. Privaloma nuolat prižiūrėti kaip vyksta strategijos įgyvendinimas ir kaip fiksuojami šio proceso rezultatai bei besikeičianti aplinka, nuolat stebėti, vertinti kaip įgyvendinamas strateginis planas, priklausomai nuo išorės veiksnių atlikti strateginio plano korekciją (Raipa, 2002; Arimavičiūtė, 2005). Planuojant strategiją būtina atsižvelgti į tai, kad sprendimai nėra priimami vakuume ir kad bet koks organizacijos veiksmas greičiausiai bus sureaguotas paveiktų asmenų – konkurentų, klientų, darbuotojų ar tiekėjų – reakcija (Maleka, 2016).

4.3. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkiai ir galimybės

Šioje disertacinio darbo dalyje, remiantis kokybinio tyrimo rezultatais, vertinami suformuoto asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkiai ir galimybės.

Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis yra sudarytas iš dviejų dimensijų:

1. Asmens duomenų apsaugos dimensija užtikrina teisėtą asmens duomenų tvarkymą ir atitinkamas technines ir organizacines priemones, siekiant apsaugoti pagrindines duomenų subjekto teises ir laisves, visų pirma jų teisę į asmens duomenų apsaugą.
2. Kibernetinio saugumo dimensija užtikrina kibernetinio saugumo valdymą ir atitinkamas technines ir organizacines priemones, siekiant apsaugoti

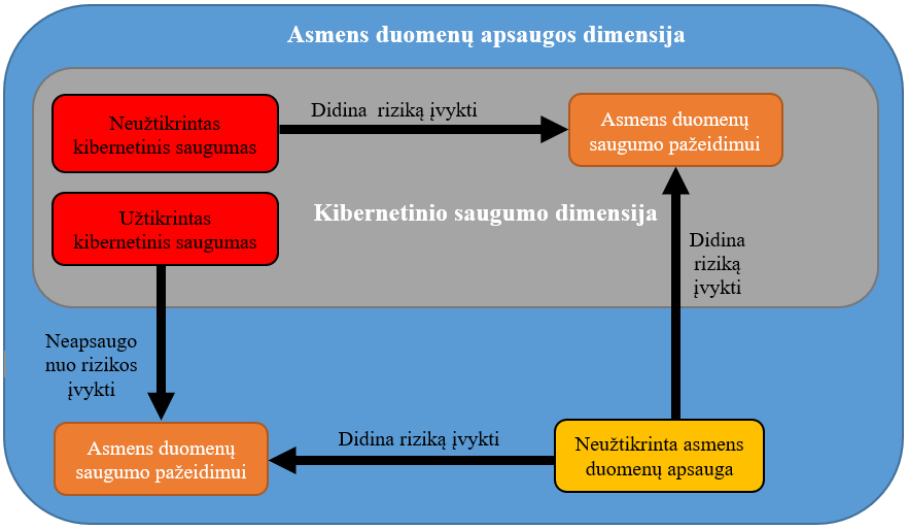
informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumą, vientisumą bei konfidencialumą.

Žvelgiant per kibernetinio saugumo dimensijos prizmę, neužtikrinant kibernetinio saugumo kyla rizika įvykti asmens duomenų saugumo pažeidimui, nes asmens duomenys gali būti atskleisti, prarasti ir neprieinami. Tačiau nors ir užtikrinant kibernetinį saugumą vertinant per asmens duomenų apsaugos dimensijos prizmę kyla rizika įvykti asmens duomenų saugumo pažeidimui, nes asmens duomenys gali būti tvarkomi pažeidžiant pagrindinius asmens duomenų tvarkymo principus:

- Duomenys tvarkomi neteisėtai, nesąžiningai ir neskaidriai;
- Nenustatytas duomenų tvarkymo tikslas
- Tvarkomi pertekliniai duomenų kiekiai;
- Duomenys yra netikslūs arba neteisingi;
- Duomenys saugomi per ilgai;
- Duomenų valdytojas arba tvarkytojas yra neatskaitingas, siekiant įrodyti, kad duomenis tvarko teisėtai ir saugiai.

Visiems aukščiau išvardintiems asmens duomenų saugumo pažeidimams, įskaitant atitinkamų kibernetinių techninių ar organizacinių priemonių netaikymas, kyla rizika įvykti neužtikrinant asmens duomenų apsaugos dimensijos.

Svarbu atkreipti dėmesį, kad kibernetinio saugumo dimensija yra asmens duomenų apsaugos dimensijos dalis, kuri negali užtikrinti asmens duomenų apsaugos (žr. pav. 20).



20 pav. Kibernetinio saugumas neapsaugo nuo asmens duomenų saugumo pažeidimo

Šaltinis: sudaryta autoriaus

Tikėtina, kad, naudojant disertacijos autoriaus sukurtą asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį asmens duomenų apsaugai ir

kibernetiniam saugumui užtikrinti, sumažins tikimybę įvykti asmens duomenų saugumo pažeidimams organizacijose valdančiose ir/ ar tvarkančiose asmens duomenis. Bus užtikrintas ne tik elektroninės informacijos, įskaitant duomenis ir asmens duomenis, prieinamumas, vientisumas bei konfidencialumas bet ir pagrindiniai asmens duomenų tvarkymo principai, apsaugant fizinių asmenų teises ir laisves dėl asmens duomenų tvarkymo.

Tačiau būtina pažymėti, kad šiame disertaciniame darbe sukurtas ir aptartas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis atspindi tik bendrą organizacijų požiūrį į asmens duomenų apsaugą ir kibernetinį saugumą ir jo valdymą, nesigilinant į konkrečius asmens duomenų apsaugos ir kibernetinio saugumo valdymo kompanijų siūlomus technologinius sprendimus. Nagrinėjant konkrečias technologines, administracines ir teisines priemones, kuriomis turi būti užtikrinama asmens duomenų apsauga ir kibernetinis saugumas organizacijoje, būtina naudoti ne tik šį asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį, kuris iš esmės yra tam tikras asmens duomenų apsaugos ir kibernetinio saugumo valdymo organizacinis pagrindas (angl. *Framework*), bet ir būtinai pasinaudoti gerosiomis asmens duomenų apsaugos ir kibernetinio saugumo valdymo praktikomis (standartais, technikomis ir kt.), kurių paskirtis yra siejama su konkrečių teisinių, organizacinių ir techninių rizikų valdymu ar kitų asmens duomenų apsaugos ir kibernetinio saugumo klausimų sprendimo būdais.

Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis yra skirtas visapusiškam organizacijos asmens duomenų apsaugos ir kibernetiniam saugumui valdyti ir užtikrinti, atsižvelgiant į visus organizacijos valdomus išteklius ir vykdomus veiklos procesus. Vien tik technologiniais sprendimais grįsta asmens duomenų apsauga ir kibernetinis saugumas, kuriam užtikrinti panaudojamos techninės ir programinės priemonės, negarantuoja saugaus asmens duomenų tvarkymo, kadangi tai yra tik viena iš priemonių. Tik konceptualus požiūris į asmens duomenų apsaugą ir kibernetinį saugumą bei jų valdymą, įtraukiant į organizacijos valdymo procesą ne tik technologines priemones, bet ir organizacines priemones bei teisines priemones, garantuoja asmens duomenų apsaugos ir kibernetinio saugumo lygio padidėjimą organizacijoje.

Pažymėtina, kad asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio dimensijų pirmasis lygmuo yra siejamas su organizacijos gebėjimais aiškiai suprasti arba nustatyti, kokios asmens duomenų apsaugos ir kibernetinio saugumo priemonės turi būti įgyvendintos organizacijoje. Antrasis asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio lygmuo yra orientuotas į konkrečių veiksmų atlikimą arba įgyvendinimą siekiant pokyčių, kurie užtikrintų asmens duomenų apsaugos ir kibernetinio saugumo valdymą. Trečiasis asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio lygmuo yra skirtas užtikrinti priemonės įgyvendinimą ir/ar ją patobulinti. Ketvirtasis lygmuo yra skirtas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modeliui harmonizuoti, asmens duomenų apsaugos ir kibernetinio saugumo dimensijose tarpusavyje integruoti visas išvardintas priemones, siekiant užtikrinti visapusišką asmens duomenų apsaugą

ir kibernetinį saugumą bei jo valdymą organizacijoje. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis gali sumažinti riziką, šiems asmens duomenų saugumo pažeidimams dėl kurių gali būti:

- Padarytas kūno sužalojimas;
- Prarasta asmens duomenų kontrolė;
- Apribotos asmens teisės;
- Kilti diskriminacija;
- Pavogta ar suklastota tapatybė;
- Padaryta finansinių nuostolių;
- Sugadinta reputacija;
- Prarastas asmens duomenų konfidencialumas;
- Padaryta kitokia didelė ekonominė ar socialinė žala.

Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis yra sudarytas iš 16 priemonių. Įgyvendinant asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį organizacijos gali susidurti su iššūkiais:

1. *Kompetencijos ir patirties trūkumas*. Kibernetinio saugumo ir asmens duomenų apsaugos disciplina reikalauja teisinių, vadybos ar technologinių žinių. Pavyzdžiui suvokiant teisės akte reglamentuotą kibernetinio saugumo arba asmens duomenų apsaugos organizacinę priemonę, reikia sukurti procedūrą kaip ją įgyvendinti, o tam reikia vadybos žinių. Taip pat be viso to gali prireikti ir technologinio sprendimo. Todėl galima teigti, kad kibernetiniam saugumui ir asmens duomenų apsaugai būdingas transdisciplinišKumas, kuris reiškia nuolatinį, sistemingą skirtingų disciplinų bendradarbiavimą. Nesuvokiant kibernetinio saugumo ir asmens duomenų apsaugos reglamentavimo ir taikomų asmens duomenų saugaus valdymo priemonių organizacijai nepavyks parengti kibernetinio saugumo politikos ir asmens duomenų apsaugos politikos, kuri sumažintų kibernetinio saugumo arba asmens duomenų saugumo pažeidimo įvykio riziką. Rengiant kibernetinio saugumo politiką ir asmens duomenų apsaugos politiką privalu vadovautis teisės aktais ir gerąja praktika. Kompetencijos trūkumo grėsmė, susijusi su organizacijos gebėjimu įgyvendinti sprendimus. Neturint reikiamos kompetencijos didėja klaidų darymo tikimybė, darbuotojams sunku tobulėti (Gjelsvik ir Saga, 2019). Dėl kompetencijos stokos bet kuri organizacija gali būti pažeidžiama (Nagahawatta ir kt., 2019). Australijos kibernetinio saugumo centro 2017 metų grėsmių ataskaitoje rašoma, kad nesirūpinimas profesiniu tobulėjimu ir žinių atnaujinimu gali lemti sąmoningumo stoką apie esamas kibernetines grėsmes. Kompetencijos trūkumas ir nesupratimas, kaip apsaugoti organizaciją nuo kibernetinių atakų, verčia organizacijas pasitelkti trečiųjų šalių paslaugų teikėjus (Kuzminykh ir kt., 2020; Gutfleisch ir kt., 2022). Taip pat kompetencijos trūkumas trukdo inovacijų sklaidai (Uyarra ir kt., 2014; Georghiou ir kt., 2014). Svarbi organizacijų problema yra kompetentingų specialistų trūkumas, net turint tinkamą saugumo užtikrinimo infrastruktūrą, suformuotą reguliavimo politiką ar naujausias technologijas, saugumo rizikos nustatymui reikalingi specializuoti įmonės darbuotojai, todėl galima teigti, kad

tik finansinių išteklių skyrimo nepakanka (Meištaitė, 2021). Būtina nuolat kelti žmogiškųjų išteklių kvalifikaciją organizacijos viduje ir kartu neatmesti galimybės, kad pakankamai kompetencijos ir svarbių lyderio savybių gali turėti ir žmogus „*iš šalies*" (Raipa ir Jurkšienė, 2013). Neužtenka vieną kartą į metus organizacijoje suorganizuoti kibernetinio saugumo ir asmens duomenų apsaugos mokymus, nes nekartojamos naujos žinios greit pasimiršta, todėl rekomenduojama tokius mokymus rengti kuo dažniau. Taip pat atsižvelgi į skirtingų specialistų poreikius, rengiant individualius mokymus.

2. *Žmogiškųjų išteklių trūkumas*. Valstybės įmonėse už kibernetinio saugumo politikos formavimą yra atsakingas informacijos saugos įgaliotinis, kitose privataus kapitalo organizacijose šią funkciją gali atlikti IT vadovas, kibernetinio saugumo vadovas ir t.t. Siekiant užtikrinti asmens duomenų apsaugą organizacijoje, duomenų apsaugo pareigūnas – prižiūri duomenų valdytojo ar duomenų tvarkytojo atitiktį Reglamentui ir padeda ją užtikrinti. Kaip aptarėme aukščiau nurodytame punkte, kibernetinio saugumo ir asmens duomenų apsaugos disciplinos reikalauja daug žinių, todėl rinkoje susiduriama su šių specialistų trūkumu. Tyrėjai dažnai apgailestauja, kad vadovai per mažai dėmesio skiria žmogiškiesiems ištekliams – personalui (Melnikova, 2008). Pažymėtina, kad organizacijos efektyvumas tiesiogiai priklauso nuo žmogiškųjų išteklių veiklos. (Kurniullah ir kt., 2020). Be žmonių, žinančių, ką, kada ir kaip tai daryti, buvimo organizacijoms būtų neįmanoma pasiekti savo tikslų. BDAR poveikis yra stipriai juntamas žmogiškųjų išteklių veikloje, nes primena, kad žmonės, žmogiškieji ištekliai, kaip ir duomenys, nėra lengva „*prekė*", kurią galima išnaudoti. Svarbų vaidmenį atlieka organizacijos požiūris į atsakomybę, skaidrumą ir pagarbą žmogaus teisėms (Tataru, 2020). Norint užtikrinti BDAR reikalavimus, organizacijoms reikia skirti didesnį dėmesį žmogiškiesiems ištekliams tvarkantiems asmens duomenis (Koski ir Valmari, 2020).
3. *Finansinių išteklių trūkumas*. Finansinių išteklių trūkumas yra viena pagrindinių projektų pradėjimo ir įgyvendinimo kliūčių (Ortas ir kt., 2013; Testa ir kt., 2019; Nigam ir kt., 2018). J. de Vries (2017) teigimu, sprendimai dėl investicijų turėtų būti priimami remiantis išsamia ekonominės naudos analize ir rizikos vertinimu. Tačiau daugelis organizacijų neatlieka šios sudėtingos analizės, nes trūksta duomenų apie išlaidas, naudą ir kibernetinių incidentų poveikį bei tikimybę. Svarbus šios rizikos valdymo aspektas yra tinkamų investicijų paskirstymas (Simon ir Omar, 2020). Asmenys, atsakingi už kibernetinio saugumo pažeidimų prevenciją savo organizacijose, taip pat tie, kurie toms organizacijoms teikia konsultavimo rizikos klausimais paslaugas, turi galvoti apie investicijų į kibernetinį saugumą sąnaudų ir naudos aspektus (Bodin ir kt., 2018).
4. *Komunikacijos ir bendradarbiavimo trūkumas*. Kai kurie tyrimai rodo, kad bendravimas skatina pasitikėjimą ir atvirkščiai. Bendravimas tarp komandos narių daro įtaką jų užduočių atlikimui, nes palengvina pasitikėjimo atsiradimą (Boies ir kt. 2015). Tyrėjai Prati ir kt. (2003) išsiaiškino, kad komandos narių bendravimas paskatino jų tarpusavio pasitikėjimo atsiradimą. Komandos nariai,

kurie pasitiki vienas kitu, yra labiau linkę dalytis informacija. Pasitikėjimas ir bendravimas yra svarbūs projekto sėkmės veiksniai. (Cheun ir kt., 2013). Bendraujančios šalys turėtų stengtis atsakyti į viena kitos klausimus ir išsiaiškinti problemas (Buene ir Fridtun, 2022).

Motyvacijos trūkumas ir pasipriešinimas pokyčiams. Svarbi socialinė ir psichologinė motyvacija (Testa ir kt., 2019, kuomet organizacija nori perteikti savo vertybes, o tam būtina dėti papildomas pastangas (Messeni Petruzzelli ir kt., 2019). Kibernetinio saugumo supratimas dar nepasiekė daugumos organizacijų vadovų. Daugelis lieka įstrigę „*neigimo*" arba „*nerimo*" fazėse. Daugelis gali nesuvokti kibernetinio saugumo kaip pridėtinės vertės savo verslui komponento (Wirth, 2017). Kibernetinis saugumas reikalauja didelių išlaidų, bet duoda nedidelę naudą. Dėl to sunku įrodyti su kibernetiniu saugumu susijusią investicijų grąžą. Atsižvelgiant į tas su kibernetiniu saugumu susijusias investicijas, reikia gerai apgalvoti, nes nėra patikimų duomenų (Blau, 2017). Organizacijoms yra sunku suprasti, į kurias technologijas investuoti (Sommer, 2015). Baumeister ir Vohs (2016) nustatė, kad nuovargis neigiamai veikia kibernetinį saugumą, nes darbuotojai kognityviai ar fiziologiškai pavargsta atlikti dažnai pasikartojančius veiksmus, reikalingus kibernetiniam saugumui palaikyti, nebūtinai formuodami blogą požiūrį. Kibernetinis nuovargis apibūdinamas kaip: „*Nuovargis, vengimas ar akivaizdus motyvacijos trūkumas kibernetinio saugumo srityje, kuris egzistuoja ne tik dėl individualių polinkių, bet pirmiausia dėl pernelyg didelio kibernetinio saugumo poveikio*" (Reeves ir kt., 2020). Kai kurie tyrimai galbūt per daug orientuoti į žmogaus pažeidžiamumą, neatsižvelgiant į aplinkos ar situacijos veiksnius, ir atvirkščiai (Morgan ir kt., 2020). Kalshoven ir Boon (2012) teigia, kad siekiant išsaugoti ir motyvuoti žmogiškuosius išteklius, būtina užtikrinti jų gerovę. Pirmiausia gerą emocinė būklę ir savijautą. Žmonės, atlieka kibernetinio saugumo rizikos kūrimo, didinimo ir mažinimo vaidmenį (Henshel ir kt., 2015; King ir kt., 2018).

Neapibrėžtumas natūraliai yra iššūkis, su kuriuo susiduria visos organizacijos priimdamos sprendimus. Tačiau didžiąją dalį žalos sumažina tik keletas kibernetinio saugumo kontrolės priemonių (Fielder ir kt.,2018). Kibernetinio saugumo kontrolės priemonių įgyvendinimas padeda aptikti, užkirsti kelią, sumažinti arba kovoti su saugumo rizika (Pawar ir Palivela, 2022).

Pažymėtina, kad asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelyje neįmanoma išskirti vienos pačios svarbiausios priemonės, kadangi tik visų priemonių taikymas organizacijoje sujungiant asmens duomenų apsaugos ir kibernetinio saugumo dimensijas į vieną bendrą organizacijos valdymo sistemą gali parodyti aiškius asmens duomenų apsaugos ir kibernetinio saugumo pokyčio rezultatus. Kaip ir buvo minėta anksčiau, kiekviena tiek asmens duomenų apsaugos, tiek kibernetinio saugumo dimensijos priemonė gali būti įgyvendinama atskirai, atsižvelgiant į organizacijos veiklos ypatumus, valdomus išteklius, turimus resursus bei finansines galimybes. Tačiau būtina pažymėti, kad asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio ketvirtasis lygmuo yra siejamas su visų asmens duomenų apsaugos ir kibernetinio saugumo dimensijose išvardintų priemonių įgyvendinimu, siekiant virsmo į integruotą asmens duomenų apsaugos ir kibernetinio

saugumo valdymo sistemą, kurioje priemonės yra vienareikšmiškai susietos bei veikia viena kitą papildo (žr. 16 pav.).

Apibendrinant šį disertacinio darbo skyrių, galima teigti, kad asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, aprašytas šioje disertacinio darbo dalyje, asmens duomenų apsaugos ir kibernetinio saugumo dimensijose nagrinėja įvairias asmens duomenų saugaus valdymo priemones, kurių tikslas yra sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo rizikas, siekiant užtikrinti elektroninės informacijos, įskaitant duomenis ir asmens duomenis, prieinamumą, vientisumą bei konfidencialumą bet ir užtikrinti pagrindinius asmens duomenų tvarkymo principus, apsaugant fizinių asmenų teises ir laisves dėl asmens duomenų tvarkymo. Pažymėtina, kad šį asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį gali naudoti visos organizacijos, valdančios arba tvarkančios asmens duomenis, kurios siekia pagerinti asmens duomenų apsaugą ir kibernetinį saugumą bei jų valdymą ir sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas.

IŠVADOS

1-asis uždavinys. Atlikus asmens duomenų apsaugos ir kibernetinio saugumo sąveikos teorinių aspektų analizę, nustatyta:

1. Organizacijoms valdančioms arba tvarkančioms asmens duomenis, kurie buvo anonimizuoti asmens duomenų apsaugos reikalavimai netaikomi. Tačiau pseudonimizuoti duomenys visiškai patenka į asmens duomenų apsaugos taikymo sritį, lyg asmens duomenys, nes pseudonimizacija nepašalina visos asmens identifikavimo informacijos iš duomenų, o tik sumažina duomenų rinkinio susiejimą su asmeniu. Įvykus kibernetiniam incidentui arba asmens duomenų saugumo pažeidimui, kuomet tvarkomi anonimizuoti ir pseudonimizuoti duomenys, mažėja žala asmens duomenų subjektams apsaugant jų teises į privatumą.
2. Duomenų subjektai turi asmens duomenų apsaugos reglamente įtvirtintas specifines teises, įgalinančias juos kontroliuoti savo asmens duomenimis, kuriuos valdo ir tvarko organizacijos.
3. Duomenų apsaugos pareigūnas užtikrina, kad organizacijoje būtų tinkamai įgyvendinami asmens duomenų apsaugos reikalavimai, tačiau atsakomybė už šių reikalavimų nesilaikymą yra priskiriama duomenų valdytojui ir (ar) tvarkytojui.
4. Absoliutaus asmens duomenų apsaugos ir kibernetinio saugumo pasiekti neįmanoma, bet tinkamai parinktos ir taikomos saugumo priemonės gali sumažinti rizikos laipsnį ir praradimų mastą.

2-asis uždavinys. Atlikus kokybinius dokumentų analizės, atvejo analizės ir ekspertų nuomonės tyrimus, kuriais remiantis būtų nustatyti asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių kriterijai modeliui sukurti, galima daryti išvadas:

1. Skirtinguose teisės aktuose ir standartuose ISO 27001 ir ISO 27002 bei VDAI gairėse tam tikri išdėstyti reikalavimai kibernetiniam saugumui ir asmens duomenų apsaugai užtikrinti yra tapatūs, tai apsunkina šių reikalavimų įgyvendinimą organizacijoms.
2. Įvertinus trijų organizacijų kibernetinio saugumo ir asmens duomenų apsaugos reglamentavimą vidaus teisės aktuose ir faktinį jų įgyvendinimas praktikoje, nustatyta, kad organizacijos periodiškai neatnaujina saugos dokumentų, neatlieka rizikos vertinimų ir informacinių technologijų saugos atitikties vertinimų, nerengia mokymų, neatlieka veiklos tęstinumo valdymo plano išbandymo pratybų ir neužtikrina trečiųjų šalių paslaugų tiekėjų kontrolės.
3. Įvertinus 100 populiariausių Lietuvos interneto svetainių, didžioji dauguma organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), nesilaiko asmens duomenų apsaugos reikalavimų ir slapukus interneto svetainėse naudoja neteisėtai, t. y. be vartotojų sutikimo ir nepateikdama svarbiausios informacijos apie jų tvarkymą privatumo politikoje.
4. Atlikus 9 ekspertų nuomonės vertinimą nustatyta, kad:

4.1. Kibernetinis saugumas yra neatsiejamas nuo asmens duomenų apsaugos, nes daugelis asmens duomenų apsaugą užtikrinančių priemonių yra kibernetinio saugumo organizacinės ir techninės priemonės.
4.2. Organizacijos nenorą investuoti į asmens duomenų apsaugą ir kibernetinį saugumą gali lemti kelios priežastys – nėra žinoma (sunkiai pamatuojama) investicijų grąža, galimas darbo produktyvumo sumažėjimas ir tolerancija rizikoms bei požiūris į jas, kad jos nesumažės.
4.3. Organizacijos prioritetą dažnu atveju teikia techninėms, o ne organizacinėms priemonėms, nes technines priemones galima nupirkti ir parodyti, o organizacinės sunkiau įgyvendinamos ir kontroliuojamos.

3-iasis uždavinys. Pasiūlius asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį, galima teigti:

1. Siūlomo asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį sudaro dvi dimensijos – asmens duomenų apsaugos ir kibernetinio saugumo, kuriose nurodytos 16 priemonių, siekiant užtikrinti asmens duomenų apsaugą organizacijoje. Kibernetinio saugumo dimensija yra asmens duomenų apsaugos dimensijos dalis.
2. Asmens duomenų apsaugos dimensija užtikrina teisėtą asmens duomenų tvarkymą ir atitinkamas technines ir organizacines priemones, siekiant apsaugoti pagrindines duomenų subjekto teises ir laisves, visų pirma jų teisę į asmens duomenų apsaugą.
3. Kibernetinio saugumo dimensija užtikrina kibernetinio saugumo valdymą ir atitinkamas technines ir organizacines priemones, siekiant apsaugoti informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumą, vientisumą bei konfidencialumą.
4. Siūlomas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, suteikia organizacijai galimybę stebėti asmens duomenų apsaugos ir kibernetinio saugumo įgyvendinimo pokyčius pagal priemonių laipsnišką įgyvendinimą, lygiais – supratimo (I), įgyvendinimo (II), užtikrinimo/ tobulinimo (III) ir integruotąjį (IV), konkrečiose dimensijose.

4-asis uždavinys. Įvertinus asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkius ir galimybes, nustatyta:

1. Neužtikrinus kibernetinio saugumo kyla rizika įvykti asmens duomenų saugumo pažeidimui, nes asmens duomenys gali būti atskleisti, prarasti ir neprieinami. Tačiau net ir užtikrinus kibernetinį saugumą vis dar kyla rizika įvykti asmens duomenų saugumo pažeidimui, nes asmens duomenys gali būti tvarkomi pažeidžiant pagrindinius asmens duomenų tvarkymo principus. Tik užtikrinus modelyje nurodytas asmens duomenų apsaugos ir kibernetinio saugumo priemones galima užtikrinti asmens duomenų apsaugą, siekiant sumažinti kibernetinių incidentų ir asmens duomenų apsaugos pažeidimų riziką.
2. Įgyvendinant asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį organizacijos gali susidurti su iššūkiais – kompetencijos ir patirties trūkumu, žmogiškųjų išteklių trūkumu, finansinių išteklių trūkumu,

komunikacijos ir bendradarbiavimo trūkumu, motyvacijos trūkumu ir pasipriešinimu pokyčiams.

3. Kiekviena asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio priemonė gali būti įgyvendinama atskirai, neišskiriant vienos pačios svarbiausios priemonės, atsižvelgiant į organizacijos veiklos ypatumus, valdomus išteklius, turimus resursus bei finansines galimybes. Tačiau asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio IV lygmuo yra siejamas su visų asmens duomenų apsaugos ir kibernetinio saugumo dimensijose išvardintų priemonių įgyvendinimu, siekiant virsmo į integruotą asmens duomenų apsaugos ir kibernetinio saugumo valdymo sistemą, kurioje priemonės yra susietos bei veiks viena kitą papildydamos.

REKOMENDACIJOS

Organizacijoms:

1. Rekomenduojama anonimizuoti ir pseudonimizuoti asmens duomenis siekiant palengvinti asmens duomenų apsaugos reikalavimų įgyvendinimą ir apsaugoti atskirų duomenų subjektų teises į privatumą.
2. Siekiant užtikrinti asmens duomenų subjektų įgyvendinimą, visų pirma glausta ir lengvai suprantama kalba informuoti duomenų subjektus apie jų teises, visų antra sukurti mechanizmus ir procedūras joms įgyvendinti.
3. Rekomenduojama duomenų valdytojui ir (ar) tvarkytojui bendradarbiauti su duomenų apsaugos pareigūnu – kuo ankstyvesniu etapu įtraukti į visus su duomenų apsauga susijusius klausimus ir suteikti reikiamus išteklius atlikti užduotis bei tobulėti. Tuo tarpu duomenų apsaugos pareigūnui atsižvelgiant į organizacijos asmens duomenų pobūdį, aprėptį, kontekstą ir tikslus privaloma įvertinti asmens duomenų tvarkymo rizikas ir informuoti duomenų valdytoją ir (ar) tvarkytoją bei konsultuotis su priežiūros institucija.
4. Siekiant įgyvendinti asmens duomenų apsaugos priemones, kurias taip pat sudaro ir kibernetinio saugumo priemonės, privaloma įsivertinti kokios priemonės yra tinkamos, priklausomai nuo duomenų jautrumo ir rizikos laipsnio, jei asmens duomenys bus pažeisti.
5. Siekiant užtikrinti asmens duomenų apsaugą privaloma įgyvendinti ne tik teisės aktuose nustatytas kibernetinio saugumo technines ir organizacines priemones, bet ir pagrindinius asmens duomenų tvarkymo principus bei gerąją praktiką įtvirtintą standartuose ISO 27001 ir ISO 27002 bei Valstybinės duomenų apsaugos inspekcijos tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėse.
6. Siekiant teisėtai tvarkyti duomenis - slapukus interneto svetainėse, duomenų valdytojas ir (ar) tvarkytojas privalo turėti tinkamą įrankį, kuris vartotojams suteiktų galimybę aktyviais veiksmais sutikti arba nesutikti su atitinkamų slapukų tvarkymu bei bet kada pakeisti apsisprendimą, taip pat pateikti visą informaciją apie slapukų tvarkymą interneto svetainės privatumo politikoje.
7. Rekomenduojama tobulinant veiklos procesus asmens duomenų apsaugos kontekste mąstyti ne apie patogumą, bet apie saugumą vadovaujantis teisės aktais ir visuotinai pripažinta gerąją praktika nustatyta tarptautiniuose standartuose.
8. Techninės priemonės tinkamai neveiks be organizacinių priemonių, todėl privalu ieškoti balanso tarp abiejų priemonių įgyvendinimo.

Vartotojams (duomenų subjektams):

1. Rekomenduojama domėtis kaip organizacijos tvarko jų asmens duomenis ir reikalauti įgyvendinti jų teises asmens duomenų kontekste.
2. Rekomenduojama informuoti priežiūros institucijas – Valstybinę duomenų inspekciją, jeigu įvyko asmens duomenų saugumo pažeidimas ir Nacionalinį kibernetinio saugumo centrą, jeigu įvyko kibernetinis incidentas.

Tolesni tyrimai disertacijos tematika galėtų būti vykdomi:

1. Siekiant įvertinti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio pritaikomumą, gali būti pasitelkti asmens duomenų apsaugos ir kibernetinio saugumo ekspertai.
2. Atskleisti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio priemonių sąryšius t. y. kaip vienos priemonės įgyvendinimas įtakoja kitą.
3. Remiantis moksliniais tyrimais tobulinti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelyje išvardintas priemones arba papildyti naujomis.

LITERATŪRA

Teisės aktai

1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB, <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016R0679>.
2. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399/asr>.
3. Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašas, patvirtintas Valstybinė duomenų apsaugos inspekcijos direktoriaus įsakymu 2018 m. d. Nr. 1T- (1.12.E) „Dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“, < https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/97401a305fda11e896f6c1bcca8cd3a8>
4. Lietuvos Respublikos kibernetinio saugumo įstatymas, Nr. XII-1428, 2014 m. gruodžio 11 d., Vilnius, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr>.
5. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, XI-1807, 2011 m. gruodžio 15 d., Vilnius, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415499/asr>.
6. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, Nr. XI-1807, 2011 m. gruodžio 15 d., Vilnius, < https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415499/asr>.
7. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr>.
8. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/117a33f038cb11eb8c97e01ffe050e1c?jfwid=-1bn3bs0lop>.

Mokslinės literatūros šaltiniai

9. Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of economic Literature*, *54*(2), 442-92.

10. Addis, C., & Kutar, M. S. (2018, March). The general data protection regulation (GDPR), emerging technologies and UK organisations: awareness, implementation and readiness. In *UK Academy for Information Systems Conference Proceedings 2018* (p. 29). UKAIS–UK Academy for Information Systems.
11. Agafonov, K. (2021). *Kibernetinio saugumo valdymo modelis elektroniniams rinkimams įgyvendinti* (Doctoral dissertation, Mykolo Romerio universitetas).
12. Aiken. G. M. (2019). Cybersecurity and productivity: has a cybersecurity culture gone too far?" *ASBBS Proceedings*, 26(2), 13-22.
13. Albanese, M., Cam, H., & Jajodia, S. (2014). Automated cyber situation awareness tools and models for improving analyst performance. In *Cybersecurity systems for human cognition augmentation* (pp. 47-60). Springer, Cham.
14. Aldawood, H., Alashoor, T., & Skinner, G. (2020). 'Does awareness of social engineering make employees more secure? *International Journal of Computer Applications*, 975, 8887.
15. Alford, S. (2020). *GDPR: a Game of Snakes and Ladders*. Routledge.
16. Alghamdi, M. I. (2021). Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. *Materials Today: Proceedings*.
17. Alhazmi, O. H., & Malaiya, Y. K. (2013, January). Evaluating disaster recovery plans using the cloud. In *2013 proceedings annual reliability and maintainability symposium (rams)* (pp. 1-6). IEEE.
18. Aliyeva, L. M., & Hwang, G. H. (2019). The Model to Implement the Cyber Security Policy and Strategy for Azerbaijan Information System. *Journal of digital convergence*, *17*(5), 23-31.
19. Alkhaledi, R., & Hawamdeh, S. (2020). Cybersecurity Challenges and Implications for the Information Profession. *Cybersecurity for Information Professionals: Concepts and Applications*.
20. Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Structuring the Chief Information Security Officer Organization. Carnegie Mellon University <https://apps.dtic.mil/sti/pdfs/AD1046633.pdf>.
21. Allison, M., & Kaye, J. (2011). *Strategic planning for nonprofit organizations: A practical guide and workbook*. John Wiley & Sons.
22. Almousa, M., Keshavarz, M., & Anwar, M. (2020). Awareness and Working Knowledge of Secure Design Principles: A User Study. In *International Conference on Human-Computer Interaction* (pp. 3-15). Springer, Cham.
23. Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, 124(1), 691–697
24. Al-Sartawi, A. M. M. (2020). Information technology governance and cybersecurity at the board level. *International Journal of Critical Infrastructures*, *16*(2), 150-161.
25. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851-1877.
26. Andress, J. (2011). The basics of information security: understanding the fundamentals of infosec in theory and practice. New York: Elsevier.
27. Andrijauskas, R., Morkūnienė, D. (2020). Asmens duomenų apsaugos priežiūros institucijos vaidmens pasikeitimai priėmus bendrąjį duomenų apsaugos reglamentą. *Jurisprudencija*, 27(2), 298-311.
28. Aoyama, T., Naruoka, H., Koshijima, I., & Watanabe, K. (2015). How management goes

wrong?–The human factor lessons learned from a cyber incident handling exercise. *Procedia Manufacturing*, *3*, 1082-1087.
29. Aoyama, T., Naruoka, H., Koshijima, I., Machii, W., & Seki, K. (2015, May). Studying resilient cyber incident management from large-scale cyber security training. In *2015 10th Asian Control Conference (ASCC)* (pp. 1-4). IEEE.
30. Arimavičiūtė, M. (2005). *Viešojo sektoriaus institucijų strateginis valdymas*. Vilnius: Mykolo Romerio universitetas.
31. Asquith, P. M., & Morgan, P. L. (2020). Representing a human-centric cyberspace. In *International Conference on Applied Human Factors and Ergonomics* (pp. 122-128). Springer, Cham.
32. Atamli, A. W., Martin. A. (2014). Threat-Based Security Analysis for the Internet of Things. In 2014 *International Workshop on Secure Internet of Things*. 35–43. https://doi.org/10.1109/SIoT.2014.10
33. Augenbaum, E., S. (2019). *The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime*. Forefront Books
34. Augustinaitis A.; Rudzkienė V.; Petrauskas R. A.; Dagytė I.; Martynaitytė E.; Leichteris E.; Malinauskienė E.; Višnevska V.; Žilionienė I. (2009). *Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas, kolektyvinė monografija*, Mykolo Romerio universitetas.
35. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1-13.
36. Awesta, A. G. (2021). European Laws' Effectiveness in Protecting Personal Data. In *Data Protection Around the World* (pp. 249-267). TMC Asser Press, The Hague.
37. Axinte, S. D., Petrică, G., & Bacivarov, I. (2018). GDPR Impact on Company Management and Processed Data. *Calitatea*, *19*(165), 150-153.
38. Ayala-Rivera, V., & Pasquale, L. (2018, August). The grace period has ended: An approach to operationalize GDPR requirements. In *2018 IEEE 26th International Requirements Engineering Conference (RE)* (pp. 136-146). IEEE.
39. Babbie, E.R. (2005). *The Basics of Social Research*. Thomson Wadsworth
40. Baig, M. M. A. (2022). Potential Challenges of Developing Large-Scale Computing Infrastructures over Distributed Clouds. *Mathematical Statistician and Engineering Applications*, *71*(4), 122-145.
41. Bailey, K. (2008). *Methods of social research*. Simon and Schuster.
42. Bamberger, K., Mulligan, D. (2015) Privacy on the Ground: Driving Corporate Behaviour in United States and Europe
43. Banga, G. (2020). Why is cybersecurity not a human-scale problem anymore?. *Communications of the ACM*, 63(4), 30-34.
44. Barnard-Wills, D., Marchetti, F., Böröcz, I., & Kulitsán, G. (2019). Journal article–What does good data protection training look like? The state of the art and requirements for GDPR training. Vrije Universiteit Brussel
45. Batutytė, I. (2019). *Ar asmens duomenys, kurie yra nuasmeninami, tačiau naudojami tiesioginės rinkodaros tikslais, papuola į naujojo ES BDAR reguliavimo sritį?* Kaunas: Vytauto Didžiojo universitetas.
46. Baumeister, R.F., Vohs, K.D. (2016) Chapter two - strength model of self-regulation as limited resource: assessment, controversies, update. In: Olson, J.M., Zanna, M.P. (eds.) Advances in Experimental Social Psychology, pp. 67–127. Academic Press, Cambridge
47. Bayne, J. S. (2008). Cyberspatial mechanics. *IEEE Transactions on Systems, Man, and Cybernetics*, Part B (Cybernetics), 38(3), 629-644.

48. Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber security policy guidebook*. John Wiley & Sons.
49. Bertoglio, D. D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, *23*(1), 1-16.
50. Bishop, L. M., Morgan, P. L., Asquith, P. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020). Examining human individual differences in cyber security and possible implications for human-machine interface design. In *International Conference on Human-Computer Interaction* (pp. 51-66). Springer, Cham.
51. Bitinas, B. (2016). Rinktiniai edukologiniai rašta, <gs.elaba.lt/object/elaba:4358642/4358642.pdf>.
52. Bitinas, B., Rupšienė, L., & Žydžiūnaitė, V. (2008). *Kokybinių tyrimų metodologija: Vadovėlis vadybos ir administravimo studentams*. Klaipėda: Ofsetinė spauda
53. Black, L., Scala, N. M., Goethals, P. L., & Howard II, J. P. (2018). Values and trends in cybersecurity. In *IIE Annual Conference. Proceedings* (pp. 2009-2014). Institute of Industrial and Systems Engineers (IISE).
54. Blaikie, N. (2007). Approaches to social enquiry: Advancing knowledge. Polity
55. Blanco-Lainé, G., Sottet, J. S., & Dupuy-Chessa, S. (2019, November). Using an enterprise architecture model for GDPR compliance principles. In IFIP Working Conference on The Practice of Enterprise Modeling (pp. 199-214). Springer, Cham.
56. Blau, A. (2017). The behavioral economics of why executives underinvest in cybersecurity. *Harvard Business Review*.
57. Blum, D. (2020). *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment* (p. 333). Springer Nature.
58. Bock, K., Kühne, C. R., Mühlhoff, R., Ost, M. R., Pohle, J., & Rehak, R. (2021). Data protection impact assessment for the corona app. arXiv preprint arXiv:2101.07292.
59. Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527-544.
60. Boies, K., Fiset, J., & Gill, H. (2015). Communication and trust are key: Unlocking the relationship between leadership and team performance and creativity. *The leadership quarterly,* 26(6), 1080-1094.
61. Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*.
62. Bryman, A. (2008). *Social Research Methods* (3rd ed.). Oxford: Oxford University Press.
63. Bryman, A., Bell, E. (2007). *Business Research Methods*. 2nd edition, Oxford University Press.
64. Bryson, J. M. (2018). *Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement*. John Wiley & Sons.
65. Buccafurri, F., Fotia, L., Furfaro, A., Garro, A., Giacalone, M., & Tundis, A. (2015, September). An analytical processing approach to supporting cyber security compliance assessment. In *Proceedings of the 8th International Conference on Security of Information and Networks* (pp. 46-53).
66. Buckley, R., & Caple, J. (2009). *The theory and practice of training*. Kogan Page Publishers.
67. Buene, K. F., & Fridtun, H. T. (2022). *Investigating trust relationships between software development teams and information security stakeholders* (Master's thesis, NTNU).
68. Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, 75, 24-35.

69. Cabral, T. S. (2021). AI and the Right to Explanation: Three Legal Bases under the GDPR. *Data Protection and Privacy: Data Protection and Artificial Intelligence*, 29.
70. Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643-1669.
71. Carey, P. (2018). *Data protection: a practical guide to UK and EU law*. Oxford University Press, Inc.
72. Cerullo, V., & Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. *Information systems management*, 21(3), 70-78.
73. Chang, H. C., Jim, C., & Hawamdeh, S. (2020). Bridging the Cybersecurity Talent Gap: Cybersecurity Education in iSchools. *Cybersecurity for Information Professionals: Concepts and Applications*.
74. Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons.
75. Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. *ecancermedicalscience*, (*11)709.*
76. Cheng, S., Zhao, G., Gao, M., Shi, Y., Huang, M., & Marefati, M. (2021). A new hybrid solar photovoltaic/phosphoric acid fuel cell and energy storage system; Energy and Exergy performance. *International Journal of Hydrogen Energy*, *46*(11), 8048-8066.
77. Cherdantseva, Y., Hilton, J. (2013). Information Security and Information Assurance. Organizational, Legal, and Technological Dimensions of IS Administrator. IGI Global Publishin.
78. Cheung, S. O., Yiu, T. W., & Lam, M. C. (2013). Interweaving trust and communication with project performance. *Journal of construction engineering and management*, 139(8), 941-950.
79. Chochlova, L. (2022). *Kibernetinio saugumo kultūros plėtra švietimo srityje: ikimokyklinio ir bendrojo ugdymo įstaigų programų pagrindu* (Magistro darbas, Mykolo Romerio universitetas).
80. Choong, Y. Y., & Theofanos, M. (2015, August). What 4,500+ people can tell you–employees' attitudes toward organizational password policy do matter. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 299-310). Springer, Cham.
81. Choong, Y. Y., & Theofanos, M. (2015, August). What 4,500+ people can tell you–employees' attitudes toward organizational password policy do matter. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 299-310). Springer, Cham.
82. Chowdhury, N.H., Adam, N.T.P., Skinner, G. (2019) The impact of time pressure on cybersecurity behaviour: a systematic review. *Behav. Inf. Technol*. 38(12), 1290–1308
83. Čižikienė, J. (2020). Vadovų lyderystė pasirenkant diegti Europos socialinių paslaugų kokybės užtikrinimo sistemą (Doctoral dissertation, Mykolo Romerio universitetas).
84. Coffey A. (2014). The SAGE Handbook of Qualitative Data Analysis. SAGE Publications Ltd, London
85. Coleman, J. S. (2005). *Socialinės teorijos pagrindai*. Vilnius: Margi raštai.
86. Corbetta P. (2003). Social Research : Theory, Methods and Techniques. SAGE Publications.
87. Corbin, J., Strauss, A. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory (3rd ed.). Thousand Oaks, CA: Sage.

88. Corradini, I. (2020). *Building a Cybersecurity Culture in Organizations*. Springer International Publishing.
89. Corradini, I., & Nardelli, E. (2018, July). Building organizational risk culture in cyber security: the role of human factors. In *International Conference on Applied Human Factors and Ergonomics* (pp. 193-202). Springer, Cham.
90. Corradini, I., & Nardelli, E. (2020, July). Developing digital awareness at school: a fundamental step for cybersecurity education. In *International Conference on Applied Human Factors and Ergonomics* (pp. 102-110). Springer, Cham.
91. Corradini, I., & Nardelli, E. (2020, July). Is Data Protection a Relevant Indicator for Measuring Corporate Reputation?. In *International Conference on Applied Human Factors and Ergonomics* (pp. 135-140). Springer, Cham.
92. Cortez, E. K. (2021). Data Protection Around the World: Future Challenges. In *Data Protection Around the World* (pp. 269-279). TMC Asser Press, The Hague.
93. Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020, July). Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In *International Conference on Human-Computer Interaction* (pp. 105-122). Springer, Cham.
94. Creswell, J. W. (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. Thousand Oaks, CA: Sage.
95. Crockett, K., Goltz, S., & Garratt, M. (2018, July). GDPR impact on computational intelligence research. In *2018 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-7). IEEE.
96. Da Conceicao Freitas. M., Silva M. (2018) GDPR compliance in SME's: There is much to be done, Journal of Information Systems Engineering and Management
97. Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019). Measuring cookies and web privacy in a post-gdpr world. In *International Conference on Passive and Active Network Measurement* (pp. 258-270). Springer, Cham.
98. Daigle, B., & Khan, M. (2020). The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities. *J. Int'l Com. & Econ.,* 1.
99. Daimi, K., & Francia III, G. (2020). *Innovations in Cybersecurity Education*. Springer International Publishing AG.
100. Dalalana Bertoglio, D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, *23*(1), 1-16.
101. Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination. *Proceedings on privacy enhancing technologies*, *2015*(1), 92-112.
102. Daukšytė, D., & Lazauskaitė-Zabielskė, J. (2016). Darbuotojų pasitenkinimas veiklos vertinimu: suvokto veiklos vertinimo teisingumo ir veiklos vertinimo ypatumų empirinė analizė. *Organizacijų vadyba: sisteminiai tyrimai*, (76), 25-42.
103. de Moura, R. L., Gonzalez, A., Franqueira, V. N., & Neto, A. L. M. (2020, December). A cyber-security strategy for internationally-dispersed industrial networks. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 62-68). IEEE.
104. Dean, B., & McDermott, R. (2017). A research agenda to improve decision making in cyber security policy. *Penn St. JL & Int'l Aff.*, *5*, 29.
105. Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., Holz, T. (2018), "We Value

Your Privacy Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy", *Computers and Society*
106. Demetzou, K. (2018, August). GDPR and the Concept of Risk. In *IFIP International Summer School on Privacy and Identity Management* (pp. 137-154). Springer, Cham.
107. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W. (2011). A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements. Requirements Engineering 16, 1, 3–32. https://doi.org/10.1007/s00766-010-0115-7
108. Dexe, J., Ledendal, J., & Franke, U. (2020, September). An Empirical Investigation of the Right to Explanation Under GDPR in Insurance. In *International Conference on Trust and Privacy in Digital Business* (pp. 125-139). Springer, Cham.
109. Di Martino, M., Robyns, P., Weyts, W., Quax, P., Lamotte, W., & Andries, K. (2019). Personal Information Leakage by Abusing the {GDPR}'Right of Access'. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.
110. Dibble, S. (2019). *GDPR for Dummies*. John Wiley & Sons.
111. Diker Vanberg, A., & Ünver, M. B. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?. *European Journal of Law and Technology*, *8*(1).
112. Dimitrova, D. (2021). The Rise of the Personal Data Quality Principle. Is it Legal and Does it Have an Impact on the Right to Rectification?. *Is it Legal and Does it Have an Impact on the Right to Rectification*.
113. Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*, 102056.
114. Dounis, N. P. (2017). GDPR Regulatory Compliance and the Role of Internal Audit: Theoretical and Practical Approach. *Int'l. In-House Counsel J.*, *11*, 1.
115. Drewer, D., Miladinova, V., (2018) The canary in the data mine, *Computer Law and Security Review* 34, 806-815
116. Eggers, S., & Le Blanc, K. (2021). Survey of cyber risk analysis techniques for use in the nuclear industry. *Progress in Nuclear Energy*, *140*, 103908.
117. E-Governance Academy (2023). National Cyber Security Index. Prieiga per internetą: https://ncsi.ega.ee/
118. Esparza, J., Caporusso, N., & Walters, A. (2020, July). Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools. In *International Conference on Applied Human Factors and Ergonomics* (pp. 88-94). Springer, Cham.
119. Esteves, B., & Rodríguez-Doncel, V. (2021). Analysis of Ontologies and Policy Languages to Represent Information Flows in GDPR. *Semantic Web – Interoperability, Usability, Applicability an IOS Press Journal*
120. Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review*, 58(3), 71e77
121. European Commission. (2016). *Scoping paper: Cyber-Security*. Scientific Advice Mechanism - Research and innovation.
122. Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba; Europos Žmogaus Teisių Teismas (2014) *Europos duomenų apsaugos teisės vadovas*. Liuksemburgas: Europos Sąjungos leidinių biuras.
123. Fani, S. V., & Subriadi, A. P. (2019). Business continuity plan: examining of multi-usable framework. *Procedia Computer Science*, *161*, 275-282.

124. Felici, M., Koulouris, T., Pearson, S. (2013) Accountability for Data Governance in Cloud Ecosystems
125. Fernando, M. S. (2017). IT disaster recovery system to ensure the business continuity of an organization. In *2017 National Information Technology Conference (NITC)* (pp. 46-48). IEEE.
126. Feth, D. (2017) Transparency through contextual privacy statements. In: Burghardt, M., Wimmer, R., Wolff, C., Womser-Hacker, C. (eds.) Mensch und Computer 2017 - Workshopband. Gesellschaft für Informatik e.V, Regensburg
127. Feth, D. (2020, July). Modelling and Presentation of Privacy-Relevant Information for Internet Users. In *International Conference on Human-Computer Interaction* (pp. 354-366). Springer, Cham.
128. Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. *Games*, *9*(2), 34.
129. Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. *Games*, *9*(2), 34.
130. Fitzgerald, T. (2018). C*ISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers*. CRC Press.
131. Flavián, C., Guinalíu, M. (2006), "Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site", Industrial Management & Data Systems, Vol. 106, No 5, pp.601-620.
132. Fletcher, C. (2001). Performance appraisal and management: The developing research agenda. *Journal of Occupational and organizational Psychology*, *74*(4), 473-487.
133. Gaižauskaitė, I., & Valavičienė, N. (2016). *Socialinių tyrimų metodai: kokybinis interviu*. Mykolo Romerio universitetas.
134. Geko, M., & Tjoa, S. (2018). An ontology capturing the interdependence of the general data protection regulation (GDPR) and information security. In *Proceedings of the Central European Cybersecurity Conference 2018* (pp. 1-6).
135. George, B. (2021). Successful strategic plan implementation in public organizations: Connecting people, process, and plan (3Ps). *Public Administration Review*, *81*(4), 793-798.
136. Georghiou, L., Edler, J., Uyarra, E., & Yeow, J. (2014). Policy instruments for public procurement of innovation: Choice, design and assessment. *Technological Forecasting and Social Change*, 86, 1-12.
137. Ghazouani M., Faris S., Sayouti A. (2014). Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk, *International Journal of Computer Applications*, 103 (8), pp. 36-42.
138. Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *Authorea Preprints*.
139. Gibson, D. (2014). *Managing risk in information systems*. Jones & Bartlett Publishers
140. Gjelsvik, N., & Saga, V. (2019). *Successfully Implementing GDPR in the Norwegian Online Advertising Industry* (Master›s thesis, NTNU).
141. Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L.F., Agarwal, Y. (2016), "How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices", Twelfth Symosium on Usable Privacy and Security, Denver, CO, USA, June 22–24, pp.321-340.
142. Gnatyuk, S., Barchenko, N., Azarenko, O., Tolbatov, A., Obodiak, V., & Tolbatov, V. (2019). Ergonomic Support for Decision-Making Management of the Chief Information Security Officer. *organization*, 1(2), 4.

143. Gobeo, A., Fowler, C., & Buchanan, W. J. (2018). *GDPR and Cyber Security for Business Information Systems*. River Publishers.
144. Goldstein, A. E. & Reiboldt, W. (2004). The multiple roles of low income, minority women in the family and community: A qualitative investigation. The Qualitative Report, 9(2), 241ơ265. http://www.nova.edu/ssss/QR/QR92/goldstein.pdf.
145. Gollmann, D., Herley C., Koenig, V., Pieters, W., Sasse M. A. (2015). SocioTechnical Security Metrics. *Dagstuhl Reports*, 4, https://doi.org/10. 4230/DagRep.4.12.1
146. Grigaitytė, U., & Mackevičiūtė, M. (2020). Nusikaltimai virtualioje erdvėje–šiuolaikiniai Iššūkiai ir prevencijos galimybės. *Vilnius University Open Series*, (4), 274-294.
147. Grincevičius, R. (2019). Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose (Doctoral dissertation, Mykolo Romerio universitetas).
148. Grütter, B., & Schneider, B. (2019). Data protection impact assessment guidelines in the context of the general data protection regulation. In *Thriving on Future Education, Industry, Business and Society; Proceedings of the MakeLearn and TIIM International Conference* (pp. 261-270). ToKnowPress.
149. Gutfleisch, M., Schöps, M., Hielscher, J., Cheney, M., Sayin, S., Schuhmacher, N., ... & Sasse, M. A. (2022, September). Caring About IoT-Security–An Interview Study in the Healthcare Sector. In *Proceedings of the 2022 European Symposium on Usable Security* (pp. 202-215).
150. Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review*, *71*(3), 455-460.
151. Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K.G., Aberer, K. (2018), "Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning", USENIX Security Symposium, August
152. Hasib, M. (2014). *Cybersecurity Leadership: Powering the Modern Organization*. Tomorrow's Strategy Today, LLC.
153. Heeks, R., & Stanforth, C. (2015). Technological change in developing countries: opening the black box of process using actor–network theory. *Development Studies Research*, 2(1), 33-50.
154. Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, *3*, 1117-1124.
155. Hintze, M., & El Emam, K. (2018). Comparing the benefits of pseudonymisation and anonymisation under the GDPR. *Journal of Data Protection & Privacy*, 2(2), 145-158.
156. Ho, S. M. (2020) Trustworthiness: Top Qualification for Cyber Information Professionals. *Cybersecurity for Information Professionals: Concepts and Applications*.
157. Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585-591.
158. Horák, M., Stupka, V., & Husák, M. (2019). GDPR compliance in cybersecurity software: a case study of DPIA in information sharing platform. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-8).
159. Hunt, E. F., Colander, D. C. (2008). *Social Science: An Introduction to the Study of Society*. Boston: Peason/Allyn and Bacon
160. Huth, D., & Matthes, F. (2020). *ProPerData-A process model to support GDPR compliance*. Technical Report March, Technical University of Munich, Munich.
161. International Telecommunication Union Telecommunication Standardization Sector) Recommendation X.1205 [Overview of Cybersecurity, 2014

162. ISACA (2017). CSX Cybersecurity Fundamentals Study Guide. Prieiga per internetą: https://www.isaca.org/bookstore/csx-certificate-exam-resources/wcsxg2
163. J. G. Cabañas, Á. Cuevas, R. Cuevas, "Facebook Use of Sensitive Data for Advertising in Europe", Social and Information Networks. Accessed 18 July, 2020. Prieiga per internet: https://arxiv.org/abs/1802.05030
164. Januševičienė, J. (2018). Praktiniai asmens sveikatos duomenų tvarkymo aspektai pagal Bendrąjį asmens duomenų apsaugos reglamentą. *Teisė*, (107), 111-128.
165. Jasmontaite, L., & Burloiu, V. P. (2017). Lithuania and Romania to introduce cybersecurity laws. In *Privacy, Data Protection and Cybersecurity in Europe* (pp. 131-145). Springer, Cham.
166. Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R., & Barnard-Wills, D. (2021). The GDPR made simple (r) for SMEs.
167. Jastiuginas, S. (2012). Integralus informacijos saugumo valdymo modelis. Informacijos mokslai, 61, 7–30.
168. Jinhua, L., Xu, H., Zhou, X., Lin, F., & An, J. (2013, November). Research of cyberspace architecture. In *International Conference on Cyberspace Technology* (CCT 2013) (pp. 367-369). IET.
169. Johns, E. (2020). Cyber security breaches survey 2020. *London: Department for Digital, Culture, Media & Sport*.
170. Judge, T. A., & Ferris, G. R. (1993). Social context of performance evaluation decisions. *Academy of management journal*, *36*(1), 80-105.
171. Kademi, A. M. A., & Koltuksuz, A. (2017, June). Formal characterization of cyberspace for cyber lexicon development. In *ECCWS 2017 16th European Conference on Cyber Warfare and Security* (p. 200). Academic Conferences and publishing limited.
172. Kahyaoglu, S. B., & Caliyurt, K. (2018). Managerial Auditing Journa. *Managerial Auditing Journal*, 33(4), 360-376.
173. Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1-34.
174. Kamleitner, B., & Mitchell, V. W. (2018). Can consumers experience ownership for their personal data? From issues of scope and invisibility to agents handling our digital blueprints. In J. Peck & S. Shu (Eds.), *Psychological ownership and consumer behavior* (pp. 91–118). Cham: Springer
175. Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security*. 25(3), 300-329.
176. Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management*, *26*(2), 23-47.
177. Kardelis, K. (2017). *Mokslinių tyrimų metodologija ir metodai*. Mokslo ir enciklopedijų leidybos centras
178. Kaselis, M., & Pivoras, S. (2012). Valstybės tarnautojų veiklos vertinimas pagal rezultatus: taikymo iššūkiai Lietuvoje. *Public policy and administration*, *11*(1), 139-152.
179. King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology*, *9*, 39.
180. Klupšas, F. (2006). Darbuotojų veiklos vertinimo aktualijos. *Lietuvos žemės ūkio akademija*.
181. Kolev, B., & Ivanov, I. (2009). Fault tree analysis in an intuitionistic fuzzy configuration management database. *Notes on Intuitionistic Fuzzy Sets*, *15*(2), 10-17.

182. Koski, H., & Valmari, N. (2020). *Short-term Impacts of the GDPR on Firm Performance* (No. 77). ETLA Working Papers.
183. Kothari, S., Santhanam, G. R., Awadhutkar, P., Holland, B., Mathews, J., & Tamrawi, A. (2018). Catastrophic Cyber-Physical Malware. In *Versatile Cybersecurity* (pp. 201-255). Springer, Cham.
184. Kott, A. (2014). Towards fundamental science of cyber security. In *Network science and cybersecurity* (pp. 1-13). Springer, New York, NY.
185. Kovács, L. (2018). Cyber security policy and strategy in the European Union and NATO. *Land Forces Academy Review*, *23*(1), 16-24.
186. Kurniullah, A. Z., Kulkarni, A., Nordin, N. A., Setiawan, R., Bagale, G., Barman, R. D., ... & Rajest, S. S. (2020). *Positive Outcomes of Human Resources Engagement and Impact on Motivation* (Doctoral dissertation, Petra Christian University).
187. Kuzminykh, I., Ghita, B., & Such, J. M. (2020). The Challenges with Internet of Things for business. *arXiv preprint arXiv:2012.03589*.
188. Kvieskienė, G., & Kvieska, V. (2018). Personalizuoto ugdymosi inovacijos ir sumanioji komunikacija. *Socialinis ugdymas: mokslo darbai. Vilnius: Lietuvos edukologijos universitetas, 2018, t. 48, nr. 1*.
189. Kyriaki Athanassouli (2019) Economic Implications of the Rise of Information Warfare, Cyber-War and Cyber-Security
190. Labuschagne, A. (2003). Qualitative research: Airy fairy or fundamental? The Qualitative Report, 8(1), Article 7. <from http://www.nova.edu/ssss/QR/QR8 1/labuschagne.html>.
191. Lambert, P. (2017). *Understanding the new European data protection rules*. CRC Press.
192. Lapoule, P.; Lynch, R. (2018). The case study method: exploring the link between teaching and research. *Journal of Higher Education Policy & Management*, 40(5): 485-500. https://doi.org/10.1080/1360080X.2018.1496515
193. Leaning, M., & Averweg, U. R. (2019). Developing the Social, Political, Economic, and Criminological Awareness of Cybersecurity Experts: A Proposal and Discussion of Non-Technical Topics for Inclusion in *Cybersecurity Education. In Global Cyber Security Labor Shortage and International Business Risk* (pp. 77-93). IGI Global.
194. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671.
195. Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security*, *108*, 102376.
196. Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2020). GDPR compliance in the context of continuous integration. *arXiv preprint arXiv:2002.06830*.
197. Limba, T., Driaunys, K., Kiškis, M., Šidlauskas, A. (2020). Development of Digital Contents: Privacy Policy Model under the General Data Protection Regulation and User Friendly Interface, *Transformations in Business & Economics,* 1(49), 21-42.
198. Limba, T.; Driaunys, M.; Šidlauskas, A. 2021. Use of Cookies After GDPR: a Case Study of Top Lithuanian Websites, *Transformations in Business & Economics,* Vol. 20, No. 3 (54): 93-116.
199. Limba, T.; Šidlauskas, A. 2020. Personal Data Processing in Educational Institutions: Anonymisation and Pseudonymisation. *ICERI20: 13th annual International Conference of Education, Research and Innovation*, 9th - 10th of November, 2020, pp. 9989-9997.
200. Lin, C. P., Chiu, C. K., & Liu, N. T. (2019). Developing virtual team performance: an integrated perspective of social exchange and social cognitive theories. *Review of Managerial Science*, *13*(4), 671-688.

201. Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2018). The privacy policy landscape after the GDPR. *arXiv preprint arXiv:1809.08396*.
202. Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. C. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE access*, *6*, 12103-12117.
203. Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Business*.
204. Longley, A. (2019). Understanding and managing cyber security threats and countermeasures in the process industries. *Loss Prevention Bulletin*, (268).
205. Lu, T., Zhao, J., Zhao, L., Li, Y., & Zhang, X. (2015). Towards a Framework for Assuring Cyber Physical System Security. *International Journal of Security and Its Applications*, 9(3), 25-40.
206. Lubua, E. W., & Maharaj, M. (2012). ICT Policy and e-Transparency in Tanzania. *IST-Africa Conference Proceedings* (pp. 1-10). Dar Es Salaam: IST-Africa.
207. Lubua, E. W., & Pretorius, P. D. (2019, July). Cyber-security policy framework and procedural compliance in public organisations. In *Proceedings of the International Conference on Industrial Engineering and Operations Management* (pp. 1-13).
208. Lukoševičienė, D. (2021). *Asmens duomenų apsaugos įgyvendinimo problemos sveikatos priežiūros įstaigose*. Magistro darbas, Mykolo Romerio universitetas.
209. Mackie, J., Taramonli, C., & Bird, R. (2017). Digital forensics and the GDPR: examining corporate readiness. In *European conference on cyber warfare and security* (pp. 683-691). Academic Conferences International Limited.
210. Madduri, H., Shi, S. S., Baker, R., Ayachitula, N., Shwartz, L., Surendra, M., ... & Patel, S. (2007). A configuration management database architecture in support of IBM Service Management. *IBM Systems Journal*, *46*(3), 441-457.
211. Makhija, A. K. (2021) Information Security Management Systems-Evolving Landscape & ISO 27001: An Empirical Study. *Journal of Accounting, Finance, Economics, and Social Sciences*, Vol. 6, No.1, pp.19-27, 19.
212. Maleka, S. (2014). Strategy management and strategic planning process. *DTPS strategic planning & monitoring*, *1*(1), 1-29.
213. Malinauskaitė-van de Castel, I. (2017). *Duomenų subjekto teisės virtualiuose socialiniuose tinkluose* (Doctoral dissertation, Mykolo Romerio universitetas).
214. Mandritsa, I. V., Peleshenko, V. I., Mandritsa, O. V., Fensel, A., Tebueva, F. B., Petrenko, V. I., ... & Mecella, M. (2018). Defining a cybersecurity strategy of an organization: criteria, objectives and functions. In *В сборнике: Integrating Research Agendas and Devising Joint Challenges. International Multidisciplinary Symposium ICT Research in Russian Federation and Europe* (pp. 199-205).
215. Mangini, V., Tal, I., & Moldovan, A. N. (2020). An empirical study on the impact of GDPR and right to be forgotten-organisations and users perspective. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-9).
216. Maurer, C., Kim, K., Kim, D., & Kappelman, L. A. (2021). Cybersecurity: is it worse than we think?. *Communications of the ACM*, *64*(2), 28-30.
217. Meištaitė, E. (2021). Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimas (Doctoral dissertation, Kauno technologijos universitetas).
218. Meištaitė, E. (2021). *Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimas* (Magistro darbas, Kauno technologijos universitetas).

219. Melnikova, J. (2008). Vadovavimas bendrojo lavinimo mokyklai: optimizavimo aspektas. *Vadyba*, (2), 99-106.
220. Menard, P., Bott, G. J., Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self Determination Theory. *Journal of Management Information Systems* 34, 4 (Oct. 2017), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083
221. Mensah, R. O. (2019). Sociological analysis of police training practices in Ghana: Theoretical and conceptual schools of thought. *Research on Humanities and Social Sciences*, 9(12): 113–122.
222. Merriam, S. B. (2009). Qualitative Research – A Guide to Design and Implementation. United States of Amerika.
223. Messeni Petruzzelli, A., Natalicchio, A., Panniello, U., Roma, P. (2019). Understanding the crowdfunding phenomenon and its implications for sustainability. *Technological Forecasting and Social Change*, Vol. 141, p. 138–148.
224. Möller, D. P. (2020). *Cybersecurity in Digital Transformation: Scope and Applications*. Springer Nature.
225. Möller, D. P., & Haas, R. E. (2019). *Guide to Automotive Connectivity and Cybersecurity*. Springer International Publishing.
226. Morgan, P. L., Asquith, P. M., Bishop, L. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020, July). A New Hope: Human-Centric Cybersecurity Research Embedded Within Organizations. In International Conference on Human-Computer Interaction (pp. 206-216). Springer, Cham.
227. Mouratidis, H., Argyropoulos, N., & Shei, S. (2016). Security requirements engineering for cloud computing: The secure tropos approach. In *Domain-specific conceptual modeling* (pp. 357-380). Springer, Cham.
228. Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., ... & Kaye, J. (2018). Are 'pseudonymised'data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, *34*(2), 222-233.
229. Mulder, T., & Tudorica, M. (2019). Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law*, 28(3), 261-274.
230. Nagahawatta, R., Warren, M., & Yeoh, W. (2019, January). Ethical Issues Relating to Cyber Security in Australian SMEs. In *Proceedings of the 8th Australian Institute Of Computer Ethics Conference (AICE 2019)* (pp. 71-76). Deakin University.
231. Nigam, N., Mbarek, S., Benetti, C. (2018). Crowdfunding to finance eco-innovation: case studies from leading renewable energy platforms. *Journal of Innovation Economics & Management*, Vol. 26(2), p. 195–219.
232. Nikolovski, S., & Mitrevski, P. (2022, June). On the Requirements for Successful Business Continuity in the Context of Disaster Recovery. In *2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)* (pp. 1-4). IEEE.
233. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).
234. Novikovienė, L., & Pedaniuk, O. (2020). Naujosios duomenų subjekto teisės bendrajame duomenų apsaugos reglamente. *Jurisprudencija*, *27*(2), 312-329.
235. Nowduri, S. (2018). Critical Thinking Skills and Best Practices for Cyber Security. *International Journal of Cyber-Security and Digital Forensics*, 7(4), 391-410.

236. Obar, J.A., Oeldorf-Hirsch, A. (2016) The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. In: The 44th Research Conference on Communication, Information and Internet Policy
237. Ortas, E., Burritt, R. L., Moneva, J. M. (2013). Socially responsible investment and cleaner production in the Asia Pacific: Does it pay to be good? *Journal of Cleaner Production*, Vol. 52, p. 272–280.
238. Oyelami, J. O., & Kassim, A. M. (2020). Cyber security defence policies: A proposed guidelines for organisations cyber security practices. *International Journal of Advanced Computer Science and Applications*, *11*(8).
239. P. N. Otto and A. I. Anton, "Addressing legal requirements in requirements engineering," *in International Requirements Engineering Conference* (RE), 2007, pp. 5–14.
240. Pandit, H. J., O'Sullivan, D., & Lewis, D. (2019, September). Test-driven approach towards GDPR compliance. In *International Conference on Semantic Systems* (pp. 19-33). Springer, Cham.
241. Parker, L. E. (2018). Creation of the national artificial intelligence research and development strategic plan. *AI Magazine*, *39*(2), 25-32.
242. Parsons, T., & Gerald, M. P. (1973). The American university. Massachussets: Hardvard University Press.
243. Pătrașcu, P. (2019). Promoting Cyber Culture through Education. The International Scientific Conference eLearning and Software for Education, 2, 273-279
244. Patterson, J. (2017). *Cyber-security policy decisions in small businesses* (Doctoral dissertation, Walden University).
245. Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080.
246. Pelenis, P. (2016). *Kibernetinio saugumo užtikrinimo įtaka verslo procesams* (Magistro darbas, Mykolo Romerio universitetas).
247. Peltier, T. R. (2005). *Information security risk analysis*. CRC press.
248. Perry, R. (2019). GDPR–project or permanent reality?. *Computer Fraud & Security*, *2019*(1), 9-11.
249. Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., ... & Zorzino, G. G. (2019, August). DEFeND architecture: a privacy by design platform for GDPR compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 78-93). Springer, Cham.
250. Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), tyy001.
251. Prati, L. M., Douglas, C., Ferris, G. R., Ammeter, A. P., & Buckley, M. R. (2003). Emotional intelligence, leadership effectiveness, and team outcomes. *The international journal of organizational analysis.* Vol. 11, No. 1, pp. 21-40.
252. Presthus, W., & Sønslien, K. F. (2021). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management*, *9*(1), 38-53.
253. Puiszis, S. M. (2018). Unlocking the EU General Data Protection Regulation. *J. Prof. Law.*, 1.
254. Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

255. Qassim, Q. S., Jamil, N., Daud, M., Patel, A., & Ja'affar, N. (2019). A review of security assessment methodologies in industrial control systems. *Information & Computer Security*.
256. Qassim, Q. S., Jamil, N., Daud, M., Patel, A., & Ja'affar, N. (2019). A review of security assessment methodologies in industrial control systems. *Information & Computer Security*, *27*(1), 47-61.
257. Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*, 3(9), 369-388. doi: 10.5281/zenodo.88708
258. Rahul, K., Banyal, R. K., & Bhatt, N. R. (2020). The Cyber Security Challenges: A Survey of Chief Information Security Officer in Indian Context. In *ICT for Competitive Strategies* (pp. 749-758). CRC Press.
259. Raipa, A. (2002). *Strateginis planavimas viešajame sektoriuje*. Viešasis administravimas, 274–286.
260. Raipa, A., & Jurkšienė, L. (2013). Inovatyvumas modernizuojant viešąjį valdymą: Baltijos šalių ir Danijos lyginamoji analizė. *Ekonomika ir vadyba: aktualijos ir perspektyvos*, (3), 22-32.
261. Raval, M. S., Gandhi, R., & Chaudhary, S. (2018). Insider threat detection: machine learning way. In *Versatile Cybersecurity* (pp. 19-53). Springer, Cham.
262. Rea-Guaman, A. M., Mejı´a, J., San Feliu, T., & CalvoManzano, J. A. (2020). AVARC-IBER: A framework for assessing cybersecurity risks. *Cluster Computing*. https://doi.org/10.1007/s10586-019-03034-9
263. Reeves, A., Calic, D., Delfabbro, P. (2020) Encouraging employee engagement with cyber security: how to tackle cyber fatigue. SAGE Open: Special Collection on Organizational Cybersecurity.
264. Reeves, A., Parsons, K., & Calic, D. (2020). Whose Risk Is It Anyway: How Do Risk Perception and Organisational Commitment Affect Employee Information Security Awareness?. In International Conference on Human-Computer Interaction (pp. 232-249). Springer, Cham.
265. Reeves, G. (2020). *A study to identify if there is a clear understanding and awareness of required records management policies and procedures in Irish Organisations, specifically, in relation to compliance with the General Data Protection Regulations (GDPR) which came into force on 28th May 2018* (Doctoral dissertation, Dublin, National College of Ireland).
266. Riordan, J., Lippmann R. P. (2016). Threat-Based Risk Assessment for Enterprise Networks.
267. Ritchey, D. (2020). The Changing Role of the CISO: And what physical enterprise security executives need to know about it. *Security: Solutions for Enterprise Security Leaders*, *57*(2), 16–18.
268. Ritzer, G. (2004). Encyclopedia of social theory. Sage publications.
269. Rothearmel, F. T. (2012). *Strategic management: concepts and cases*. Londra: McGraw-Hill Education.
270. Rudzkienė, V. (2005). Socialinė statistika. Mykolo Romerio universitetas
271. Rusydiyah, E. F., & Rohman, F. (2020). Local Culture-Based Education: An Analysis of Talcott Parsons' Philosophy. *International Journal of Innovation, Creativity and Change*, 12(3), 592-607.
272. Ryan, P., Crane, M., & Brennan, R. (2020). Design challenges for GDPR RegTech. *arXiv preprint arXiv:2005.12138*.
273. Sababa, B., Avogian, K., Dionysiou, I., & Gjermundrod, H. (2020). SMAD: A Configurable

and Extensible Low-Level System Monitoring and Anomaly Detection Framework. In *Innovations in Cybersecurity Education* (pp. 19-38). Springer, Cham.
274. Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2), 15-18.
275. Samardžić, D. (2021). Records of Processing Activities (Art. 30 Gdpr) in Analogue and Digital Ecosystems. *Anali Pravnog Fakulteta Univerziteta u Zenici*, *14*(29).
276. Sánchez, D., Viejo, A., & Batet, M. (2021). Automatic Assessment of Privacy Policies under the GDPR. *Applied Sciences*, *11*(4), 1762.
277. Sarantakos, S. (2004). *Social Research*. London: Palgrave Macmillan International Higher Education.
278. Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*(10), 2119-2126.
279. Scarfone K., Souppaya M., Cody A., Orebaugh A.. NIST SP 800-115 technical guide to information security testing and assessment. 2008.
280. Schreider, T. (2017). *Building Effective Cybersecurity Programs: A Security Manager's Handbook*. Rothstein Publishing.
281. Schreider, T. (2020). *Cybersecurity Law, Standards and Regulations*. Rothstein Publishing.
282. Schünemann, W. J., & Baumann, M. O. (Eds.). (2017). *Privacy, data protection and cybersecurity in Europe*. Springer International Publishing.
283. Schwab, K., Marcus, A., Oyola, J. O., Hoffman, W., & Luzi, M. (2011). Personal data: The emergence of a new asset class. In *An Initiative of the World Economic Forum*.
284. Sharma, S. (2019). *Data privacy and GDPR handbook*. John Wiley & Sons.
285. Shimonski, R. (2016). *CEH v9: Certified Ethical Hacker Version 9 Study Guide* (Vol. 9). John Wiley & Sons.
286. Siaurusevičiūtė, J., & Vasiliauskienė, B. (2015). Inventorizacijos reguliavimas Lietuvoje. In *Verslo aktualijos būsimųjų specialistų požiūriu, 2015: tarptautinė mokslinė konferencija, 2015 m. kovo 19 d. D. 2* (pp. 86-92). Kauno kolegijos Leidybos centras.
287. Šidlauskas, A, ir Ungurytė-Ragauskienė, S. (2020). Iššūkiai kibernetiniam saugumui: socialinė inžinerija institucinio izomorfizmo kontekste. *Visuomenės saugumas ir viešoji tvarka*, *25*, 389–405. https://doi.org/10.13165/PSPO-20-25-26
288. Šidlauskas, A. 2019. Video Surveillance and the GDPR. *Social Transformations in Contemporary Society (STICS 2019): Proceedings of an Annual International Conference for Young Researchers*, (7), 55-65.
289. Šidlauskas, A., & Ungurytė-Ragauskienė, S. (2020). Iššūkiai kibernetiniam saugumui: socialinė inžinerija institucinio izomorfizmo kontekste. *Public Security and Public Order*, (25).
290. Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*(1), 161-171.
291. Skukauskaitė, A., & Rupšienė, L. (2017). Teaching and learning qualitative methodologies in the context of developing doctoral education in Lithuania. *Acta Paedagogica Vilnensia*, *39*, 61-82.
292. Sommer, L. 2015. "Industrial Revolution – Industry 4.0: Are German Manufacturing SMEs the First Victims of This Revolution?" *Journal of Industrial Engineering and Management* 8 (5): 1512–1532.
293. Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. *Electronic markets*, *25*(2), 161-167.

294. Stallings, W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley Professional.
295. Štarchoň, P., & Pikulík, T. (2019). GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices-mobile phones. Procedia Computer Science, 151, 303-312.
296. Štareikė, E., & Kausteklytė-Tunkevičienė, S. (2018). Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą. *Visuomenės saugumas ir viešoji tvarka*, (20), 293-312.
297. Štitilis, D., Kiškis, M., Limba, T., Rotomskis, I., Agafonov, K., Gulevičiūtė, G. ir Panka, K. (2016). *Interneto ir technologijų teisė*. Vilnius: Registrų centras
298. Štitilis, D., Pakutinskas, P., Kinis, U., & Malinauskaitė, I. (2016). Concepts And Principles Of Cyber Security Strategies. *Journal of Security & Sustainability Issues*, *6*(2).
299. Štitilis, D., Pakutinskas, P., Laurinaitis, M., & Malinauskaitė-van de Castel, I. (2017). *Lietuvos kibernetinio saugumo strategijos modelis*. Mykolo Romerio universitetas.
300. Štitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., & Khorunzhak, N. (2020). National cyber security strategies: management, unification and assessment. The Independent Journal of Management & Production (IJM&P) v.11, n. 9, Special Edition (Baltic States), November 2020
301. Subramanian, O. (2020). Moving from blocker to enabler: cloud security and the modern CISO. *Computer Fraud & Security*, *2020*(10), 6-8.
302. Tamavičiūtė, V. (2019). Teisė būti (ne) pamirštam: kokias teisės ištrinti savo duomenis ribas nustato Europos Sąjungos Teisingumo Teismas?.
303. Tataru, G. F., & Tataru, Ș. R. (2020). Human Resources and Personal Data Protection: An Indissoluble Relationship. *Journal of Public Administration, Finance and Law*, *18*, 303-311.
304. Teixeira, G. A., da Silva, M. M., Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, 21(4), 402-418.
305. Testa, S., Nielsen, K. R., Bogers, M., Cincotti, S. (2019). The role of crowdfunding in moving towards a sustainable society. *Technological Forecasting and Social Change*, Vol. 141, p. 66–73.
306. Thiéry, S., & Fass, D. (2020, July). Cybersecurity Risks and Situation Awareness: Audit Committees' Appraisal. In *International Conference on Applied Human Factors and Ergonomics* (pp. 83-87). Springer, Cham.
307. Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018). EU general data protection regulation: changes and implications for personal data collecting companies, *Computer Law & Security Review*, 34(1), 134-153.
308. Tiliute, D. (2019). GDPR and its impact on it departments of companies. *The USV Annals of Economics and Public Administration*, *19*(2 (30)), 198-204.
309. Trochim, W. M. (2006). Qualitative measures. *Research measures knowledge base*, *361*(1), 2-16.
310. Tziogas, C., & Tsolakis, N. (2019). The dawn of GDPR: implications for the digital business landscape. In *Strategic Innovative Marketing and Tourism* (pp. 623-627). Springer, Cham.
311. Urban, T., Tatang, D., Degeling, M., Holz, T., & Pohlmann, N. (2019). A study on subject data access in online advertising after the gdpr. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 61-79). Springer, Cham.
312. Uyarra, E., Edler, J., Garcia-Estevez, J., Georghiou, L., & Yeow, J. (2014). Barriers to innovation through public procurement: A supplier perspective. *Technovation*, *34*(10), 631-645.

313. van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of consumer policy*, *42*(1), 91-107.
314. Vanagas, R., & Tumėnas, A. (2008). Savivaldybės darbuotojų tarnybinės veiklos vertinimas veiklos valdymo kontekste. Viešoji politika ir administravimas, nr. 25.
315. Varela-Vaca, Á. J., Gasca, R. M., Carmona-Fombella, J. A., & Gómez-López, M. T. (2020, October). AMADEUS: Towards the AutoMAteD secUrity testing. In *Proceedings of the 24th ACM Conference on Systems and Software Product Line: Volume A-Volume A* (pp. 1-12).
316. Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, *10*, 3152676.
317. von Solms, B., & von Solms, R. (2018). Cybersecurity and information security–what goes where?. *Information & Computer Security*.
318. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.
319. Waldman, A.E.: Privacy, notice, and design (2016)
320. Wang, P. (2018). Designing a doctoral level cybersecurity course. *Issues in Information Systems*, *19*(1)
321. Williams, E. J., Beardmore, A., Joinson, A. (2017) Individual differences in susceptibility to online influence: a theoretical review. *Comput. Hum. Behav*. 72, 412–421
322. Wirth, A. (2017). The economics of cybersecurity. *Biomedical instrumentation & technology*, *51*(s6), 52-59.
323. Wu, T., Zhang, R., Ma, W., Wen, S., Xia, X., Paris, C., ... & Xiang, Y. (2020). What risk? I don't understand. An Empirical Study on Users' Understanding of the Terms Used in Security Texts. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (pp. 248-262).
324. Wuyts, K., Scandariato, R., Joosen, W. (2014). Empirical Evaluation of a Privacy-Focused Threat Modeling Methodology. Journal of Systems and Software 96, 122–138. https://doi.org/10.1016/j.jss.2014.05.075
325. Xiong, W., Lagerström, R. (2019). Threat Modeling – A Systematic Literature Review. *Computers & Security* 84, 53–69. https://doi.org/ 10.1016/j.cose.2019.03.010
326. Yin, R. K. (2009). Case Study Research: Design and Methods. <https://books.google.lt/books/about/Case_Study_Research.html?id=FzawIAdilHkC&redir_esc=y>.
327. Zaleskis, J. (2017). Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą. *Teisė*, (104), 159-170.
328. Zaleskis. J. (2019) *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė.* Vilnius: Registrų centras.
329. Zanker, M., Bures, V., Cierniak-Emerych, A., & Nehez, M. (2021). The GDPR at the organizational level: a comparative study of eight European countries. *E & M Ekonomie a Management*, *24*(2).
330. Zgureanu, A. (2022). The role of RPO and RTO in disaster recovery planning. In *30 years of economic reforms in the Republic of Moldova: economic progress via innovation and competitiveness* (Vol. 3, pp. 221-232).
331. Zhuge, H. (2018). The complex link. arXiv preprint arXiv:1805.00434.
332. Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187.

333. Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety*, *177*, 176-190.
334. Žydžiūnaitė, V., Sabaliauskas, S. (2017). *Kokybiniai tyrimai: principai ir metodai: vadovėlis socialinių mokslų studijų programų studentams*. Vilnius: Vaga.

Kiti šaltiniai

335. Australian Cyber Security Centre, (2017). Threat Report 2017, Retrieved from: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC_Threat_Report_2017.pdf
336. Alvero, M. K. (2021) The Global Pandemic's Affect on Business Continuity - https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/the-global-pandemics-affect-on-business-continuity
337. Article 29 Data Protection Working Party (2014) *Opinion 05/2014 on Anomymisation Techniques*, WP216, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.
338. Article 29 Data Protection Working Party (2016) Guidelines on Data Protection Officers, WP243, <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf>.
339. Article 29 Data Protection Working Party, (2007). *Opinion 4/2007 on the concept of personal data*, WP136, <https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2007/wp136_en.pdf>.
340. Article 29 Data Protection Working Party, (2017). Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairės, WP251, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.
341. Article 29 Data Protection Working Party, (2017). Poveikio duomenų apsaugai vertinimo (PDAV) gairės, WP248, <https://ec.europa.eu/newsroom/article29/items/611236>.
342. Article 29 Data Protection Working Party, (2017). Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairės, WP260, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227>.
343. Basin, P. D (2020). Analyzing cookies compliance with the GDPR https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/information-security-group-dam/education/studentProjects/Thesis_proposal_Cookies_compliance.pdf
344. Bisson, D. (2021, May 24). What every incident response plan needs. Security Intelligence. *https://securityintelligence.com/articles/what-every-incident-response-plan-needs/*
345. Claroty, 2021. Claroty biannual ICS risk & vulnerability report: 2H 2020, Claroty Resarch Group. https://security.claroty.com/biannual-ics-risk-vulnerability-report-2H-2020
346. de Vries, J. (2017). What drives cybersecurity investment?: organizational factors and perspectives from decision-makers. https://repository.tudelft.nl/islandora/object/uuid:119719ff-cb69-44c5-a566-3ee8373509f7/datastream/OBJ1/download
347. Eijk van R., H. Asghari, Winter, P., Narayanan, A. The impact of user location on cookie notices (inside and outside of the European Union). In: Workshop on Technology and Consumer Protection (ConPro) (2019) https://ssrn.com/abstract=3361360
348. Enforcement Tracker (2021) Statistics: Countries with highest fines, <https://www.enforcementtracker.com>.
349. ENISA (2021) Threat Landscape, <https://www.enisa.europa.eu/topics/threat-risk-management/threats-andtrends/>.

350. ENISA (2022) Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.
351. European Commission. Directorate-General for Justice Consumers. (2018). *BDAR: Naujos galimybės, naujos prievolės: Ką kiekviena įmonė turi žinoti apie ES bendrąjį duomenų apsaugos reglamentą*. Luxembourg: Publications Office.
352. European Data Protection Supervisor. (2019). *Bendrojo duomenų apsaugos reglamento (BDAR) taikymas ES institucijoms jūsų teisės skaitmeniniame amžiuje*. Luxembourg: Publications Office.
353. European Union Agency for Network and Information Security (ENISA). (2018). Cyber Security Culture in organisations. Prieiga per internetą: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
354. Europos komisija (2019). Duomenų apsaugos taisyklių kaip priemonės pasitikėjimui didinti ES ir už ES ribų vertinimas, <https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:52019DC0374>.
355. Europos komisija (2020) Kas yra Europos duomenų apsaugos valdyba?, <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_lt>.
356. Gabel, D ir Hickman, T (2019) *Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law*, <https://www.whitecase.com/publications/article/chapter-17-issues-subject-national-lawunlocking-eu-general-data-protection>.
357. Garrett, G. (2018, December 13). Cyberattacks skyrocketed in 2018. Are you ready for 2019?, <https://www.industryweek.com/technology-and-iiot/ article/22026828/cyberattacks-skyrocketed-in-2018-areyou-ready-for-2019>.
358. Gunawardena, G. (2018). The Bitter Cookie: Right to Cyber Privacy in Sri Lanka Vs. the Misappropriation of Data Gathered Using Cookies http://ir.kdu.ac.lk/handle/345/2578
359. Helbing, T. (2022) GDPR - Records of Processing Activities (also: Data Inventory, Data Mapping): Information, Examples, Templates, Free Excel, <https://www.thomashelbing.com/en/info/records-data-processing-activities-data-mapping-data-inventory>
360. Hilberg, S. L. (2022) The new records of data processing activities <https://www2.deloitte.com/dl/en/pages/legal/articles/dsgvo-verfahrensverzeichnis.html>
361. ID Agent, 2021, How often should businesses run cybersecurity awareness training? https://www.idagent.com/blog/ how-often-should-businesses-runcybersecurity-awareness-training
362. Information Commissioner's Office (2021) Right to erasure <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/>.
363. International Telecommunication Union (ITU). (2015). Global Cyber-Security index & cyberwellness profiles. ABI research Telecommunication Development Sector, Geneve, <www.itu.int>.
364. ISO 10015 Quality management -- Guidelines for competence management and people development https://eshop.lsd.lt/public#!/product/info/0a64031e-6f57-1255-816f-582a566d0134
365. ISO 27005 standartas. Informacinės technologijos. Saugumo metodai. Informacijos saugumo rizikos valdymas - https://eshop.lsd.lt/public#!/product/info/0a640324-6747-1da0-8167-607d2e57014a
366. ISO 27035-1 Information technology -- Security techniques -- Information security

incident management Principles of incident management https://eshop.lsd.lt/public#!/product/info/0a640324-6747-1da0-8168-8084f5261474
367. ISO 31000 standartas. Įmonės veiklos organizavimas ir vadyba. Bendrieji dalykai https://eshop.lsd.lt/public#!/product/info/0a640325-61b4-16b2-8161-e358e27a015a
368. Jurkonis, J. (2021) Darbuotojas, atsakingas už duomenų apsaugą https://www.trustguru.lt/blog/darbuotojas-atsakingas-uz-duomenu-apsauga
369. Kalshoven, K., & Boon, C. T. (2012). Ethical leadership, employee well-being, and helping: The moderating role of human resource management. *Journal of Personnel Psychology*, 11(1), 60.
370. Koskelo, M. (2020). OT-asset CMDB Solutions. https://www.theseus.fi/bitstream/handle/10024/339177/Koskelo_Miska.pdf?sequence=2
371. Kosutic, D (2017) What is the difference between Recovery Time Objective (RTO) and Recovery Point Objective (RPO)? https://advisera.com/27001academy/knowledgebase/what-is-the-difference-between-recovery-time-objective-rto-and-recovery-point-objective-rpo/
372. Krašto apsaugos ministerija (2020) Nacionalinio kibernetinio saugumo būklės ataskaita už 2020 metus, <https://www.nksc.lt/doc/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf>.
373. Krašto apsaugos ministerija (2021) Nacionalinio kibernetinio saugumo būklės ataskaita už 2021 metus, <https://kam.lt/wp-content/uploads/2022/05/Kibernetinio-saugumo-santrauka-1.pdf>.
374. Krašto apsaugos ministerija (2022) Nacionalinio kibernetinio saugumo būklės ataskaita už 2022 metus, <https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf>.
375. Lietuvos Respublikos valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos (2018). *Grėsmių nacionaliniam saugumui vertinimas,* <https://www.vsd.lt/wp-content/uploads/2018/03/LTU.pdf>.
376. Lietuvos standartizacijos departamentas (2020) ISO standartai, < https://www.lsd.lt/ >.
377. Lord, N. (2018) What is Security Incident Management? The Cybersecurity Incident Management Process, Examples, Best Practices, and More https://digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-process
378. McCarthy, D. (2018). 7 Elements of a Strategic Plan. Retrieved from thebalancecareers: https://
379. Nadeau (2017) General Data Protection Regulation (GDPR): What you need to know to stay compliant, <https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html>
380. National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity. Version* 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP.04162018.pdf
381. Overfelt, M. (2016). World's Oldest Hacking Profession Doesn't Rely on Internet. The Hacking Economy, <https://www.cnbc.com/2016/05/13/a-surprising-source-of-hackers-and-costly-data-breaches.html?&web_view=true>.
382. Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226-241.
383. Ponemon Institute (2017) *The Evolving Role of CISOs and Their Importance to the Business*,

<https://www.ponemon.org/research/ponemon-library/security/the-evolving-role-of-cisos-and-their-importance-to-the-business.html>.
384. Projektas „*SolPriPa*“ (2020) Asmens duomenų apsaugos gairės smulkiajam ir vidutiniam verslui, <https://vdai.lrv.lt/lt/naudinga-informacija/solpripa-projektas>.
385. Rauf, A. (2019). The Importance of Human Factor in Cyber security. https://www.researchgate.net/publication/332539716_The_Importance_of_Human_Factor_in_Cybersecurity
386. Reuter, P. (2018). General data protection regulation (GDPR). *Intersoft Consulting, Accessed in October*, 24(1).
387. Richie Koch (2020). Cookies, the gdpr, and the eprivacy directive, Retrieved from https://gdpr.eu/cookies/
388. SANS instituto „*CIS Critical Security Controls Version 8*“ prioritetinių apsaugos priemonių rinkinys - https://www.cisecurity.org/controls/v8
389. Satariano, A (2020) *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, <https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html>.
390. Scarfone, K., Souppaya, M., Cody, A. ir Orebaugh, A. (2021) Technical Guide to Information Security Testing and Assessment. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
391. Siegel, B. (2016) "Privacy policy or privacy notice: what's the difference?" https://www.csoonline.com/article/3063601/privacy/privacy-policies-and-privacy-notices-whats-the-difference.html
392. Slivka, M. (2020), What is Alexa Rank and Its Value?, < https://attentioninsight.com/what-is-alexa-rank-and-its-value>.
393. Stravinskaitė, R. (2022) Kaip kuo greičiau suvaldyti duomenų saugumo incidentą? https://motieka.com/lt/naujienos/kaip-kuo-greiciau-suvaldyti-duomenu-saugumo-incidenta/
394. The North Atlantic Treaty Organization (2011) *Defending the networks: The NATO Policy on Cyber Defence*, <https://www.ccdcoe.org/uploads/2018/10/NATO-110608-CyberdefencePolicyExecSummary.pdf>.
395. Thomson Reuters, (2019) GDPR+1 YEAR: Business Struggles with Data Privacy Regulations Increasing, <http://ask.legalsolutions.thomsonreuters.info/GDPR1YearBusinessStrugglesReport>.
396. Valstybės kontrolės 2022 m. spalio 27 d. valstybinio audito ataskaita „Kibernetinio saugumo užtikrinimas“ https://www.valstybeskontrole.lt/LT/Product/24128/kibernetinio-saugumo-uztikrinimas
397. Valstybinė duomenų apsaugos inspekcija (2020) „2019 m. Lietuvos gyventojų tyrimas apie asmens duomenų apsaugą – išlaikyti aukšti žinančių apie savo teises ir pareigas asmens duomenų apsaugos srityje rodikliai“, <https://vdai.lrv.lt/lt/naujienos/2019-m-lietuvos-gyventoju-tyrimas-apie-asmens-duomenu-apsauga-islaikytiauksti-zinanciu-apie-savo-teises-ir-pareigas-asmens-duomenu-apsaugos-srityje-rodikliai>.
398. Valstybinė duomenų apsaugos inspekcija (2021) Apklausos rezultatai – ką Lietuvos gyventojai galvoja apie asmens duomenų apsaugą?, <https://vdai.lrv.lt/lt/naujienos/apklausos-rezultatai-ka-lietuvos-gyventojai-galvoja-apie-asmens-duomenu-apsauga-1>.
399. Valstybinė duomenų apsaugos inspekcija (2022) 2021 metų veiklos ataskaita https://vdai.lrv.lt/lt/naujienos/valstybines-duomenu-apsaugos-inspekcijos-2021-m-veiklos-ataskaita
400. Valstybinė duomenų apsaugos inspekcija (2022) I pusmečio pranešimų apie asmens duomenų saugumo pažeidimus apžvalga https://vdai.lrv.lt/lt/naujienos/2022-m-i-pusmecio-pranesimu-apie-asmens-duomenu-saugumo-pazeidimus-apzvalga
401. Valstybinės duomenų apsaugos inspekcijos parengtos gairės „Tvarkomų asmens duomenų

saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“ (3 versija, 2020-06-18), <https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf>.
402. Wolford, B (2022) Writing a GDPR-compliant privacy notice (template included) https://gdpr.eu/privacy-notice/
403. Woods, T., (2019) “GDPR’s Impact on Incident Response,” last modified April 25, 2019, <https://securitytoday.com/articles/2019/04/24/gdprs-impact-on-incident-response.aspx>
404. www.thebalancecareers.com/strategic-plan-elements-2276139.
405. Žurnalistų etikos inspektoriaus tarnyba (2019) Žurnalistų etikos inspektoriaus 2018 metų veiklos ataskaita. <http://www.zeit.lt/data/public/uploads/2019/04/2018-metu-pataisyta-ataskaita.pdf>.

PRIEDAI

1 PRIEDAS

1 lentelė. Duomenų apsaugos pareigūno statusas

Reglamentas	ES 29 straipsnio darbo grupės rekomendacijos
Duomenų valdytojas ir duomenų tvarkytojas užtikrina, kad Pareigūnas būtų tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų nagrinėjimą.	Pareigūnas turi būti kuo ankstyvesniu etapu įtraukiamas į visus su duomenų apsauga susijusius klausimus ir organizacijoje laikomas diskusijų partneriu, dalyvaujančiu atitinkamose darbo grupėse arba vyresniosios ir vidurinio lygmens vadovybės posėdžiuose.
Duomenų valdytojas ir duomenų tvarkytojas padeda Pareigūnui atlikti Reglamente nurodytas užduotis suteikdamas toms užduotims atlikti būtinus išteklius, taip pat suteikdamas galimybę susipažinti su asmens duomenimis, dalyvauti duomenų tvarkymo operacijose ir išlaikyti savo ekspertines žinias.	Organizacijoje turi būti įvertinami šie aspektai: • Aktyvi vyresniosios vadovybės parama Pareigūnui. • Pakankamai laiko Pareigūnui jo pareigoms atlikti. • Pakankama parama finansiniais ištekliais, infrastruktūra, o prireikus – ir darbuotojais. • Oficialus pranešimas apie Pareigūno paskyrimą visiems darbuotojams. • Būtina galimybė naudotis kitomis tarnybomis, pvz., žmogiškųjų išteklių, teisės, IT, apsaugos ir kt., kad Pareigūnas galėtų gauti būtiną paramą ir informaciją. • Nuolatinis mokymas. Pareigūnui turi būti suteikta galimybė sekti naujausias tendencijas duomenų apsaugos srityje. • Atsižvelgiant į organizacijos dydį ir struktūrą, esant poreikiui, sudaryti Pareigūno grupę, kurią sudarytų Pareigūnas ir darbuotojai, vykdantys jo užduotis.

Duomenų valdytojas ir duomenų tvarkytojas užtikrina, kad Pareigūnas negautų jokių nurodymų dėl savo užduočių vykdymo. Duomenų valdytojas arba duomenų tvarkytojas negali jo atleisti arba bausti dėl jam nustatytų užduočių atlikimo. Pareigūnas tiesiogiai atsiskaito duomenų valdytojo arba duomenų tvarkytojo aukščiausio lygio vadovybei.	Pareigūnas neturi gauti nurodymų, kaip spręsti su duomenų apsauga susijusius klausimus. Jeigu duomenų valdytojas arba duomenų tvarkytojas priima sprendimus, kurie yra nesuderinami su Reglamentu ir Pareigūno konsultacija, Pareigūnui turėtų būti suteikta galimybė aiškiai pareikšti savo nesutikimą aukščiausio lygmens vadovybei ir sprendimus priimantiems asmenims. Pagal Reglamentą nuobaudas draudžiama taikyti tik tuo atveju, jeigu jos skiriamos dėl dalykų, susijusių su Pareigūno pareigų atlikimu.
Duomenų subjektai gali kreiptis į Pareigūną visais klausimais, susijusiais jų asmeninių duomenų tvarkymu ir naudojimusi savo teisėmis pagal Reglamentą.	Labai svarbu suteikti galimybę kreiptis į Pareigūną fiziškai ar kitomis saugiomis ryšių priemonėmis.
Pareigūnas privalo užtikrinti slaptumą arba konfidencialumą, susijusį su jo užduočių vykdymu.	Įpareigojimu laikytis slaptumo ar konfidencialumo Pareigūnui nedraudžiama susisiekti su VDAI ir kreiptis į ją konsultacijos.
Pareigūnas gali vykdyti kitas užduotis ir pareigas. Duomenų valdytojas arba duomenų tvarkytojas užtikrina, kad dėl bet kokių tokių užduočių ir pareigų nekiltų interesų konfliktas.	Organizacijos gali taikyti šią gerąją patirtį: • Parengti vidaus taisykles ir nustatyti pareigybes, kurios būtų nesuderinamos su Pareigūno funkcijomis ir bendrai paaiškinti apie interesų konfliktą, siekiant jo išvengti. • Paskelbti, kad Pareigūnui nekyla interesų konflikto.

Šaltinis: Šidlauskas, 2021

2 PRIEDAS

Kibernetinio saugumo ir asmens duomenų apsaugos priemonės

Organizacijos norėdamos užtikrinti kibernetinį saugumą ir asmens duomenų apsaugą taiko įvairias priemones. Taikomos priemonės yra pateikiamos tarptautiniuose teisės aktuose ir LR teisės aktuose, standartuose, priežiūros institucijų gairėse:

1. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (žr. 1 lentelę).

1 lentelė. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas

Priemonė	Techninių kibernetinio saugumo priemonių detalizavimas
Atpažinties, tapatumo patvirtinimo ir naudojimosi RIS saugumas ir kontrolė	IS naudotojų ir administratorių paskyrų ir teisių kontrolė; Virtualus privatus tinklo šifravimas; Tapatybės patvirtinimas; Slaptažodžių reikalavimai.
RIS, RIS naudotojų ir RIS administratorių atliekamų veiksmų auditas ir kontrolė	Audito įrašų rinkimas, stebėjimas ir analizavimas, saugojimas, prieigos prie įrašų ribojimas, įrašų keitimų ir trynimų draudimas, įrašų kopijų darymas.
Įsibrovimų aptikimas ir prevencija	Įsibrovimo aptikimo sistemos ir ugiasienės.
Belaidžio tinklo saugumas ir kontrolė	Belaidžių įrenginių identifikavimas, jų stebėjimas, apribojimas. Belaidės prieigos taškai; tapatumo patvirtinimas; Saugumo protokolų reikalavimai.
Mobiliųjų įrenginių, naudojamų prisijungti prie RIS, saugumas ir kontrolė	Mobiliųjų įrenginių atpažinties, tapatumo patvirtinimo ir naudojimosi reikalavimai; apribojimas neleistinų mobiliųjų įrenginių ar asmenų; centralizuotas mobiliųjų įrenginių valdymas; duomenų šifravimas ir t.t.
RIS naudojamos svetainės, pasiekiamos iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė	Svetainės atpažinties, tapatumo patvirtinimo ir naudojimosi reikalavimai; Svetainės, svetainės kriptografijos reikalavimų įgyvendinimas, saugos parametrų testavimas; svetainės saugasienės naudojimas.
RIS naudojamo interneto saugumas ir kontrolė	Su interneto paslaugos teikėju turi būti sudarytos sutartys: Reagavimo į kibernetinius incidentus (ne)darbo valandomis; nepertraukiamo interneto paslaugos teikimo, apsaugos nuo trikdymo ir sutrikimų registravimo.

Priemonė	Organizacinių kibernetinio saugumo priemonių detalizavimas
Rizikos ir Atitikties vertinimai	Ne rečiau kaip kartą per metus arba po esminių pokyčių organizuojamas ir atliekamas rizikos vertinimas ir (arba) atitikties vertinimas.
Veiklos tęstinumo valdymo ar kibernetinių incidentų valdymo planai	Atsižvelgiant į atlikto Rizikos vertinimo rezultatus, tobulinamas IS veiklos tęstinumo valdymo planas ar kibernetinių incidentų valdymo planas. Atliekami šių planų išbandymai, pastebėtų trūkumų ataskaitos, ne vėliau kaip per penkias darbo dienas pateikiamos Nacionaliniam kibernetinio saugumo centrui.
Kibernetinio saugumo politika	Suderinus su NKSC, tvirtinami kibernetinio saugumo politikos dokumentai. Šie dokumentai turi būti peržiūrimi (persvarstomi) ne rečiau kaip kartą per metus.
Audito įrašų analizė	Ne rečiau kaip kartą per mėnesį turi būti atliekama IS ar IS naudotojų veiksmų audito įrašų analizė. Ne rečiau kaip kartą per mėnesį turi būti atliekama saugasienių užfiksuotų įvykių analizė ir šalinamos pastebėtos neatitiktys saugumo reikalavimams.
Programiniai atnaujinimai	Ne rečiau kaip kartą per mėnesį turi būti įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.
Sąlygos paslaugų teikėjams	Pirkimo dokumentuose turi iš anksto nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį kibernetinio saugumo reikalavimams.

Šaltinis: sudaryta autoriaus pagal Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimą Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“

2. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (žr. 2 lentelę).

2 lentelė. Bendrieji elektroninės informacijos saugos reikalavimai

Priemonė	Organizacinių kibernetinio saugumo priemonių detalizavimas
Saugos dokumentai	IS valdytojas privalo turėti saugos dokumentus: Saugos nuostatus; Saugaus elektroninės informacijos tvarkymo taisykles; IS veiklos tęstinumo valdymo planą; IS naudotojų administravimo taisykles. Saugos dokumentai institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus arba po esminių pokyčių organizacijoje. Keičiami saugos dokumentai derinami su NKSC.
Saugos įgaliotinis	Koordinuoja elektroninės informacijos saugos incidentų, tyrimą ir bendradarbiauja su kompetentingoms institucijoms. Teikia administratoriui ir IS naudotojams privalomus vykdyti nurodymus, susijusius su saugos politikos įgyvendinimu. Organizuoja rizikos įvertinimą. Periodiškai organizuoja IS naudotojų mokymą elektroninės informacijos saugos klausimais ir IS naudotojų supažindinimą su saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą.
IS administratorius	Administratorius atlieka funkcijas, susijusias su IS naudotojų teisių valdymu, IS komponentais, šių IS komponentų sąranka, IS pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus.
Informavimas apie incidentus	Pastebėjus saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalu nedelsdami pranešti apie tai administratoriui, saugos įgaliotiniui arba jeigu įsteigta informacinių technologijų pagalbos tarnybai.
Rizikos vertinimas	Saugos įgaliotinis kasmet organizuoja arba pats atlieka visų IS rizikos įvertinimą. Rizikos įvertinimo ataskaita pateikiama organizacijos vadovui. Atsižvelgus į rizikos įvertinimo ataskaitą, tvirtinamas rizikos valdymo priemonių planas. Šie dokumentai ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti ARSIS.
Pokyčių planavimas	IS valdytojas užtikrina IS pokyčių valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą, įtakos vertinimą ir pokyčių prioritetų nustatymą.
IS sąrankos stebėsena, testavimas	IS sąrankos aprašai turi būti nuolat atnaujinami ir rodyti esamą IS sąrankos būklę. Pokyčiai, galintys daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje.
Atitikties vertinimas	Atlikus Atitikties vertinimą, rengiama Atitikties vertinimo ataskaita, kuri pateikiama organizacijos vadovui, ir pastebėtų trūkumų šalinimo planas. Atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo planas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateiktas ARSIS.

Atsakomybė ir konfidencialumas	IS naudotojai, pažeidę saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.
Konfidencialumas	IS naudotojai privalo saugoti duomenų ir informacijos paslaptį, įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

Šaltinis: sudaryta autoriaus pagal Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo...".

3. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašą, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo"(žr. 3 lentelę).

3 lentelė. Elektroninės informacijos saugos reikalavimai

Priemonė	**Bendrųjų IS kibernetinio saugumo priemonių detalizavimas**
Atitikties vertinimas	Atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per du metus, jei kituose teisės aktuose nenustatyta kitaip.
Audito įrašai	IS turi būti įrašomi ir IS valdytojo nustatytą laiką saugomi audito įrašų duomenys, kurie turi būti saugomi ne toje pačioje IS, kurioje jie įrašomi, taip pat jie turi būti analizuojami ne rečiau kaip kartą per savaitę.
IS paskyros ir prieigos teisės	Paskyrų valdymas ir kontrolė; IS naudotojų unikalus atpažinimas; prieigos teisių suteikimas; tapatybės patvirtinimas; nuotolinis prisijungimas ir t.t.
Maksimalus IS neveikimo laikotarpis	IS neveikimo laikotarpis negali būti ilgesnis nei: ketvirtos kategorijos IS – 24 val.; trečios kategorijos IS – 16 val.; antros kategorijos informacinės sistemos – 12 val.; pirmos kategorijos informacinės sistemos – 8 val.
Reikalavimai įrangai ir patalpoms	Pagrindinė IS kompiuterinė įranga turi turėti įtampos filtrą ir rezervinį maitinimo šaltinį; IS tarnybinių stočių patalpos oro kondicionavimo įrangą.
Kenksmingosios programinės įrangos aptikimo priemonės	IS tarnybinėse stotyse ir vidinių IS naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės.
Programinės įrangos atnaujinimas	Turi būti operatyviai ištestuojami ir įdiegiami IS tarnybinių stočių ir vidinių IS naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai ir t.t.

Legali programinė įranga	IS tarnybinėse stotyse ir vidinių IS naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali programinė įranga; parengtas leistinos programinės įrangos sąrašas.
IS įrangos priežiūra	IS techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų, priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai.
IS tarnybinių stočių patalpos	IS tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas, įrengti gaisro ir įsilaužimo davikliai.
Minimalus IS prieinamumas	Per metus turi būti užtikrintas IS prieinamumas priklausomai nuo IS svarbos kategorijos – ne mažiau kaip 70 proc., 90 proc., 96 proc. ir 99 proc. laiko darbo metu darbo dienomis.
Atsarginės kopijos	Turi būti daromos atsarginės kopijos, kurios turi būti laikomos kitose patalpose arba kitame pastate nei yra IS tarnybinės stotys; elektroninė informacija kopijose turi būti užšifruota.
Ugniasienės	Ugniasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos.
Slaptažodžių reikalavimai	Slaptažodžių ilgis ir sudėtis – raidės, skaičiai ir specialieji simboliai; mėginimų skaičius įvesti teisingą slaptažodį, slaptažodžių saugojimas, slaptažodžių keitimo terminas.
Priemonė	**Papildomos trečiosios kategorijos IS kibernetinio saugumo techninės priemonės**
Kompiuterio resursų stebėsena	IS turi perspėti IS administratorių, kai pagrindinėje IS kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;
Virtualus privatus tinklas	Viešaisiais ryšių tinklais perduodamos informacinės šifravimas, virtualų privatų tinklą (angl. *Virtual private network*).
IS tarnybinių stočių patalpos	Patekimo ribojimas į IS tarnybinių stočių ir atsarginių kopijų saugojimo patalpas. Atsarginių patalpų reikalavimai ir atsarginių laikmenų saugojimo reikalavimai
Programinė įranga	Programinę įrangą diegia tik įgalioti asmenys prieš tai ją ištestavę testavimo aplinkoje.
Priemonė	**Papildomi antrosios kategorijos IS kibernetinio saugumo techninės priemonės**
Atitikties vertinimas	Atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per metus.
Išorinės laikmenos	Vidinių IS naudotojų darbo vietose gali būti naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (pavyzdžiui, USB, CD/DVD ir kt.).

Svarbiausia įranga	Svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima; rezervinį maitinimo šaltinį.
Gedimų registravimas	Svarbiausios kompiuterinės įrangos gedimai turi būti registruojami, taip pat turi būti paskirtas asmuo už gedimų registravimą.
Audito įrašai	Įrašų rinkimas, stebėjimas ir analizavimas, saugojimas (1 metus), prieigos prie įrašų ribojimas, įrašų keitimų ir trynimų draudimas.
Reikalavimai patalpoms	IS tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga; gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų.
Ugniasienės	Turi būti naudojamos ugniasienės ir automatinės įsilaužimo aptikimo sistemos.
Priemonė	**Papildomos pirmosios kategorijos IS kibernetinio saugumo techninės priemonės**
Trečiųjų šalių auditas	Ne rečiau kaip kartą per trejus metus atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai;
ISO 27002 ir ISO 27001	Institucija turi įgyvendinti Lietuvos standarte LST ISO/IEC 27002 ir LST ISO/IEC 27001 nurodytas saugos priemones.
Kitos priemonės	IS valdytojai ir tvarkytojai privalo užtikrinti saugos priemonių, skirtų ne žemesnei kategorijai negu yra nustatyta jų informacinei sistemai, taikymą. Taip pat gali būti taikomos saugos priemonės, nenurodytos reikalavimuose, tačiau rekomenduojamos pripažintose metodikose ar Lietuvos ir tarptautiniuose standartuose.

Šaltinis: sudaryta autoriaus pagal Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo...“

4. Lietuvos standartas LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos“ Reikalavimai (žr. 4 lentelę).

4 lentelė. ISO 27001 reikalavimai

Priemonė	**ISO 27001 reikalavimai (YSII ir I kategorijos IS)**
Organizacijos situacija	Organizacijos ir jos situacijos supratimas; Suinteresuotųjų šalių poreikių ir lūkesčių supratimas; Informacijos saugumo valdymo sistemos taikymo srities nustatymas; Informacijos saugumo valdymo sistema.
Vadovavimas	Vadovavimas ir įsipareigojimas; Politika; Vaidmenys, atsakomybės ir įgaliojimai organizacijoje.
Planavimas	Veiksmai rizikoms ir galimybėms valdyti: Bendrosios nuostatos; Informacijos saugumo rizikos vertinimas; Informacijos saugumo rizikos priežiūra. Informacijos saugumo tikslai ir jų pasiekimo planavimas.

Priemonės	Ištekliai; Kompetencija; Informuotumas; Komunikacija; Dokumentuota informacija: Bendrosios nuostatos; Kūrimas ir atnaujinimas; Dokumentuotos informacijos kontrolė.
Eksploatavimas	Eksploatavimo planavimas ir valdymas; Informacijos saugumo rizikos vertinimas; Informacijos saugumo rizikos priežiūra.
Veiksmingumo vertinimas	Stebėsena, matavimas, analizė ir vertinimas; Vidaus auditas; Vadovybės peržiūra.
Gerinimas	Neatitiktis ir korekciniai veiksmai; Nuolatinis gerinimas.

Šaltinis: sudaryta autoriaus pagal standartą ISO 27001

5. Lietuvos standartas LST EN ISO/IEC 27002:2017 "*Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai*" (žr. 5 lentelę).

5 lentelė. ISO 27002 reikalavimai

Priemonė	**ISO 27002 reikalavimai (YSII ir I kategorijos IS)**
Informacijos saugumo politika	Informacijos saugumo politika ii jos peržiūra.
Informacijos saugumo organizavimas	Informacijos saugumo funkcijos ir atsakomybė; Pareigų atskyrimas; Ryšys su valdžios institucijomis ir specialių interesų grupėmis; Mobilieji įrenginiai ir nuotolinis darbas.
Žmogiškųjų išteklių saugumas	Tikrinimas prieš įdarbinimą; Vadovybės atsakomybės; Informacijos saugumo mokymas; Drausminės procedūros; Darbo sutartyje nustatytų atsakomybių pabaiga arba keitimas.
Turto valdymas	Turto inventorizavimas; Atsakomybė už turtą; Turto naudojimas; Turto grąžinimas. Informacijos klasifikavimas ir žymėjimas, Turto priežiūra. Duomenų laikmenų priežiūra.
Prieigos valdymas	Veiklos reikalavimai prieigos valdymui; Naudotojų prieigos valdymas; Naudotojų atsakomybės; Prieigos prie sistemų ir taikomųjų programų valdymas.
Kriptografija	Kriptografijos kontrolės priemonių naudojimo politika; Raktų valdymas.
Fizinis ir aplinkos saugumas	Fizinė perimetro apsauga; Įstaigų, patalpų ir priemonių apsauga; Apsauga nuo išorinių ir aplinkos grėsmių; Įrangos priežiūra ir saugumas.
Darbo saugumas	Darbo procedūros ir atsakomybės; Apsauga nuo kenkimo programų; Registravimas ir stebėsena; Operacinės programinės įrangos kontrolė; Techninio pažeidžiamumo valdymas; Informacinių sistemų auditas.
Ryšių saugumas	Tinklo apsaugos valdymas; Informacijos perdavimas.

Sistemų įsigijimas, kūrimas ir priežiūra	Informacinių sistemų saugumo reikalavimai; Kūrimo ir priežiūros procesų saugumas; Testavimo duomenų apsauga.
Santykiai su tiekėjais	Informacijos saugumo politika palaikant santykius su tiekėjais; Tiekėjų paslaugų teikimo valdymas
Informacijos saugumo incidentų valdymas	Pranešimas apie informacijos saugumo įvykius, jų vertinimas ir sprendimų priėmimas; Reagavimas į informacijos saugumo incidentus; Mokymasis iš informacijos saugumo incidentų; Įrodymų rinkimas.
Veiklos tęstinumo valdymo informacijos saugumo aspektai	Informacijos saugumo tęstinumo planavimas; Informacijos saugumo tęstinumo įgyvendinimas, tikrinimas, peržiūra ir įvertinimas.
Atitiktis	Atitiktis teisiniams ir sutartiniams reikalavimams; Nepriklausoma informacijos saugumo peržiūra; Atitiktis saugumo politikoms ir standartams; Techninės atitikties tikrinimas.

Šaltinis: sudaryta autoriaus pagal standartą ISO 27002

6. Valstybinės duomenų apsaugos inspekcijos parengtos gairės „*Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*“ (3 versija, 2020-06-18) (žr. 6 lentelę).

6 lentelė. Tvarkomų asmens duomenų saugumo priemonės

Priemonė	VDAI organizacinių priemonių detalizavimas
Asmens duomenų saugumo politika ir procedūros	Saugumo politika yra svarbus dokumentas, nustatantis pagrindinius informacijos saugumo ir asmens duomenų apsaugos principus ir bendrą valdymą organizacijoje. Remiantis saugumo politika, konkrečios techninės ir organizacinės priemonės aprašomos detalesnėse politikose.
Vaidmenys ir atsakomybės	Pagrindinės asmens duomenų saugumo priemonės organizacijos personalui, turinčiam prieigą prie asmens duomenų – aiškiai apibrėžta ir dokumentuota atsakomybė bei vaidmenys, taip pat darbo su asmens duomenimis kompetencijos. Ypač svarbus vaidmuo tenka saugos specialistui (ar įgaliotiniui), kuris yra atsakingas už tinkamos saugumo politikos įgyvendinimą. Kitas svarbus vaidmuo tenka duomenų apsaugos pareigūnui (toliau – DAP), kurio viena iš užduočių yra stebėti, kaip organizacijoje laikomasi BDAR. Tiek saugos specialistas (ar įgaliotinis), tiek DAP turi glaudžiai bendradarbiauti.
Prieigos valdymo politika	Būtina nustatyti prieigos kontrolės politiką sistemoms, naudojamoms tvarkant asmens duomenis. Kontrolė turi būti grindžiama principu „būtina žinoti“, t. y. kiekvienam vaidmeniui ar naudotojui turi būti suteiktas tik toks asmens duomenų prieinamumo lygis, kuris yra būtinas jo užduotims atlikti.

Išteklių ir turto valdymas	Tinkamas techninės, programinės ir tinklo įrangos valdymas yra būtinas asmens duomenų saugumui ir vientisumui, nes tai leidžia kontroliuoti duomenų tvarkymo priemones. Išteklių valdymas būtinai turi apimti IT išteklių ir tinklo topologijos (schemos), kuri yra naudojama tvarkant asmens duomenis, registravimą.
Keitimų valdymas	Keitimų valdymo tikslas – sinchronizuoti ir kontroliuoti visus IT sistemose, naudojamose tvarkant asmens duomenis, atliekamus keitimus. Tai yra svarbi saugumo priemonė, nes nesėkmingas keitimų įgyvendinimas gali sukelti neteisėtą duomenų atskleidimą, pakeitimą ar sunaikinimą.
Duomenų tvarkytojai	BDAR 28 straipsnis numato, kad „duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga.“ Tame pačiame straipsnyje nurodoma, kad duomenų valdytojo ir duomenų tvarkytojo santykiai turi būti apibrėžti sutartyje ar teisės akte.
Asmens duomenų saugumo pažeidimai ir saugumo incidentai	Duomenų saugumo pažeidimo atveju organizacija turi įvertinti, ar tai turės įtakos „atsitiktiniam ar neteisėtam perduodamų, saugomų ar kitaip tvarkomų asmens duomenų sunaikinimui, praradimui, pakeitimui, neteisėtam atskleidimui ar prieigai prie jų“. Tiek duomenų valdytojai, tiek ir duomenų tvarkytojai turi turėti tinkamas procedūras ne tik pranešti apie asmens duomenų pažeidimus, bet ir juos suvaldyti.
Veiklos tęstinumas	Veiklos ar paslaugų tęstinumo planas yra būtinas nustatant procesus ir technines priemones, kurių organizacija turi laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju. Šis planas papildo organizacijos saugumo politiką. Ši priemonė aiškiai susijusi su BDAR 32 straipsnio 1 dalies c punktu, kuris įpareigoja duomenų valdytoją ir tvarkytoją „laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“.
Personalo konfidencialumas	Siekiant užtikrinti asmens duomenų konfidencialumą pagal BDAR 32 straipsnį, organizacija turi užtikrinti, kad jos darbuotojai gebėtų konfidencialiai tvarkyti informaciją tiek techniniu, tiek asmeninio sąžiningumo požiūriu.
Mokymai	Personalo mokymai apie duomenų apsaugos ir saugumo procedūras yra svarbūs tinkamam organizacinių ir techninių duomenų saugumo priemonių įgyvendinimui ir prevencijai dėl „netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų“.
Priemonė	**VDAI techninių priemonių detalizavimas**
Prieigų kontrolė ir autentifikavimas	Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie IT sistemos, kurioje yra tvarkomi asmens duomenys.

Techninių žurnalų įrašai ir stebėsena	Techninių žurnalų įrašai yra esminis saugos reikalavimas, kuris leidžia identifikuoti ir stebėti, sekti naudotojų veiksmus (kurie susiję su asmens duomenų tvarkymu), taip užtikrinant atskaitingumą (jei įvyktų neautorizuotas asmens duomenų atskleidimas, keitimas ar panaikinimas). Taip pat svarbu nuolat stebėti techninių žurnalų įrašus, kurie leistų identifikuoti potencialius vidinius ar išorinius bandymus pažeisti sistemos saugumą ir integralumą.
Tarnybinių stočių, duomenų bazių apsauga	Informacinių sistemų pagrindas yra tarnybinės stotys ir duomenų bazės. Jų apsauga privalo būti sustiprinta, siekiant užtikrinti saugią darbo aplinką.
Darbo vietų apsauga	Šis reikalavimas yra susijęs su saugos nustatymais naudotojų darbo stotyse ar kituose įrenginiuose. Yra svarbu priverstinai nustatyti specifinę saugos politiką ir apriboti naudotojų veiksmus, siekiant apsaugoti IT sistemas (pvz., antivirusinės programinės įrangos išjungimas, neautorizuotos programinės įrangos diegimas).
Tinklo ir komunikacijos sauga	Tinklo ir komunikacijos sauga yra ypač svarbi, siekiant užtikrinti asmens duomenų saugą (tiek vidinių, tiek išorinių tinklų). Komunikacijai naudojamose susirašinėjimo programose, esant galimybei, rekomenduojama aktyvuoti ištisinio šifravimo (angl. *End-to-end encryption*) nuostatas.
Atsarginės kopijos	Atsarginių kopijų sistema yra esminis veiksnys, užtikrinantis organizacijos darbo ir procesų atstatymą, įvykus duomenų praradimui ar sugadinimui. Duomenų kopijų darymo dažnumas ir poreikis priklauso nuo organizacijos ir joje tvarkomų asmens duomenų. BDAR 32 straipsnis numato „gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“.
Mobilieji, nešiojamieji įrenginiai	Mobilieji, nešiojamieji įrenginiai gali išplėsti paslaugas, kurias teikia duomenų valdytojas, tačiau padidina juose esančių duomenų nutekėjimo riziką. Mobiliuosius ir nešiojamuosius įrenginius, tokius kaip išmanieji telefonai ar planšetiniai kompiuteriai, naudotojai gali panaudoti savo asmeninėms reikmėms, todėl reikia užtikrinti, kad naudotojų asmens duomenys ir organizacijoje administruojami asmens duomenys nebūtų atskleisti.
Programinės įrangos sauga	Visuose programinės įrangos kūrimo ir administravimo etapuose organizacija turi užtikrinti duomenų saugos laikymąsi, asmens duomenų apsaugą. Projektuojant ir kuriant naujas programinės įrangos sistemas, kuriose numatoma tvarkyti asmens duomenis, būtina laikytis BDAR 25 straipsnyje (Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga – angl. *Privacy by Design and Privacy by Default*) numatytų principų.

Duomenų naikinimas, šalinimas	Pagrindinis duomenų naikinimo tikslas yra negrįžtamas asmens duomenų šalinimas, sunaikinimas be teorinės ir praktinės galimybės juos pakartotinai nuskaityti ar atstatyti. Kai yra šalinama pasenusi, nenaudojama, nebereikalinga techninė įranga, duomenų valdytojas privalo užtikrinti, kad visi prieš tai joje buvę sukaupti asmens duomenys būtų negrįžtamai sunaikinti. Pagal BDAR 5 straipsnį asmens duomenys neturi būti saugomi, kaupiami ilgiau, negu tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi. Kai kuriais atvejais duomenų subjektai turi teisę reikalauti duomenis sunaikinti anksčiau, negu yra nustatytas duomenų saugojimo, kaupimo terminas.
Fizinė sauga	Fizinė apsauga yra ne mažiau svarbi, negu technologinės saugumo priemonės, nes tiesioginės fizinės prieigos kontrolė prie IT infrastruktūros yra visos taikomos saugos strategijos pagrindas.

Šaltinis: sudaryta autoriaus pagal Valstybinės duomenų apsaugos inspekcijos parengtos gairės

7. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (žr. 7 lentelę).

7 lentelė. Bendrojo duomenų apsaugos reglamento reikalavimai

Priemonė	BDAR priemonių detalizavimas
Duomenų apsaugos pareigūno skyrimas	Duomenų valdytojas ir duomenų tvarkytojas paskiria duomenų apsaugos pareigūną, paskelbia jo kontaktinius duomenis bei praneša juos priežiūros institucijai.
Duomenų apsaugos pareigūno statusas	Duomenų valdytojas ir tvarkytojas užtikrina, kad duomenų apsaugos pareigūnas būtų tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų nagrinėjimą. Duomenų apsaugos pareigūnas gali vykdyti kitas užduotis ir pareigas, tačiau turi nekilti interesų konfliktas.
Duomenų apsaugos pareigūno užduotys	Duomenų apsaugos pareigūnas atlieka BDAR 39 nurodytas užduotis.
Poveikio duomenų apsaugai vertinimas	Tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą.
Išankstinės konsultacijos	Duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, konsultuojasi su priežiūros institucija, jeigu tvarkant duomenis kiltų didelis pavojus.

Duomenų tvarkymo veiklos įrašai	Kiekvienas duomenų valdytojas ir, kai taikoma, duomenų valdytojo atstovas tvarko duomenų tvarkymo veiklos, už kurią jis atsako, įrašus.
Duomenų subjekto teisės	Duomenų valdytojas ir tvarkytojas privalo užtikrinti BDAR III skyriuje nurodytas duomenų subjekto teises.
Pranešimas priežiūros institucijai apie asmens duomenų saugumo pažeidimą	- Asmens duomenų saugumo pažeidimo atveju duomenų valdytojas nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip per 72 valandoms nuo tada, kai jis sužino apie asmens duomenų saugumo pažeidimą, apie tai praneša priežiūros institucijai. Visus asmens duomenų saugumo pažeidimus dokumentuoja.
Pranešimas duomenų subjektui apie asmens duomenų saugumo pažeidimą	Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nepagrįstai nedelsdamas praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui.
Tvarkymo teisėtumas	Duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šių sąlygų nurodytų BDAR 6 straipsnyje.
Sutikimo sąlygos	Duomenų valdytojas turi galėti įrodyti, kad duomenų subjektas davė sutikimą, kad būtų tvarkomi jo asmens duomenys. Prašymas duoti sutikimą yra aiškiai atskirtas nuo kitų klausimų, pateiktas suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba. Duomenų subjektas turi teisę bet kuriuo metu atšaukti savo sutikimą. sutikimas duodamas laisva valia.
Specialių kategorijų asmens duomenų tvarkymas	Duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šių sąlygų nurodytų BDAR 9 straipsnyje.
Skaidrus informavimas	Duomenų valdytojas imasi tinkamų priemonių, kad visą BDAR 13 ir 14 straipsniuose nurodytą informaciją ir visus pranešimus pagal BDAR 15–22 ir 34 straipsnius, susijusius su duomenų tvarkymu, duomenų subjektui pateiktų glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba.
Duomenų valdytojo atsakomybė	Atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis BDAR.
Duomenų tvarkytojas	Duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų BDRA reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga. Duomenų tvarkytojo atliekamas duomenų tvarkymas reglamentuojamas sutartimi ar kitu teisės aktu.

Šaltinis: sudaryta autoriaus pagal Bendrąjį duomenų apsaugos reglamentą

3 PRIEDAS

Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio empirinio tyrimo klausimynas

Gerbiamas eksperte, dėkoju Jums, kad sutikote dalyvauti mano atliekamame moksliniame tyrime, kuris organizuojamas rengiant daktaro disertaciją tema „*Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis*“. Empirinio tyrimo metu surinkta informacija, neatskleidžiant arba atskleidžiant (jeigu to pageidaujama) respondentų tapatybę, bus apibendrinta ir paskelbta rengiamoje disertacijoje.

Empirinis tyrimas yra suskirstytas į dvi logines dalis:

- Pirmoji dalis (I – III klausimai) remiasi atlikta moksline literatūros analize. Jums bus pateikti klausimai apie asmens duomenų apsaugą ir kibernetinį saugumą bei įgyvendinimo problematiką.
- Antroji dalis (IV – VI klausimai) remiasi empirinių tyrimų gautais rezultatais.

Tyrimo tikslas – sužinoti ekspertų nuomonę apie asmens duomenų apsaugą ir kibernetinį saugumą bei jo įgyvendinimo problematiką, siekiant sukurti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį, atsižvelgiant į tyrimo metu gautus respondentų atsakymus.

Dėkoju už Jūsų skirtą laiką
Aurimas Šidlauskas

I. **Klausimas. Asmens duomenų apsaugos, kaip reiškinio, teorinis pagrindimas:**
   1. Kokią reikšmę asmens duomenų apsaugos įgyvendinimas turi kibernetiniam saugumui?
   2. Kokią įtaką asmens duomenų apsauga turi organizacijai?
   3. Kaip tobulintumėte duomenų apsaugos pareigūno funkcijas, siekiant užtikrinti asmens duomenų apsaugą organizacijoje?
   4. Kokių veiksmų privalo imtis organizacija, siekdama patobulinti savo valdymo procesus asmens duomenų apsaugos reiškinio kontekste?

II. **Klausimas. Kibernetinio saugumo, kaip reiškinio, teorinis pagrindimas:**
   1. Kokią reikšmę kibernetinio saugumo įgyvendinimas turi asmens duomenų apsaugai?
   2. Kokią įtaką organizacijai turi kibernetinio saugumo:
      - Teisinis reglamentavimas.

- Priežiūros institucijos (Nacionalinis kibernetinio saugumo centras) veikla.
- Valdymo procesai.
- Kultūra.
- Komunikacija.

3. Kaip tobulintumėte informacijos saugos įgaliotinio funkcijas, siekiant užtikrinti kibernetinį saugumą organizacijoje?

III. **Klausimas. Asmens duomenų apsaugos ir kibernetinio saugumo įgyvendinimo problematika:**

1. Dėl kokių priežasčių daugelis organizacijų turi formaliai apsibrėžę saugos procesus, gaires?
2. Dėl ko kai kurios organizacijos nesilaiko pagrindinių asmens duomenų tvarkymo principų?
3. Kas lemia, kad organizacijos norėdamos užtikrinti asmens duomenų apsaugą ir kibernetinį saugumą daugiau investuoja į technines priemones, o ne į organizacines?
4. Kaip vertinate Valstybinės duomenų apsaugos inspekcijos darbą užtikrinant kontrolę Bendrojo duomenų apsaugos reglamento reikalavimų įgyvendinimo kontekste?
5. Kaip vertinate Nacionalinio kibernetinio saugumo centro darbą užtikrinant kontrolę kibernetinio saugumo reikalavimų įgyvendinimo kontekste?

IV. **Klausimas. Kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymo ir imties nustatymas:**

1. Kokių techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos įgyvendinimo priemonių pasigendate nacionaliniuose teisės aktuose?
2. Kaip tobulintumėte techninių ir organizacinių kibernetinio saugumo ir asmens duomenų apsaugos priemonių įgyvendinimo procesą organizacijoje?

V. **Klausimas. Informacinių technologijų saugos atitikties vertinimas:**

1. Kaip užtikrinti nuolatinį kibernetinio saugumo ir asmens duomenų apsaugos dokumentacijos peržiūros ir, esant poreikiui, atnaujinimo procesą?
2. Kokios priežastys lemia, kad kai kurios organizacijos periodiškai neatlieka rizikos ir atitikties vertinimų, kaip būtų galima tobulinti šias priemones?
3. Kaip turėtų būti organizuojamas kibernetinio saugumo ir asmens duomenų apsaugos mokymo procesas organizacijoje?
4. Kaip užtikrinti/kontroliuoti paslaugų teikėjų atitiktį kibernetinio saugumo ir asmens duomenų apsaugos reikalavimams?

VI. **Klausimas. Asmens duomenų tvarkymo teisėtumo nustatymas:**

1. Dėl ko daugelis organizacijų neteisėtai tvarko interneto svetainių slapukus (angl. *Cookies*)?
2. Kaip paskatinti organizacijas tvarkyti interneto svetainių slapukus teisėtai?

MYKOLO ROMERIO UNIVERSITETAS

Aurimas Šidlauskas

ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE SISTEMOS MODELIS

Mokslo daktaro disertacijos santrauka
Socialiniai mokslai, vadyba (S 003)

Vilnius, 2024

Mokslo daktaro disertacija rengta 2019–2023 metais Mykolo Romerio universitete pagal Vytauto Didžiojo universitetui su Klaipėdos universitetu, Mykolo Romerio universitetu ir Vilniaus universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 suteiktą doktorantūros teisę.

Mokslinis vadovas:
prof. dr. Tadas Limba (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija ginama Vytauto Didžiojo universiteto, Klaipėdos universiteto, Mykolo Romerio universiteto ir Vilniaus universiteto Šiaulių akademijos vadybos mokslo krypties taryboje:

Pirmininkas:
prof. dr. Andrius Stasiukynas (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Nariai:
prof. dr. Vida Davidavičienė (Vilniaus Gedimino technikos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Fernando Galindo (Saragosos universitetas, Ispanijos Karalystė, socialiniai mokslai, teisė, S 001);
prof. dr. Ligita Šimanskienė (Klaipėdos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Jan Žukovskis (Vytauto Didžiojo universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija bus ginama viešame Vadybos mokslo krypties tarybos posėdyje 2024 m. gegužės 10 d. 9.00 val. Mykolo Romerio universitete, I-414 auditorijoje.
Adresas: Ateities g. 20, Vilnius.

Aurimas Šidlauskas

ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE SISTEMOS MODELIS

SANTRAUKA

Tyrimo aktualumas ir naujumas. Sparti technologinė plėtra dėl skaičiavimo galios progreso, padidėjusių duomenų saugojimo kiekių ir pažangesnio tinklo technologijos leidžia organizacijoms rinkti ir apdoroti vis didesnius duomenų kiekius. Žinių ekonomikoje duomenys tapo svarbia konkurencinio pranašumo kūrimo dalimi. Organizacijos, kurios nesugeba tinkamai apsaugoti asmens duomenų, gali prarasti vartotojų pasitikėjimą, kuris yra būtinas skatinant žmones naudotis naujais gaminiais ir paslaugomis. Asmens duomenų apsauga yra svarbus mokslinių tyrimų objektas, nes egzistuoja platus interpretavimo laukas, kaip ir kokiomis priemonėmis organizacijos turėtų apsaugoti asmens duomenis. Netinkamas asmens duomenų tvarkymas organizacijoms kelia finansinę, teisinę ir reputacijos riziką, todėl organizacijos, tvarkančios ES piliečių asmens duomenis privalo įgyvendinti ir užtikrinti Bendrojo duomenų apsaugos reglamento atitikties reikalavimus.

Šiuolaikinių organizacijų valdymo neįmanoma įsivaizduoti be informacinių technologijų ir informacinių sistemų bei interneto prieigos. Interneto, informacinių technologijų plėtra, informacijos perkėlimas į elektroninę erdvę didina informacinių procesų ir veiklos kokybę. Nors naujos technologijos ir paslaugos yra naudingos tiek verslui, tiek vartotojams, tačiau jos taip pat kelia rimtą pavojų kibernetiniam saugumui. Pasaulyje kiekvienais metais didėjant kibernetinių incidentų skaičiui, kibernetinis saugumo aktualumas didėja. Tai nėra tik technologinė problema, nes didžiąją daugumą kibernetinio saugumo problemų sukuria ne technologijos, o žmonės. Dažnai tai yra tyčiniai, gerai apgalvoti, tikslingai orientuoti į siekiamus tikslus, aukštos kvalifikacijos reikalaujantys veiksmai. Nėra universalaus sprendimo, siekiant užtikrinti kibernetinį saugumą, todėl svarbiomis tampa kompleksinės priemonės, apimančios nacionalinį reguliavimą, organizacijos vidaus politiką ir sėkmingų tarptautinių praktikų atkartojimą. Absoliutaus kibernetinio saugumo pasiekti neįmanoma, bet tinkamai parinktos ir taikomos saugumo priemonės, procedūros ir procesai gali sumažinti rizikos laipsnį ir praradimų mastą.

Organizacijos, norėdamos užtikrinti asmens duomenų apsaugą, yra privestos keisti, tobulinti duomenų tvarkymo procesus ir procedūras bei taikyti kibernetinio saugumo priemones. Bendrajame duomenų apsaugos reglamente nėra įvardyta, kokios kibernetinio saugumo priemonės yra tinkamos. Asmens duomenų apsauga yra aktuali ir svarbi šiandienos problematika, todėl tinkamų kibernetinio saugumo priemonių taikymas svarbus tiek teorine, tiek praktine prasme. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis leistų numatyti ir sumažinti galimas asmens duomenų apsaugos ir kibernetinio saugumo rizikas.

Apibendrinant disertacijoje analizuotus informacijos šaltinius galima teigti, kad mokslinėje literatūroje tyrėjai atkreipia dėmesį į tokias asmens duomenų apsaugos ir kibernetinio saugumo sąveikos reiškinio problematikas: kokie pagrindiniai asmens duomenų apsaugos ir kibernetinio saugumo reikalavimai; kokios pagrindinės asmens duomenų apsaugos ir kibernetinio saugumo užtikrinimo interpretacijos; koks duomenų apsaugos pareigūno vaidmuo organizacijoje; kaip valdyti asmens duomenų saugumo pažeidimą ir kibernetinį incidentą; kaip asmens duomenų saugaus valdymo elektroninėje erdvėje priemonės gali sumažinti asmens duomenų pažeidimo ir kibernetinio incidento rizikas; ir kt. Verta pastebėti, kad asmens duomenų apsaugos ir kibernetinio saugumo užtikrinimo organizacijose vertinimo tyrimai nėra išplėtoti. Taigi asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos priemonės vertinimo aspektu yra aktualus tyrimų objektas tiek teoriniu, tiek ir praktiniu požiūriais, jo platesniam pažinimui ir skiriamas šis disertacinis darbas.

Temos ištirtumo lygis. Pasaulio ir Lietuvos mokslininkai, tarptautinės ir Lietuvos organizacijos kibernetinį saugumą ir asmens duomenų apsaugą nagrinėja įvairiais aspektais.

Asmens duomenų apsaugą, kaip reiškinį, nagrinėjo: Tikkinen-Piri, 2018; Cortez, 2021; Voigt, Von dem Bussche, 2017; Kamleitner, Mitchell, 2018; Cabral, 2021; Malinauskaitė-van de Castel, 2017; Zaleskis, 2019; Limba, Šidlauskas, 2020; Tamavičiūtė, 2019; Diker Vanberg, Ünver, 2017; Ooijen, Vrabec, 2019; Feth, 2020; Sánchez, ir kt. 2021; Dibble, 2019; Gobeo ir kt., 2018; Alkhaledi, Hawamdeh, 2020; Teixeira, 2019; Europos komisija (EK), 2020; Andrijauskas, Morkūnienė, 2020; Europos duomenų apsaugos valdyba; Alford, 2020; Gabel, Hickman, 2019; Presthus, Sønslien, 2021; Piras, 2019.

Kibernetinį saugumą, kaip reiškinį, nagrinėjo: Bayne, 2008; Jastiuginas, 2011; Asquith, Morgan, 2020; Möller, 2020; Nacionalinis kibernetinio saugumo centras (NKSC), Solms, von Solms, 2018; Štitilis, 2016; Horák, 2019; National Institute of Standards and Technology (NIST); International Organization for Standardization (ISO); Schreider, 2020; Raval, 2018; Corradini, 2020; Esparza, 2020; Thiéry, Fass, 2020; Chang, 2020; Wu, 2020; Reeves, 2020; Schreider, 2017; Agafonov, 2021; Hooper, McKissack, 2016; Ritchey, 2020; Maurer, 2021; Blum, 2020; Harknett, Grincevičius, 2019.

Asmens duomenų apsaugos priemones nagrinėjo: Štarchoň, Pikulík, 2019; Blanco-Lainé, 2019; Grütter, Schneider, 2019; Bock, 2021; Chassang, 2017; Valstybinė duomenų apsaugos inspekcija (VDAI); Pandit, 2019; Helbing, 2022; Hilberg, 2022; Valstybės kontrolė (VK); Drewer, 2018; Felici, 2013; Freitas, Silva, 2018; Mouratidis, 2016; Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA); International Organization for Standardization (ISO); Ryan, 2020; Haes, 2013; Demetzou, 2018; Europos duomenų apsaugos valdyba; Aven, 2016; Shimonski, 2016; Gibson, 2014; Tikkinen-Piri, 2018; Barnard-Wills, 2019; Perry, 2019; Werner, 2020; Carey, 2019; Tiliute, 2019; Harkous, 2018; Linden, 2018; Wolford, 2022; Degeling, 2018; Eijk, 2019; Nouwens, 2020; SANS institutas.

Kibernetinio saugumo priemones nagrinėjo: Cheng, 2020; Alghamdi, 2021; Ghelani, 2022; Kahyaoglu, Caliyurt, 2018; Lubua, Pretorius, 2019; Aliyeva, Hwang, 2019;

Patterson, 2017; Koskelo, 2020; Wang, 2018; Cabaj, 2018; Hooper, McKissack, 2016; Kaselis, Pivoras, 2012; Scarfone, 2021; Buccafurri, 2015; Chapple, 2018; Gollmann, 2015; Menard, 2017; Kovács, 2018; Cains ir kt., 2022; Rea-Guaman, 2020; Black, 2018; Fielder, 2018; Claroty, 2021; Zimmermann, Renaud, 2019; Chowdhury, 2019; Chochlova, 2022; Dean, McDermott, 2017; Aldawood, 2020; Lois, 2020; Fernando, 2017; Bisson, 2021; Aoyama, 2015; Baig, 2022; George, 2021; Mandritsa, 2018.

Mokslinė problema – Koks turi būti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, siekiant sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas?

Mokslinio tyrimo objektas – Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio priemonės.

Mokslinio tyrimo tikslas – parengti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį, kuris padėtų sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas.

Siekiant iškelto tikslo, disertacijoje sprendžiami tokie uždaviniai:

1. Išanalizuoti asmens duomenų apsaugos ir kibernetinio saugumo sąveikos teorinius aspektus.
2. Atlikti kokybinius dokumentų analizės, atvejo analizės ir ekspertų nuomonės tyrimus, kuriais remiantis būtų nustatyti asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių kriterijai modeliui sukurti.
3. Pasiūlyti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį.
4. Įvertinti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkius ir galimybes.

Mokslinio tyrimo metodai ir pagrindiniai šaltiniai. Siekiant iškelto tikslo ir sprendžiant iškeltus uždavinius disertacijos teorinėje dalyje atliekama mokslinės literatūros šaltinių sisteminė lyginamoji analizė ir apibendrinimas. Rengiant disertacijos empirinę dalį pasitelkta atvejo studija, taikomi vienas kitą papildantys kokybiniai empiriniai tyrimai: dokumentų analizė, ekspertinis interviu, kokybinė turinio analizė, antrinių šaltinių duomenų analizė. Empirinė tyrimo dalis grindžiama teorinėje dalyje išdėstytomis įžvalgomis ir remiamasi interpretacinės paradigmų teorinėmis prielaidomis.

Disertacijos ginamieji teiginiai:

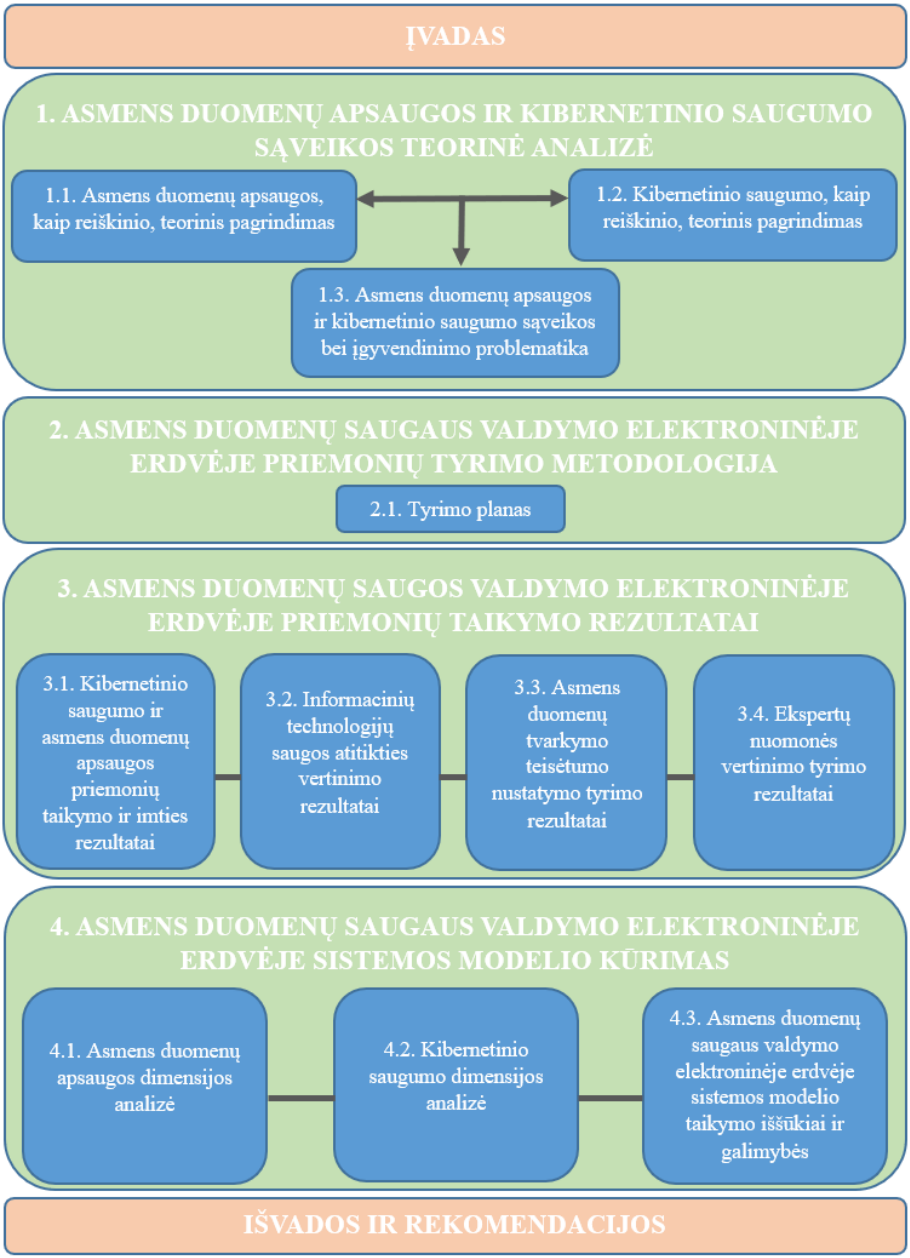
1. Kibernetinis saugumas yra asmens duomenų apsaugos dalis.
2. Kibernetinio saugumo užtikrinimas neapsaugo nuo rizikos įvykti asmens duomenų saugumo pažeidimui.
3. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis sumažina riziką įvykti asmens duomenų saugumo pažeidimui ir kibernetiniam incidentui.

Tyrimo teorinis ir praktinis reikšmingumas. Sukurtas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, kurio asmens duomenų apsaugos ir kibernetinio saugumo dimensijose nagrinėjamos įvairios asmens duomenų saugaus valdymo priemonės, kurių tikslas yra sumažinti asmens duomenų saugumo pažeidimo

ir kibernetinio saugumo rizikas, siekiant užtikrinti elektroninės informacijos, įskaitant duomenis ir asmens duomenis, prieinamumą, vientisumą bei konfidencialumą bet ir užtikrinti pagrindinius asmens duomenų tvarkymo principus, apsaugant fizinių asmenų teises ir laisves dėl asmens duomenų tvarkymo.

Pažymėtina, kad šį asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį galės naudoti visos organizacijos, valdančios arba tvarkančios asmens duomenis, kurios siekia pagerinti asmens duomenų apsaugą ir kibernetinį saugumą bei jų valdymą ir sumažinti asmens duomenų saugumo pažeidimo ir kibernetinio saugumo incidento rizikas. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelyje kiekviena tiek asmens duomenų apsaugos, tiek kibernetinio saugumo dimensijos priemonė, nuo I iki III lygio, galės būti įgyvendinama atskirai, atsižvelgiant į organizacijos veiklos ypatumus, valdomus išteklius, turimus resursus bei finansines galimybes. Tačiau asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio IV lygmuo bus siejamas su visų asmens duomenų apsaugos ir kibernetinio saugumo dimensijose išvardintų priemonių įgyvendinimu, siekiant virsmo į integruotą asmens duomenų apsaugos ir kibernetinio saugumo valdymo sistemą, kurioje priemonės yra susietos bei veiks viena kitą papildydamos.

Darbo struktūra. *Darbo pradžioje* yra pateikiamas įvadas. Darbą sudaro keturios dalys. *Pirmoje dalyje* yra nagrinėjama asmens duomenų apsaugos ir kibernetinio saugumo sąveikos teorinė analizė: Asmens duomenų apsaugos, kaip reiškinio, teorinis pagrindimas; Kibernetinio saugumo, kaip reiškinio, teorinis pagrindimas; Asmens duomenų apsaugos ir kibernetinio saugumo sąveikos bei įgyvendinimo problematika. *Antroje dalyje* yra pristatoma asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių tyrimo metodologija: Tyrimo planas. *Trečioje dalyje* yra pateikti asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių taikymo rezultatai: Kibernetinio saugumo ir asmens duomenų apsaugos priemonių taikymo ir imties rezultatai; Informacinių technologijų saugos atitikties vertinimo rezultatai; Asmens duomenų tvarkymo teisėtumo nustatymo tyrimo rezultatai; Ekspertų nuomonės vertinimo tyrimo rezultatai. *Ketvirtoje dalyje* yra atliekamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio kūrimas: Asmens duomenų apsaugos dimensijos analizė; Kibernetinio saugumo dimensijos analizė; Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkiai ir galimybės. *Darbo pabaigoje* yra pateikiamos išvados ir rekomendacijos (žr. 1 pav.).



1 pav. Disertacinio darbo struktūros loginė schema

Šaltinis: sudaryta autoriaus

PIRMOSIOS DALIES APŽVALGA: ASMENS DUOMENŲ APSAUGOS IR KIBERNETINIO SAUGUMO SĄVEIKOS TEORINĖ ANALIZĖ

Pirmajame poskyryje yra aptariama asmens duomenų apsaugos, kaip reiškinio, svarba organizacijoms ir asmenims šiuolaikiniame pasaulyje. Nagrinėjama asmens duomenų samprata, klasifikavimas ir jų tvarkymo pagrindai bei pagrindiniai principai. Pastebėtina, kad asmens duomenys tapo labai vertingu organizacijų, duomenų valdytojų ir tvarkytojų, turtu, kuris dažnai yra pagrindas teikti ir vystyti paslaugas. Pažymėtina, kad organizacijoms tvarkant asmens duomenis turėtų būti svarbūs ne tik jų interesai, bet ir duomenų subjektų, t. y. asmenų, kurių asmens duomenis jos tvarko, nes įsigaliojus Reglamentui už netinkamą asmens duomenų tvarkymą gali kilti atsakomybė – teisinė, finansinė, reputacijos. Atlikta duomenų apsaugos pareigūno organizacijoje ir duomenų apsaugos priežiūros institucijos vaidmenų analizė.

Antrajame poskyryje yra aptariamas kibernetinio saugumo, kaip reiškinio, svarba organizacijoms ir asmenims šiuolaikiniame pasaulyje. Nagrinėjama kibernetinio saugumo samprata, turinys ir principai. Pažymėtina, kad kibernetinis saugumai – tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama užtikrinti IS ir jose tvarkomos elektroninės informacijos prieinamumą, vientisumą ir konfidencialumą. Išanalizuoti kibernetinio saugumo politikos įgyvendinimo organizacijose aspektai. Lietuvoje kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato LR Vyriausybė. LR KAM kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja. Kibernetinio saugumo politiką įgyvendina NKSC, VDAI, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu. Pagrindžiama, kad Lietuvoje kibernetinio saugumo valdymo sistema nepakankamai veiksminga, tobulintinas kibernetinių incidentų valdymas, neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas.

Trečiajame poskyryje aptariama asmens duomenų apsaugos ir kibernetinio saugumo sąveikos bei įgyvendinimo problematika. Nurodoma, kad kibernetinio saugumo priemonės yra viena iš būtinų sąlygų užtikrinti asmens duomenų apsaugą. Asmens duomenų apsaugos reikalavimai yra labai abstraktūs, juos galima įvairiai interpretuoti, kiekviena organizacija turi savo būdą, kaip užtikrinti pagrindinius asmens duomenų principus ir įrodyti atitiktį reikalavimams.

ANTROSIOS DALIES APŽVALGA: ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE PRIEMONIŲ TYRIMO METODOLOGIJA

Pirmajame poskyryje yra aptariamas tyrimo planas. Tyrimo metodologija remiasi keliais tyrimų metodais, kurie padidina tyrimo rezultatų tikslumą, pagerina atskirų metodų ribotą pritaikomumą bei padeda užčiuopti silpnai išreikštus reiškinius. Norint pasiekti pagrindinį tyrimo tikslą buvo atlikti keturi tyrimai:

Pirmasis tyrimas. Naudojant dokumentų analizės metodą siekiama nustatyti: Kokios yra privalomos kibernetinio saugumo ir asmens duomenų apsaugos priemonės bei jų taikymo imtis Lietuvoje. Tyrimo metu bus sudarytas svarbiausių kibernetinio saugumo ir asmens duomenų srities teisės aktų, standartų ir gairių sąrašas su juose įtvirtintais reikalavimais ir/ar kontrolės priemonėmis, kurios išskirtos į organizacines ir technines.

Antrasis tyrimas. Naudojant atvejo analizės metodą, šis tyrimas yra skirtas atlikti organizacijų informacinių technologijų saugos atitikties teisės aktų, reglamentuojančių kibernetinį saugumą ir asmens duomenų apsaugą, standartams ir gairėms, vertinimą, siekiant nustatyti pagrindines neatitiktis ir jų keliamas grėsmes organizacijų kibernetiniam saugumui ir asmens duomenų apsaugai.

Trečiasis tyrimas. Naudojant atvejo analizės ir lyginamąjį metodą siekiama nustatyti organizacijų asmens duomenų, konkrečiai slapukų (angl. *Cookies*) naudojimo teisėtumą interneto svetainėse. Šio tyrimo metu gauti rezultatai palyginti su anksčiau t. y. 2020 metais atliktu tyrimu, siekiant įvertinti, kaip pakito situacija, ar organizacijos skiria daugiau dėmesio asmens duomenų apsaugai.

Ketvirtasis tyrimas. Naudojant ekspertų interviu metodą buvo atliktas pusiau struktūruotas interviu, kurio metu buvo apklausti 9 ekspertai, siekiant sužinoti jų nuomonę apie asmens duomenų saugaus valdymo elektroninėje erdvėje priemones ir jų taikymą. Apdorojant gautus duomenis, remiamasi turinio (angl. *Content*) analize.

TREČIOSIOS DALIES APŽVALGA: ASMENS DUOMENŲ SAUGOS VALDYMO ELEKTRONINĖJE ERDVĖJE PRIEMONIŲ TAIKYMO REZULTATAI

Pirmajame poskyryje nustatytos kibernetinio saugumo ir asmens duomenų apsaugos priemonės ir jų taikymo imtis. Pažymėtina, kad visos organizacijos privalo užtikrinti atitiktį asmens duomenų apsaugos reikalavimams, kurie įpareigoja duomenis tvarkyti pagal pagrindinius asmens duomenų tvarkymo principus ir taikyti tinkamas technines ir organizacines apsaugos priemones.

Antrajame poskyryje atlikti trijų organizacijų informacinių technologijų saugos atitikties vertinimai tarptautinių ir nacionalinių teisės aktų, standartų ir gairių reglamentuojančių elektroninės kibernetinį saugumą ir asmens duomenų apsaugą, reikalavimams ir pateiktos rekomendacijos nustatytoms neatitiktims pašalinti. Nustatyta, kad organizacijos periodiškai neatnaujina saugos dokumentų, neatlieka rizikos vertinimų ir informacinių technologijų saugos atitikties vertinimų, nerengia mokymų, neatlieka veiklos tęstinumo valdymo plano išbandymo pratybų ir neužtikrina trečiųjų šalių paslaugų tiekėjų kontrolės.

Trečiajame poskyryje nustatytas 100 populiariausių Lietuvos interneto svetainių asmens duomenų tvarkymo teisėtumas naudojant slapukus. Pažymėtina, kad organizacijos rinkti slapukus interneto svetainėse gali tik gavusios vartotojo sutikimą.

Ketvirtajame poskyryje gauti ir išanalizuoti 9 ekspertų atsakymai apie asmens duomenų apsaugos ir kibernetinio saugumo priemones ir jų įgyvendinimo problematiką.

KETVIRTOSIOS DALIES APŽVALGA: ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE SISTEMOS MODELIO KŪRIMAS

Ketvirtame skyriuje kuriamas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis. Siekiant supaprastinti šio asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio įdiegimą organizacijoje, yra numatomas modelio priemonių įgyvendinimas pakopomis, išskiriant keturis asmens duomenų apsaugos ir kibernetinio saugumo valdymo modelio lygius – supratimo (I lygis), įgyvendinimo (II lygis), užtikrinimo/ tobulinimo (III lygis), integruotąjį (IV lygis). Pateikiamas asmens duomenų asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis (žr. 2 pav.).

Pirmame poskyryje analizuojamos pateikto asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio asmens duomenų apsaugos dimensijos aštuonios priemonės.

Antrame poskyryje analizuojamos pateikto asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio aštuonios kibernetinio saugumo dimensijos priemonės.

Trečiame poskyryje vertinami asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkiai ir galimybės. Pažymėtina, kad asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelyje neįmanoma išskirti vienos pačios svarbiausios priemonės, kadangi tik visų priemonių taikymas organizacijoje sujungiant asmens duomenų apsaugos ir kibernetinio saugumo dimensijas į vieną bendrą organizacijos valdymo sistemą gali parodyti aiškius asmens duomenų apsaugos ir kibernetinio saugumo pokyčio rezultatus. Kaip ir buvo minėta anksčiau, kiekviena tiek asmens duomenų apsaugos, tiek kibernetinio saugumo dimensijos priemonė gali būti įgyvendinama atskirai, atsižvelgiant į organizacijos veiklos ypatumus, valdomus išteklius, turimus resursus bei finansines galimybes. Tačiau būtina pažymėti, kad asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio ketvirtasis lygmuo yra siejamas su visų asmens duomenų apsaugos ir kibernetinio saugumo dimensijose išvardintų priemonių įgyvendinimu, siekiant virsmo į integruotą asmens duomenų apsaugos ir kibernetinio saugumo valdymo sistemą, kurioje priemonės yra susietos bei veikia viena kitą papildydamos.

Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis

2 pav. Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis

Šaltinis: sudaryta autoriaus

IŠVADOS

1-asis uždavinys. Atlikus asmens duomenų apsaugos ir kibernetinio saugumo sąveikos teorinių aspektų analizę, nustatyta:

1. Organizacijoms valdančioms arba tvarkančioms asmens duomenis, kurie buvo anonimizuoti asmens duomenų apsaugos reikalavimai netaikomi. Tačiau pseudonimizuoti duomenys visiškai patenka į asmens duomenų apsaugos taikymo sritį, lyg asmens duomenys, nes pseudonimizacija nepašalina visos asmens identifikavimo informacijos iš duomenų, o tik sumažina duomenų rinkinio susiejimą su asmeniu. Įvykus kibernetiniam incidentui arba asmens duomenų saugumo pažeidimui, kuomet tvarkomi anonimizuoti ir pseudonimizuoti duomenys, mažėja žala asmens duomenų subjektams apsaugant jų teises į privatumą.
2. Duomenų subjektai turi asmens duomenų apsaugos reglamente įtvirtintas specifines teises, įgalinančias juos kontroliuoti savo asmens duomenimis, kuriuos valdo ir tvarko organizacijos.
3. Duomenų apsaugos pareigūnas užtikrina, kad organizacijoje būtų tinkamai įgyvendinami asmens duomenų apsaugos reikalavimai, tačiau atsakomybė už šių reikalavimų nesilaikymą yra priskiriama duomenų valdytojui ir (ar) tvarkytojui.
4. Absoliutaus asmens duomenų apsaugos ir kibernetinio saugumo pasiekti neįmanoma, bet tinkamai parinktos ir taikomos saugumo priemonės gali sumažinti rizikos laipsnį ir praradimų mastą.

2-asis uždavinys. Atlikus kokybinius dokumentų analizės, atvejo analizės ir ekspertų nuomonės tyrimus, kuriais remiantis būtų nustatyti asmens duomenų saugaus valdymo elektroninėje erdvėje priemonių kriterijai modeliui sukurti, galima daryti išvadas:

5. Skirtinguose teisės aktuose ir standartuose ISO 27001 ir ISO 27002 bei VDAI gairėse tam tikri išdėstyti reikalavimai kibernetiniam saugumui ir asmens duomenų apsaugai užtikrinti yra tapatūs, tai apsunkina šių reikalavimų įgyvendinimą organizacijoms.
6. Įvertinus trijų organizacijų kibernetinio saugumo ir asmens duomenų apsaugos reglamentavimą vidaus teisės aktuose ir faktinį jų įgyvendinimas praktikoje, nustatyta, kad organizacijos periodiškai neatnaujina saugos dokumentų, neatlieka rizikos vertinimų ir informacinių technologijų saugos atitikties vertinimų, nerengia mokymų, neatlieka veiklos tęstinumo valdymo plano išbandymo pratybų ir neužtikrina trečiųjų šalių paslaugų tiekėjų kontrolės.
7. Įvertinus 100 populiariausių Lietuvos interneto svetainių, didžioji dauguma organizacijų, valdančių arba tvarkančių asmens duomenis (slapukus), nesilaiko asmens duomenų apsaugos reikalavimų ir slapukus interneto svetainėse naudoja neteisėtai, t. y. be vartotojų sutikimo ir nepateikdama svarbiausios informacijos apie jų tvarkymą privatumo politikoje.
8. Atlikus 9 ekspertų nuomonės vertinimą nustatyta, kad:

4.1. Kibernetinis saugumas yra neatsiejamas nuo asmens duomenų apsaugos, nes daugelis asmens duomenų apsaugą užtikrinančių priemonių yra kibernetinio saugumo organizacinės ir techninės priemonės.
4.2. Organizacijos nenorą investuoti į asmens duomenų apsaugą ir kibernetinį saugumą gali lemti kelios priežastys – nėra žinoma (sunkiai pamatuojama) investicijų grąža, galimas darbo produktyvumo sumažėjimas ir tolerancija rizikoms bei požiūris į jas, kad jos nesumažės.
4.3. Organizacijos prioritetą dažnu atveju teikia techninėms, o ne organizacinėms priemonėms, nes technines priemones galima nupirkti ir parodyti, o organizacinės sunkiau įgyvendinamos ir kontroliuojamos.

3-iasis uždavinys. Pasiūlius asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį, galima teigti:

1. Siūlomo asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį sudaro dvi dimensijos – asmens duomenų apsaugos ir kibernetinio saugumo, kuriose nurodytos 16 priemonių, siekiant užtikrinti asmens duomenų apsaugą organizacijoje. Kibernetinio saugumo dimensija yra asmens duomenų apsaugos dimensijos dalis.
2. Asmens duomenų apsaugos dimensija užtikrina teisėtą asmens duomenų tvarkymą ir atitinkamas technines ir organizacines priemones, siekiant apsaugoti pagrindines duomenų subjekto teises ir laisves, visų pirma jų teisę į asmens duomenų apsaugą.
3. Kibernetinio saugumo dimensija užtikrina kibernetinio saugumo valdymą ir atitinkamas technines ir organizacines priemones, siekiant apsaugoti informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumą, vientisumą bei konfidencialumą.
4. Siūlomas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis, suteikia organizacijai galimybę stebėti asmens duomenų apsaugos ir kibernetinio saugumo įgyvendinimo pokyčius pagal priemonių laipsnišką įgyvendinimą, lygiais – supratimo (I), įgyvendinimo (II), užtikrinimo/ tobulinimo (III) ir integruotąjį (IV), konkrečiose dimensijose.

4-asis uždavinys. Įvertinus asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio taikymo iššūkius ir galimybes, nustatyta:

1. Neužtikrinus kibernetinio saugumo kyla rizika įvykti asmens duomenų saugumo pažeidimui, nes asmens duomenys gali būti atskleisti, prarasti ir neprieinami. Tačiau net ir užtikrinus kibernetinį saugumą vis dar kyla rizika įvykti asmens duomenų saugumo pažeidimui, nes asmens duomenys gali būti tvarkomi pažeidžiant pagrindinius asmens duomenų tvarkymo principus. Tik užtikrinus modelyje nurodytas asmens duomenų apsaugos ir kibernetinio saugumo priemones galima užtikrinti asmens duomenų apsaugą, siekiant sumažinti kibernetinių incidentų ir asmens duomenų apsaugos pažeidimų riziką.
2. Įgyvendinant asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelį organizacijos gali susidurti su iššūkiais – kompetencijos ir patirties trūkumu, žmogiškųjų išteklių trūkumu, finansinių išteklių trūkumu,

komunikacijos ir bendradarbiavimo trūkumu, motyvacijos trūkumu ir pasipriešinimu pokyčiams.

3. Kiekviena asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio priemonė gali būti įgyvendinama atskirai, neišskiriant vienos pačios svarbiausios priemonės, atsižvelgiant į organizacijos veiklos ypatumus, valdomus išteklius, turimus resursus bei finansines galimybes. Tačiau asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio IV lygmuo yra siejamas su visų asmens duomenų apsaugos ir kibernetinio saugumo dimensijose išvardintų priemonių įgyvendinimu, siekiant virsmo į integruotą asmens duomenų apsaugos ir kibernetinio saugumo valdymo sistemą, kurioje priemonės yra susietos bei veiks viena kitą papildydamos.

REKOMENDACIJOS

Organizacijoms:

1. Rekomenduojama anonimizuoti ir pseudonimizuoti asmens duomenis siekiant palengvinti asmens duomenų apsaugos reikalavimų įgyvendinimą ir apsaugoti atskirų duomenų subjektų teises į privatumą.
2. Siekiant užtikrinti asmens duomenų subjektų įgyvendinimą, visų pirma glausta ir lengvai suprantama kalba informuoti duomenų subjektus apie jų teises, visų antra sukurti mechanizmus ir procedūras joms įgyvendinti.
3. Rekomenduojama duomenų valdytojui ir (ar) tvarkytojui bendradarbiauti su duomenų apsaugos pareigūnu – kuo ankstyvesniu etapu įtraukti į visus su duomenų apsauga susijusius klausimus ir suteikti reikiamus išteklius atlikti užduotis bei tobulėti. Tuo tarpu duomenų apsaugos pareigūnui atsižvelgiant į organizacijos asmens duomenų pobūdį, aprėptį, kontekstą ir tikslus privaloma įvertinti asmens duomenų tvarkymo rizikas ir informuoti duomenų valdytoją ir (ar) tvarkytoją bei konsultuotis su priežiūros institucija.
4. Siekiant įgyvendinti asmens duomenų apsaugos priemones, kurias taip pat sudaro ir kibernetinio saugumo priemonės, privaloma įsivertinti kokios priemonės yra tinkamos, priklausomai nuo duomenų jautrumo ir rizikos laipsnio, jei asmens duomenys bus pažeisti.
5. Siekiant užtikrinti asmens duomenų apsaugą privaloma įgyvendinti ne tik teisės aktuose nustatytas kibernetinio saugumo technines ir organizacines priemones, bet ir pagrindinius asmens duomenų tvarkymo principus bei gerąją praktiką įtvirtintą standartuose ISO 27001 ir ISO 27002 bei Valstybinės duomenų apsaugos inspekcijos tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėse.
6. Siekiant teisėtai tvarkyti duomenis - slapukus interneto svetainėse, duomenų valdytojas ir (ar) tvarkytojas privalo turėti tinkamą įrankį, kuris vartotojams suteiktų galimybę aktyviais veiksmais sutikti arba nesutikti su atitinkamų slapukų tvarkymu bei bet kada pakeisti apsisprendimą, taip pat pateikti visą informaciją apie slapukų tvarkymą interneto svetainės privatumo politikoje.
7. Rekomenduojama tobulinant veiklos procesus asmens duomenų apsaugos kontekste mąstyti ne apie patogumą, bet apie saugumą vadovaujantis teisės aktais ir visuotinai pripažinta gerąją praktika nustatyta tarptautiniuose standartuose.
8. Techninės priemonės tinkamai neveiks be organizacinių priemonių, todėl privalu ieškoti balanso tarp abiejų priemonių įgyvendinimo.

Vartotojams (duomenų subjektams):

1. Rekomenduojama domėtis kaip organizacijos tvarko jų asmens duomenis ir reikalauti įgyvendinti jų teises asmens duomenų kontekste.
2. Rekomenduojama informuoti priežiūros institucijas – Valstybinę duomenų inspekciją, jeigu įvyko asmens duomenų saugumo pažeidimas ir Nacionalinį kibernetinio saugumo centrą, jeigu įvyko kibernetinis incidentas.

Tolesni tyrimai disertacijos tematika galėtų būti vykdomi:

1. Siekiant įvertinti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio pritaikomumą, gali būti pasitelkti asmens duomenų apsaugos ir kibernetinio saugumo ekspertai.
2. Atskleisti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelio priemonių sąryšius t. y. kaip vienos priemonės įgyvendinimas įtakoja kitą.
3. Remiantis moksliniais tyrimais tobulinti asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelyje išvardintas priemones arba papildyti naujomis.

Mokslinės publikacijos disertacijos tema

1. Limba, T., Šidlauskas, A., Juozėnaitė, E. (2023). **Direct Marketing in Lithuania under GDPR: Consent and Legitimate Interests**, *12th International Conference on Applied Economics Contemporary Issues in Economy*, 99-106. https://doi.org/10.24136/eep.proc.2023.2
2. Šidlauskas, A. (2021). **Valstybinės duomenų apsaugos inspekcijos administracinių baudų skyrimo praktika ES šalių kontekste**. *Socialiniai tyrimai*, 44(2), 153-169. https://doi.org/10.15388/Soctyr.44.2.10
3. Limba, T., Šidlauskas, A. (2021). **Cybersecurity-Related Roles Identification and Alignment**. *In Edulearn21.13th International Conference on Education and New Learning Technology, Online Conference, 5nd-6th of July, 2021, pp.* 7404-7413. https://doi.org/10.21125/edulearn.2021.1500
4. *Šidlauskas, A. (2021).* **The Role and Significance of the Data Protection Officer in the Organization**. *Socialiniai tyrimai*, 44 (1), 8-28. https://www.zurnalai.vu.lt/social-research
5. *Šidlauskas, A. (2021).* **General Data Protection Regulation (GDPR) Awareness Training Opportunities in Lithuania**. *ICERI20: 14th annual International Conference of Education, Research and Innovation, 8th - 9th of November, 2021: Conference Proceedings*, 9158-9166. http://dx.doi.org/10.21125/iceri.2021.2109
6. Limba, T.; Driaunys, M.; Šidlauskas, A. (2021). **Use of Cookies After GDPR: a Case Study of Top Lithuanian Websites**, *Transformations in Business & Economics,* Vol. 20, No. 3 (54): 93-116. http://www.transformations.knf.vu.lt/54/article/useo
7. Limba, T.; Šidlauskas, A. (2020). **Personal Data Processing in Educational Institutions: Anonymisation and Pseudonymisation**. *ICERI20: 13th annual International Conference of Education, Research and Innovation,* 9th - 10th of November, 2020, pp. 9989-9997. http://dx.doi.org/10.21125/iceri.2020.2262
8. *Šidlauskas, A.; Ungurytė-Ragauskienė, S.* (2020). **Iššūkiai Kibernetiniam Saugumui: Socialinė Inžinerija Institucinio Izomorfizmo Kontekste,** *SUSTAINSECURE-2020: 11th International Scientific Conference „Problems of Ensuring Public Security: Theoretical and Practical Aspects"*, 20th-22th of October. https://doi.org/10.13165/PSPO-20-25-26
9. Limba, T.; Driaunys, K.; Kiškis, M.; Šidlauskas, A. (2020). **Development of Digital Contents: Privacy Policy Model under the General Data Protection Regulation and User Friendly Interface**, *Transformations in Business & Economics,* 1(49): 21-42. http://www.transformations.knf.vu.lt/49/article/deve
10. Limba, T.; Šidlauskas, A. (2020). **Consent as a Lawful Basis for Processing Personal Data under the GDPR**. *INTED20: 14th International Technology, Education and Development Conference, Valencia, Spain. 2-4 March, 2020,* 1374-1383. http://dx.doi.org/10.21125/inted.2020.0456

Kitos mokslinės publikacijos ne disertacijos tema

1. Limba, T., Šidlauskas, A., & Juozėnaitė, E. (2022). **The Role of User-generated Content in Brand Communication and the Tactics to Encourage It**. *ICERI2022: 15th annual International Conference of Education, Research and Innovation*, Seville, Spain, 7-9 November, 2022, 865-871. https://dx.doi.org/10.21125/iceri.2022.0262
2. Šidlauskas, A. (2019). **Opportunities for DPO (Data Protection Officer) Occupational Training and Improvement**. *INTED19: 13th International Technology, Education and Development Conference*, Valencia, Spain. 11-13 March, 2019, pp. 808-814. http://dx.doi.org/10.21125/inted.2019.0280
3. Šidlauskas, A. (2019). **Video Surveillance and the GDPR**. *Social Transformations in Contemporary Society (STICS 2019): Proceedings of an Annual International Conference for Young Researchers*, (7), 55-65. https://repository.mruni.eu/handle/007/15840
4. Limba, T.; Šidlauskas, A. (2019). **General Data Protection Regulation Interpretation in Higher Education Institutions**. *EDULEARN19: 11th International Conference on Education and New Learning Technologies*, Palma, Spain. 1-3 July, 2019, pp. 2040-2047. http://dx.doi.org/10.21125/edulearn.2019.0555
5. Limba, T.; Šidlauskas, A. (2018). **Secure Personal Data Administration in the Social Networks: the Case of Voluntary Sharing of Personal Data on the Facebook**, *Entrepreneurship and Sustainability Issues* 5(3): 528-541. https://doi.org/10.9770/jesi.2018.5.3(9)
6. Šidlauskas, A. (2018). **Users Electronic Data Protection Features**. *Social Transformations in Contemporary Society (STICS 2018): Proceedings of Annual International Conference for Young Researchers*, (6), 78-88. https://repository.mruni.eu/handle/007/15344
7. Limba, T.; Šidlauskas, A. (2018). **Peculiarities of anonymous comments' management: a case study of Lithuanian news portals**, *Entrepreneurship and Sustainability Issues* 5(4): 875-889. http://doi.org/10.9770/jesi.2018.5.4(12)
8. Limba, T.; Šidlauskas, A. (2018). **An Analysis of Comments Containing Hate Speech: Facebook and the Delfi News Portal**. *EDULEARN18: 10th International Conference on Education and New Learning Technologies*, Palma, Spain, 2nd–4th of July, 2018, 3413-3419. http://dx.doi.org/10.21125/edulearn.2018.0887

Pranešimai mokslinėse konferencijose

1. Šidlauskas, A. **Cybersecurity-Related Roles Identification and Alignment**, *EDULEARN21:13th International Conference on Education and New Learning Technology, Online Conference*, 5nd-6th of July, 2021.
2. Šidlauskas, A. **General Data Protection Regulation (GDPR) Awareness Training Opportunities in Lithuania**, *ICERI20: 14th annual International Conference of Education, Research and Innovation*, 8th - 9th of November, 2021.

3. Šidlauskas, A. Personal Data Processing in Educational Institutions: **Anonymisation and Pseudonymisation**, *ICERI20: 13th annual International Conference of Education, Research and Innovation*, 9th - 10th of November, 2020.
4. Šidlauskas, A., Ungurytė-Ragauskienė, S. Iššūkiai Kibernetiniam Saugumui: **Socialinė Inžinerija Institucinio Izomorfizmo Kontekste**, *SUSTAINSECURE-2020: 11th International Scientific Conference „Problems of Ensuring Public Security: Theoretical and Practical Aspects"*, 20th-22th of October, 2020.
5. Šidlauskas, A. **Consent as a Lawful Basis for Processing Personal Data under the GDPR**, *INTED20: 14th International Technology, Education and Development Conference*, Valencia, Spain. 2-4, 2019.

GYVENIMO APRAŠYMAS

Asmeninė informacija
Vardas, pavardė Aurimas Šidlauskas

Išsilavinimas
2019 – 2023 Vadybos mokslo krypties Mykolo Romerio universiteto doktorantas
2016 – 2018 Kibernetinio saugumo valdymo magistras, Mykolo Romerio universitetas
2013 – 2015 Elektroninio verslo vadybos magistras, Mykolo Romerio universitetas
2005 – 2011 Verslo teisės magistro, Kazimiero Simonavičiaus universitetas

Darbo patirtis
Nuo 2023 UAB „Adwisery“, Kibernetinio saugumo grupės vadovas
2021 – 2023 UAB „Adwisery“, Informacijos saugos valdymo ekspertas
2019 – 2021 UAB „Delfi“, Tekstų autorius ir kito turinio kūrėjas
2018 – 2020 VšĮ Lietuvos nacionalinis radijas ir televizija (LRT), Informacijos saugos įgaliotinis
2018 – 2020 VšĮ Lietuvos nacionalinis radijas ir televizija (LRT), Duomenų apsaugos pareigūnas
2011 – 2016 Bakkavor Group plc, Kokybės kontrolierius
2010 – 2011 UAB „Aviva Lietuva“, Finansų konsultantas

Asociacijos
Nuo 2023 ISC2 asociacijos narys
Nuo 2021 ISACA Lietuva asociacijos narys
2020 – 2022 Lietuvos duomenų apsaugos pareigūnų asociacijos narys

MYKOLAS ROMERIS UNIVERSITY

Aurimas Šidlauskas

MODEL OF A SYSTEM FOR THE SECURE MANAGEMENT OF PERSONAL DATA IN CYBERSPACE

Summary of Doctoral Dissertation
Social Sciences, Management (S 003)

Vilnius, 2024

This doctoral dissertation has been prepared during the period of 2019–2023 at Mykolas Romeris University under the doctoral program right conferred to Vytautas Magnus University, Klaipėda University, Mykolas Romeris University and Vilnius University by the order of the Minister of Education, Science and Sport of the Republic of Lithuania No. V-160 dated February 22, 2019.

Scientific Supervisor:
Prof. Dr. Tadas Limba (Mykolas Romeris University, Social Sciences, Management, S 003).

The doctoral dissertation will be defended at the Committee of Management of Vytautas Magnus University, Klaipėda University, Mykolas Romeris University and Vilnius University Šiauliai Academy:

Chairperson:
Prof. Dr. Andrius Stasiukynas (Mykolas Romeris University, Social Sciences, Management, S 003).

Members:
Prof. Dr. Vida Davidavičienė (Vilnius Gediminas Technical University, Social Sciences, Management, S 003);
Prof. Dr. Fernando Galindo (University of Zaragoza, Spain, Social Sciences, Law, S 001);
Prof. Dr. Ligita Šimanskienė (Klaipėda University, Social Sciences, Management, S 003);
Prof. Dr. Jan Žukovskis (Vytautas Magnus University, Social Sciences, Management, S 003).

The doctoral dissertation will be defended at the open meeting of the Scientific Council in the field of Management on 10 May 2024 at 9.00 am at Mykolas Romeris University, I-414 Room.
Address: Ateities st. 20, Vilnius, Lithuania.

Aurimas Šidlauskas

MODEL OF A SYSTEM FOR THE SECURE MANAGEMENT OF PERSONAL DATA IN CYBERSPACE

SUMMARY

Relevance and novelty of the research. Rapid technological developments caused by advances in computing power, increased amounts of data storage and more advanced networking technology are enabling organisations to collect and process ever larger amounts of data. In the knowledge economy, data has become an important part of creating a competitive advantage. Organisations that fail to adequately protect personal data may lose the trust of consumers, which is essential to encourage people to use new products and services. The protection of personal data is an important subject of researches and studies as there is a wide field of interpretation on how and by what means organisations should protect personal data. The improper processing of the personal data exposes organisations to financial, legal and reputational risks, which is why organisations that process personal data of EU citizens must implement and ensure compliance with the General data protection regulation.

It is impossible to imagine the management of modern organisations without information technology, information systems and internet access. The development of the internet, information technologies and the transfer of information into cyberspace is improving the quality of information processes and activities. While new technologies and services are good for both businesses and consumers, they also pose serious risks to cyber security. With the number of cyber incidents increasing every year around the world, cyber security is becoming increasingly important. This is not just a technological problem, as the vast majority of cyber security problems are not caused by technology but by people. They are often deliberate, well thought-out, goal-oriented and highly qualification requiring actions. There is no one-size-fits-all solution to cyber security, so complex measures involving national regulation, internal organisational policies and the replication of successful international practices are becoming increasingly important. Absolute cyber security cannot be achieved, but properly selected and applied security measures, procedures and processes can reduce the degree of risk and the extent of loss.

Organisations are forced to change and improve their data processing processes and procedures, and to apply cyber security measures to ensure the protection of personal data. The General data protection regulation does not specify what cyber security measures are appropriate. The protection of personal data is a topical and important issue today, and the application of appropriate cyber security measures is important both in theory and in practice. A model for a system for the secure management of personal data in cyberspace would anticipate and mitigate potential risks to the protection of personal data and cyber security.

Summarising the sources of information analysed in the dissertation, it can be stated that in the scientific literature, researchers pay attention to the following issues of the phenomenon of interaction between the protection of personal data and cyber security: what are the basic requirements for personal data protection and cyber security; what are the main interpretations of personal data protection and cyber security; what is the role of the data protection officer in the organisation; how to manage a breach of personal data and a cyber incident; how can the measures for the secure management of personal data in cyberspace mitigate the risks of a personal data breach and a cyber incident; etc. It is worth noting that research on the evaluation of the protection of personal data and cyber security in organisations is not well developed. Thus, the evaluation of the measure for the secure management of personal data in cyberspace is a relevant object of research from both theoretical and practical points of view, and this dissertation is devoted to its broader understanding.

Level of research on the topic. Researchers, international and Lithuanian organisations, and academics from around the world, as well as from Lithuania, are looking at cyber security and the protection of personal data from various perspectives.

Personal data protection as a phenomenon has been examined by: Tikkinen-Piri, 2018; Cortez, 2021; Batutytė, 2019; Voigt, Von dem Bussche, 2017; Kamleitner, Mitchell, 2018; Cabral, 2021; Malinauskaitė-van de Castel, 2017; Zaleskis, 2019; Limba, Šidlauskas, 2020; Tamavičiūtė, 2019; Diker Vanberg, Ünver, 2017; Ooijen, Vrabec, 2019; Feth, 2020; Sánchez, ir kt. 2021; Dibble, 2019; Gobeo ir kt., 2018; Alkhaledi, Hawamdeh, 2020; Teixeira, 2019; Europos komisija (EK), 2020; Andrijauskas, Morkūnienė, 2020; Europos duomenų apsaugos valdyba; Valstybinė duomenų apsaugos inspekcija (VDAI); Alford, 2020; Lambert, 2017; Sharma, 2019; Daigle, Khan, 2020; Gabel, Hickman, 2019; Presthus, Sønslien, 2021; Piras, 2019; Nadeau, 2017.

Cyber security as a phenomenon has been examined by: Bayne, 2008; Jinhua, 2013; Jastiuginas, 2011; Asquith, Morgan, 2020; Möller, 2020; Nacionalinis kibernetinio saugumo centras (NKSC), Solms, von Solms, 2018; Štitilis, 2016; Horák, 2019; National Institute of Standards and Technology (NIST); International Organization for Standardization (ISO); Schreider, 2020; Tarptautinė informacinių sistemų valdymo ir audito asociacija (ISACA); Raval, 2018; Corradini, 2020; Esparza, 2020; Thiéry, Fass, 2020; Chang, 2020; Wu, 2020; Baumeister, Vohs, 2016; Reeves, 2020; Schreider, 2017; Agafonov, 2021; Hooper, McKissack, 2016; Fitzgerald, 2017; Ritchey, 2020; Maurer, 2021; 2015; Blum, 2020; Harknett, Stever, 2011; Grincevičius, 2019.

Personal data protection measures have been examined by: Štarchoň, Pikulík, 2019; Blanco-Lainé, 2019; Grütter, Schneider, 2019; Bock, 2021; Information Commissioner's Office (ICO); Chassang, 2017; Valstybinė duomenų apsaugos inspekcija (VDAI); Pandit, 2019; Helbing, 2022; Hilberg, 2022; Valstybės kontrolė (VK); Bamberger, Mulligan, 2015; Drewer, 2018; Ayala-Rivera, Pasquale, 2018; Felici, 2013; Freitas, Silva, 2018; Mouratidis, 2016; Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA); International Organization for Standardization (ISO); Ryan, 2020; Haes, 2013; Ghazouani, 2014; Demetzou, 2018; Europos duomenų apsaugos valdyba; Aven, 2016; Shimonski, 2016; Gibson, 2014; Tikkinen-Piri, 2018; Barnard-Wills, 2019; Perry,

2019; Werner, 2020; Carey, 2019; Tiliute, 2019; Flavián, Guinalíu, 2006; Harkous, 2018; Linden, 2018; Wolford, 2022; Degeling, 2018; Eijk, 2019; Nouwens, 2020; SANS institutas.

Cyber security measures have been examined by: Cheng, 2020; Alghamdi, 2021; Ghelani, 2022; Kahyaoglu, Caliyurt, 2018; Lubua, Pretorius, 2019; Aliyeva, Hwang, 2019; Patterson, 2017; Koskelo, 2020; Wang, 2018; Cabaj, 2018; Hooper, McKissack, 2016; Kaselis, Pivoras, 2012; Scarfone, 2021; Buccafurri, 2015; Chapple, 2018; Gollmann, 2015; Menard, 2017; Kovács, 2018; Cains ir kt., 2022; Rea-Guaman, 2020; Black, 2018; Fielder, 2018; Claroty, 2021; Zimmermann, Renaud, 2019; Chowdhury, 2019; Chochlova, 2022; Dean, McDermott, 2017; Nacionalinis kibernetinio saugumo centras (NKSC); Aldawood, 2020; Lois, 2020; Fernando, 2017; Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA); International Organization for Standardization (ISO); Bisson, 2021; Aoyama, 2015; Baig, 2022; George, 2021; Mandritsa, 2018.

Scientific problem - What are the concepts of personal data protection and cyber security management, and what should be the model of a system for the secure management of personal data in cyberspace in order to reduce the risks of a personal data breach and a cyber security incident?

Object of the scientific research - measures for secure management of personal data in cyberspace.

Objective of the scientific research - to develop a model for a system for the secure management of personal data in cyberspace, which would help to reduce the risks of a personal data breach and a cyber security incident.

In order to achieve the objective, the dissertation has addressed the following **tasks:**

1. Analyse the theoretical aspects interaction between personal data protection and cyber security.
2. Perform qualitative analysis of documents, case studies and expert opinion to identify criteria for the development of a model for measures to securely manage personal data in cyberspace.
3. Propose a model for a system for the secure management of personal data in the cyberspace.
4. Assess the challenges and opportunities for the application of a model of a system for the secure management of personal data in cyberspace.

Scientific research methods and main sources. In order to achieve the set objective and solve the set tasks, the theoretical part of the dissertation includes systematic comparative analysis and generalisation of the sources of scientific literature. The empirical part of the dissertation is based on a case study and complementary qualitative empirical research: document analysis, expert interviews, qualitative content analysis, and analysis of secondary source data. The empirical part of the research builds on the insights presented in the theoretical part and draws on the theoretical assumptions of the interpretative assumptions.

Dissertation backed statements:

1. Cyber security is part of personal data protection.

2. The model of the system for the secure management of personal data in cyberspace reduces the risk of personal data breaches and cyber incidents.
3. The model of the system for the secure management of personal data in cyberspace reduces the risk of personal data breaches and cyber incidents.

Theoretical and practical relevance of the research. A model for the system for the secure management of personal data in cyberspace has been developed, which addresses the dimensions of personal data protection and cyber security through a range of measures for the secure management of personal data, with the aim of minimising the risks of personal data breaches and cyber security, in order to ensure the accessibility, integrity and confidentiality of electronic information, including data and personal data but also to ensure the fundamental principles of personal data processing, protecting the rights and freedoms of natural persons with regard to the processing of personal data.

It should be noted that this model of a system for the secure management of personal data in cyberspace will be available for use by all organisations that manage or process personal data and aim to improve the protection and management of personal data and cyber security, and to mitigate the risks of personal data breaches and cyber security incidents. In the model of a system for the secure management of personal data in cyberspace, each of the dimensions of both the protection of personal data and the cyber security, from level I to level III, can be implemented separately, taking into account the organisation's operational specificities, the resources under management, the resources available and the financial capacity. However, level IV of the model of a system for the secure management of personal data in cyberspace will be linked to the implementation of all the measures listed in the dimensions of personal data protection and cyber security, with the aim of transforming the system into an integrated management system for the protection of personal data and for the management of cyber security, where the measures are clearly interlinked and act complementary to each other.

Structure of the thesis. *At the beginning of the thesis* is the introduction. The thesis is divided into four parts. *The first part* deals with the theoretical analysis of the interaction between personal data protection and cyber security: The theoretical substantiation for personal data protection as a phenomenon; The theoretical substantiation for cyber security as a phenomenon; The issues of the interaction between the protection of personal data and the cyber security and its implementation. *The second part* presents the methodology of the research on measures for the secure management of personal data in cyberspace: Research plan. The *third part* presents the results of the application of the measures for the secure management of personal data in cyberspace: the results of the application of the measures for cybersecurity and protection of personal data and the results of the sampling; Results of a research on the conformity assessment of information technology safety; Results of a research to establish the lawfulness of processing of personal data; Results of an expert evaluation research. *The fourth part* performs the development of a model for a system for the secure management of personal data in cyberspace: Analysis of the personal data protection dimension; Analysis

of the cyber security dimension; The challenges and opportunities for the application of the system model for the secure management of personal data in cyberspace. *The ending part of the thesis* provides conclusions and recommendations (see Figure 1).

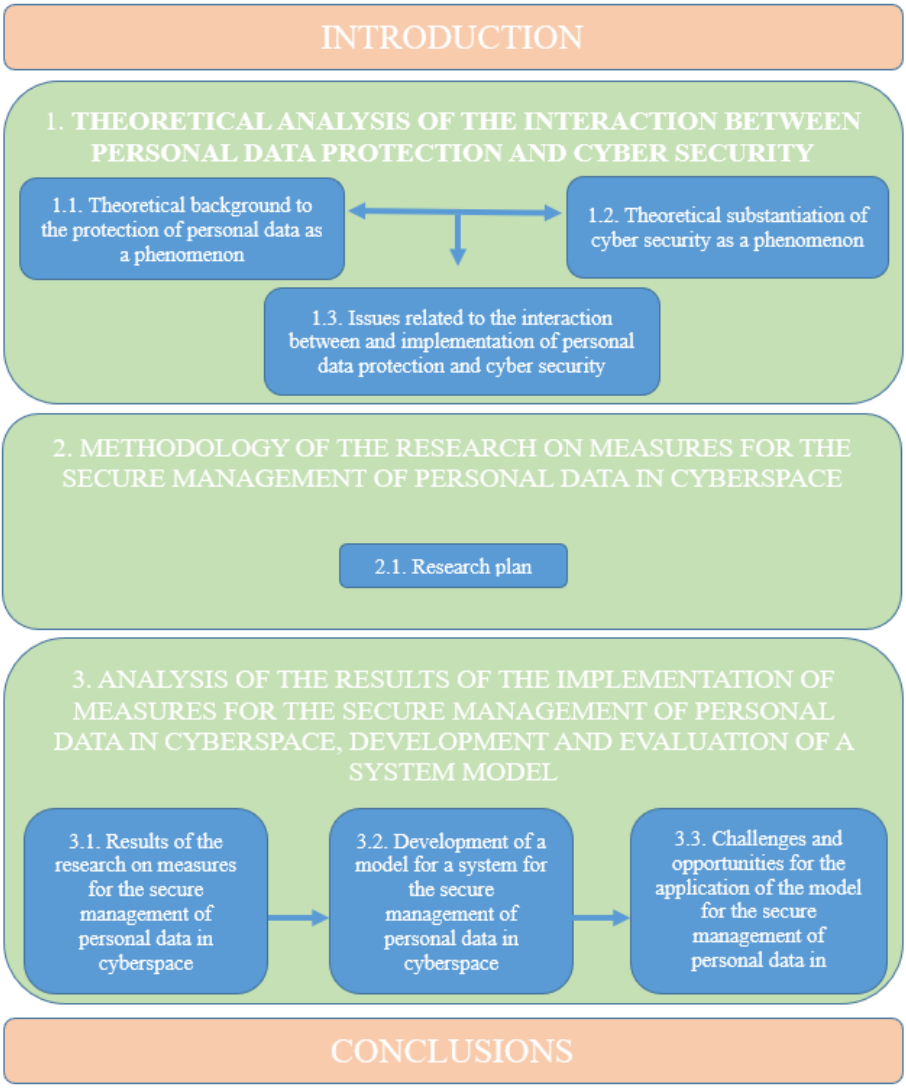


Fig. 1. The logical structure of the dissertation

Source: created by the author

REVIEW OF PART ONE: THEORETICAL ANALYSIS OF THE INTERACTION BETWEEN PERSONAL DATA PROTECTION AND CYBER SECURITY

The first section discusses the importance of personal data protection, as a phenomenon, for organisations and individuals in the modern world. Concept, classification, substantiation for management and principles of processing personal data are discussed. Attention should be brought to the fact that personal data has become a very valuable asset for organisations, both controllers and processors, and is often the basis for the provision and development of services. It should be noted that when organisations process personal data, it should not only be in their interests, but also in the interests of the data subjects, i.e. the individuals whose personal data they process, as the Regulation may lead to liability - legal, financial, reputational - for the inappropriate processing of personal data. Analysis of the roles of the data protection officer and data protection supervising institution in the organisation is performed.

The second section discusses the importance of cyber security as a phenomenon for organisations and individuals in the modern world. Concept, content and principles of cyber security are discussed. It should be noted that cyber security is a set of legal, information dissemination, organisational and technical measures aimed at ensuring the accessibility, integrity and confidentiality of IS and the electronic information they contain. Aspects of the implementation of cyber security policies in organisations are analysed. In Lithuania, the strategic goals, priorities and measures necessary to achieve them are set by the Government of the Republic of Lithuania. The Ministry of Defence of the Republic of Lithuania formulates, organises, controls and coordinates cyber security policy. The National Cyber Security Centre (hereinafter - NCSC), the SDPI, the Lithuanian Police and other institutions with cyber security-related functions implement the cyber security policy. The thesis substantiates that Lithuania's cyber security management system is not sufficiently effective, that cyber incident management needs to be improved, and that consistent implementation of cyber security planning is not ensured.

The third section discusses the interaction and implementation of personal data protection and cyber security. It points out that cyber security measures are one of the prerequisites for the protection of personal data. The requirements for the protection of personal data are very abstract and open to interpretation, and each organisation has its own way of ensuring compliance with the basic principles of personal data protection and of demonstrating compliance with the requirements.

REVIEW OF PART TWO: METHODOLOGY OF THE RESEARCH ON MEASURES FOR THE SECURE MANAGEMENT OF PERSONAL DATA IN CYBERSPACE

The first section discusses the study research plan. The methodology of the research relies on a number of research methods that increase the precision of the results, improve the limited applicability of individual methods, and help to capture underrepresented phenomena. To achieve the main aim of the research, four researches were carried out:

First research. The use of document analysis method is used to identify: What are the mandatory cyber security and personal data protection measures and their application in Lithuania. During the research, a list of the most relevant legislation, standards and guidelines in the field of cyber security and personal data shall be compiled, including requirements and/or controls, divided into organisational and technical measures.

Second research. Using a case study approach, this research is designed to assess the compliance of organisations' IT security with the standards and guidelines of the legislation governing cyber security and personal data protection, in order to identify the main non-compliances and the threats they pose to the organisations' cyber security and personal data protection.

Third research. The case study and comparative approach methods were used to identify the lawfulness of the use of personal data by organisations, specifically cookies, on their websites. The results of this research are compared with a previous survey conducted in 2020 to assess how the situation has changed and whether organisations are paying more attention to the protection of personal data.

Fourth research. A semi-structured interview was carried out with 9 experts using the expert interview method to obtain their views on the measures for the secure management of personal data in cyberspace and their application. Content analysis is used in processing received data.

REVIEW OF PART THREE: RESULTS OF THE APPLICATION OF MEASURES TO MANAGE THE SECURITY OF PERSONAL DATA IN CYBERSPACE

The first section sets out the measures for cybersecurity and the protection of personal data, and the scope of their application. It should be noted that all organisations are required to ensure compliance with personal data protection requirements, which oblige them to process data in accordance with the basic principles of personal data processing and to apply appropriate technical and organisational safeguards.

The second section assesses the IT security compliance of the three organisations against international and national legislation, standards and guidelines on cyber security and personal data protection and makes recommendations to address the identified gaps. Organisations were found not to periodically update security documents, conduct risk assessments and IT security compliance assessments, provide training, conduct business continuity management plan exercises and ensure control over third-party service providers.

The legality of the processing of personal data using cookies by the 100 most popular Lithuanian websites has been established in the third section. It should be noted that organisations can only collect cookies on websites with the user's consent.

The fourth section describes the receipt analysis of the responses of 9 experts on personal data protection and cybersecurity measures and their implementation issues.

REVIEW OF PART FOURTH: DEVELOPING A MODEL OF A SYSTEM FOR THE SECURE MANAGEMENT OF PERSONAL DATA IN CYBERSPACE

The fourth chapter contains development of a model of a system for the secure management of personal data in cyberspace. In order to simplify the implementation of this model of the system for the secure management of personal data in cyberspace in the organisation, the implementation of the model's measures is foreseen to be carried out in stages, distinguishing four levels of the model for the management of personal data protection and cyber security - awareness (level I), implementation (level II), assurance/improvement (level III), integrated level (level IV). A model of a system for the secure management of personal data in cyberspace is presented (see Figure 2).

The first section analyses the eight measures of the personal data protection dimension of the model of a system for the secure management of personal data in cyberspace.

The second section analyses the measures of eight cybersecurity dimensions of the proposed model of a system for the secure management of personal data in cyberspace.

The third section assesses the challenges and opportunities for the application of the model of a system for the secure management of personal data in cyberspace. It should be noted that it is not possible to single out a separate, most important measure in the model of a system for the secure management of personal data in cyberspace, as only the application of all measures in an organisation, combining the dimensions of personal data protection and cyber security into a single organisational management system, can show clear results in terms of change in the protection of personal data and in the cyber security. As mentioned above, each of the dimensions of both the personal data protection and the cyber security can be implemented individually, depending on the organisation's operational specificities, the resources it manages, the resources available and its financial capacity. However, it should be noted that the fourth level of the model of a system for the secure management of personal data in cyberspace is linked to the implementation of all the measures listed in the dimensions of personal data protection and cyber security, with the aim of transforming the system into an integrated management system for the protection of personal data and for the management of cyber security, where the measures are clearly interlinked and act in a complementary way to each other.

Fig. 2. A model for a system for the secure management of personal data in cyberspace

Source: created by the author

CONCLUSIONS

Objective 1. An analysis of the theoretical aspects of the interaction between personal data protection and cybersecurity shows the following:

1. Organisations managing or processing personal data that have been anonymised are exempt from the personal data protection requirements. However, pseudonymised data are fully covered by the scope of protection of personal data as personal data, since pseudonymisation does not remove all identifying information from the data, but only reduces the association of the data set with the individual. In the event of a cyber incident or a personal data breach, where anonymised and pseudonymised data are processed, the damage to personal data subjects is reduced by protecting their privacy rights.
2. Data subjects have specific rights under the data protection regulation that give them control over their personal data held and processed by organisations.
3. The data protection officer ensures that the personal data protection requirements are properly implemented in the organisation, but the responsibility for non-compliance is attributed to the data controller and/or processor.
4. Absolute protection of personal data and cybersecurity cannot be achieved, but properly selected and applied security measures can reduce the degree of risk and the extent of loss.

Objective 2. After the completion of qualitative analysis of documents, case studies and expert opinions, used to identify criteria for the development of a model for measures to securely manage personal data in cyberspace, the following conclusions can be made:

1. Some of the requirements for cybersecurity and protection of personal data are identical in different legislation and in the ISO 27001 and ISO 27002 standards and in the State Data Protection Inspectorate guidelines, making it difficult for organisations to implement these requirements.
2. The assessment of the three organisations' cybersecurity and personal data protection regulations in internal legislation and their actual implementation in practice showed that the organisations do not periodically update their security documents, do not conduct risk assessments and IT security compliance assessments, do not provide training, do not conduct business continuity management plan testing exercises, and do not ensure control over third-party service providers.
3. According to an assessment of the 100 most popular websites in Lithuania, the vast majority of organisations that manage or process personal data (cookies) do not comply with personal data protection requirements and use cookies illegally on their websites, i.e., without the users' consent and without providing key information about their processing in their privacy policy.
4. The evaluation of 9 expert opinions found that:

4.1. Cybersecurity is inextricably linked to the protection of personal data, as many of the measures to protect personal data are organisational and technical cybersecurity measures.
4.2. There are several reasons why an organisation may be reluctant to invest in personal data protection and cyber security - unknown (difficult to measure) return on investment, potential reduction of productivity, and tolerance and perception of risks that could not be mitigated.
4.3. Organisations often prioritise technical measures over organisational ones, as technical measures can be bought and demonstrated, while organisational measures are more difficult to implement and control.

Objective 3. After a proposal of a model for a system for the secure management of personal data in the cyberspace, the following can be stated:

1. The proposed model of the system for the secure management of personal data in cyberspace consists of two dimensions - personal data protection and cybersecurity - which contain 16 measures to ensure the protection of personal data in an organisation. The cybersecurity dimension is part of the personal data protection dimension.
2. The personal data protection dimension ensures the lawful processing of personal data and appropriate technical and organisational measures to protect the fundamental rights and freedoms of the data subject, in particular their right to the protection of personal data.
3. The cybersecurity dimension provides for cybersecurity management and appropriate technical and organisational measures to protect the availability (accessibility), integrity and confidentiality of electronic information transmitted or processed through information systems.
4. The proposed model of the system for the secure management of personal data in cyberspace, enables an organisation to monitor changes in the implementation of the protection of personal data and cybersecurity according to the gradual implementation of measures, at the levels of awareness (I), implementation (II), assurance/improvement (III) and integrated level (IV), in specific dimensions.

Objective 4. Having assessed the challenges and opportunities of applying the model of a system for the secure management of personal data in cyberspace, it has been found that:

1. Failure to ensure cybersecurity is a risk of a personal data breach as personal data may be disclosed, lost, and become inaccessible. However, even with cybersecurity ensured, there is still a risk of a personal data breach, as personal data may be processed in breach of the basic principles of personal data processing. Only by ensuring the personal data protection and cybersecurity measures outlined in the model can the protection of personal data be ensured, in order to reduce the risk of cyber incidents and personal data breaches.
2. Organisations may face challenges in implementing the model of a system for the secure management of personal data in cyberspace, such as lack of expertise

and experience, lack of human resources, lack of financial resources, lack of communication and cooperation, lack of motivation and resistance to change.

3. Each of the measures in the model of the system for the secure management of personal data in cyberspace can be implemented separately, without singling out a single most important measure, taking into account the organisation's operational specificities, the resources it manages, the resources available and the financial possibilities. However, level IV of the model of a system for the secure management of personal data in cyberspace is linked to the implementation of all the measures listed in the dimensions of personal data protection and cybersecurity, with the aim of transforming the system into an integrated management system for the protection of personal data and for the management of cybersecurity, where the measures are interlinked and shall act complementary to each other.

RECOMMENDATIONS

For organizations:

1. Anonymisation and pseudonymisation of personal data is recommended to facilitate the implementation of data protection requirements and to protect the privacy rights of individual data subjects.
2. In order to ensure the exercise of the rights of data subjects, they should, in particular, inform data subjects in short and easily understandable language of their rights and, in particular, establish mechanisms and procedures for their exercise.
3. It is recommended that the controller/processor cooperates with the data protection officer by involving him at the earliest possible stage in all data protection issues and by providing the necessary resources to carry out the tasks and to develop. Meanwhile, the data protection officer is obliged to assess the risks of processing personal data in the light of the nature, scope, context, and purposes of the organisation's personal data, and to inform the controller/processor and consult the supervisory authority.
4. The implementation of personal data protection measures, which also include cyber security measures, requires an assessment of what measures are appropriate, depending on the sensitivity of the data and the degree of risk of personal data being compromised.
5. In order to ensure the protection of personal data, it is mandatory to implement not only the technical and organisational measures for cybersecurity laid down in the legislation, but also the basic principles of personal data processing and the best practices set out in the ISO 27001 and ISO 27002 standards and the guidelines on security measures and risk assessment of processed personal data issued by the State data protection inspectorate.
6. In order to lawfully process data in the form of cookies on websites, the data controller and/or processor must have an appropriate tool to enable users to actively consent or object to the processing of the relevant cookies and to change their mind at any time, as well as to provide full information on the processing of cookies in the website's privacy policy.
7. It is recommended to think in terms of security rather than convenience when improving business processes in the context of personal data protection, in accordance with the law and generally accepted best practices set out in international standards.
8. Technical measures will not work properly without organisational measures, so a balance must be struck between the two.

For users (data subjects):

1. It is recommended to inquire about how organisations process their personal data and to claim their rights in the context of personal data.

2. It is recommended to inform the supervisory authorities - the State data protection inspectorate in case of a personal data breach and the National cyber security centre in case of a cyber incident.

Further research could be carried out on the thesis topic:

1. Experts in personal data protection and cybersecurity may be used to assess the applicability of the model for the secure management of personal data in cyberspace.
2. Reveal how the measures of the model for the system of secure management of personal data in cyberspace relate to each other, i.e., how the implementation of one measure influences the other.
3. Improve or add new measures to the model system for the secure management of personal data in cyberspace, based on research.

Academic Publications Related to the Dissertation

1. Limba, T., Šidlauskas, A., & Juozėnaitė, E. (2023). **Direct Marketing in Lithuania under GDPR: Consent and Legitimate Interests**, *12th International Conference on Applied Economics Contemporary Issues in Economy*, 99-106. https://doi.org/10.24136/eep.proc.2023.2
2. Šidlauskas, A. (2021). **The Practice of Imposing Administrative Fines by the State Data Protection Inspectorate in the Context of Other EU Member States**, *Social research*, 44(2), 153-169. https://doi.org/10.15388/Soctyr.44.2.10
3. Limba, T., Šidlauskas, A. (2021). **Cybersecurity-Related Roles Identification and Alignment**. *In Edulearn21.13th International Conference on Education and New Learning Technology, Online Conference, 5nd-6th of July, 2021: Conference Proceedings,* 7404-7413. https://doi.org/10.21125/edulearn.2021.1500
4. *Šidlauskas, A. (2021).* **The Role and Significance of the Data Protection Officer in the Organization**. *Social research*, 44(1), 8-28. https://www.zurnalai.vu.lt/social-research
5. *Šidlauskas, A. (2021).* **General Data Protection Regulation (GDPR) Awareness Training Opportunities in Lithuania**. *ICERI20: 14th annual International Conference of Education, Research and Innovation, 8th - 9th of November, 2021: Conference Proceedings*, 9158-9166. http://dx.doi.org/10.21125/iceri.2021.2109
6. Limba, T.; Driaunys, M.; Šidlauskas, A. (2021). **Use of Cookies After GDPR: a Case Study of Top Lithuanian Websites**, *Transformations in Business & Economics,* Vol. 20, No. 3 (54): 93-116. http://www.transformations.knf.vu.lt/54/article/useo
7. Limba, T.; Šidlauskas, A. (2020). **Personal Data Processing in Educational Institutions: Anonymisation and Pseudonymisation**. *ICERI20: 13th annual International Conference of Education, Research and Innovation, 9th - 10th of November, 2020: Conference Proceedings,* 9989-9997. http://dx.doi.org/10.21125/iceri.2020.2262
8. *Šidlauskas, A.; Ungurytė-Ragauskienė, S. (2020).* **Challenges for Cyber Security: Social Engineering in the Context of Institutional Isomorphism**, *SUSTAINSECURE-2020: 11th International Scientific Conference „Problems of Ensuring Public Security: Theoretical and Practical Aspects"*, 20th-22th of October. https://doi.org/10.13165/PSPO-20-25-26
9. Limba, T.; Driaunys, K.; Kiškis, M.; Šidlauskas, A. (2020). **Development of Digital Contents: Privacy Policy Model under the General Data Protection Regulation and User Friendly Interface**, *Transformations in Business & Economics,* 1(49): 21-42. http://www.transformations.knf.vu.lt/49/article/deve
10. Limba, T.; Šidlauskas, A. (2020). **Consent as a Lawful Basis for Processing Personal Data under the GDPR**. *INTED20: 14th International Technology, Education and Development Conference, Valencia, Spain. 2-4 March, 2020: Conference Proceedings,* 1374-1383. http://dx.doi.org/10.21125/inted.2020.0456

Other Academic Publications

1. Limba, T., Šidlauskas, A., & Juozėnaitė, E. (2022). **The Role of User-generated Content in Brand Communication and the Tactics to Encourage It**. *ICERI2022:*

15th annual International Conference of Education, Research and Innovation, Seville, Spain, 7-9 November, 2022. pp. 865-871. https://dx.doi.org/10.21125/iceri.2022.0262

2. Šidlauskas, A. (2019). **Opportunities for DPO (Data Protection Officer) Occupational Training and Improvement**. *INTED19: 13th International Technology, Education and Development Conference*, Valencia, Spain. 11-13 March, 2019, pp. 808-814. http://dx.doi.org/10.21125/inted.2019.0280
3. Šidlauskas, A. (2019). **Video Surveillance and the GDPR**. *Social Transformations in Contemporary Society (STICS 2019): Proceedings of an Annual International Conference for Young Researchers*, (7), 55-65. https://repository.mruni.eu/handle/007/15840
4. Limba, T.; Šidlauskas, A. (2019). **General Data Protection Regulation Interpretation in Higher Education Institutions**. *EDULEARN19: 11th International Conference on Education and New Learning Technologies*, Palma, Spain. 1-3 July, 2019, pp. 2040-2047. http://dx.doi.org/10.21125/edulearn.2019.0555
5. Limba, T.; Šidlauskas, A. (2018). **Secure Personal Data Administration in the Social Networks: the Case of Voluntary Sharing of Personal Data on the Facebook**, *Entrepreneurship and Sustainability Issues* 5(3): 528-541. https://doi.org/10.9770/jesi.2018.5.3(9)
6. Šidlauskas, A. (2018). **Users Electronic Data Protection Features**. *Social Transformations in Contemporary Society (STICS 2018): Proceedings of Annual International Conference for Young Researchers*, (6), 78-88. https://repository.mruni.eu/handle/007/15344
7. Limba, T.; Šidlauskas, A. (2018). **Peculiarities of Anonymous Comments' Management: a Case Study of Lithuanian News Portals**, *Entrepreneurship and Sustainability Issues* 5(4): 875-889. http://doi.org/10.9770/jesi.2018.5.4(12)
8. Limba, T.; Šidlauskas, A. (2018). **An Analysis of Comments Containing Hate Speech: Facebook and the Delfi News Portal**. *EDULEARN18: 10th International Conference on Education and New Learning Technologies*, Palma, Spain, 2nd–4th of July, 2018, 3413-3419. http://dx.doi.org/10.21125/edulearn.2018.0887

Presentations at Scientific Conferences

1. Šidlauskas, A. **Cybersecurity-Related Roles Identification and Alignment**, *EDULEARN21:13th International Conference on Education and New Learning Technology*, Online Conference, 5nd-6th of July, 2021.
2. Šidlauskas, A. **General Data Protection Regulation (GDPR) Awareness Training Opportunities in Lithuania**, *ICERI20: 14th annual International Conference of Education, Research and Innovation*, 8th - 9th of November, 2021.
3. Šidlauskas, A. Personal Data Processing in Educational Institutions: **Anonymisation and Pseudonymisation**, *ICERI20: 13th annual International Conference of Education, Research and Innovation*, 9th - 10th of November, 2020.
4. Šidlauskas, A., Ungurytė-Ragauskienė, S. Iššūkiai Kibernetiniam Saugumui: **Socialinė Inžinerija Institucinio Izomorfizmo Kontekste**, *SUSTAINSECURE-2020: 11th International Scientific Conference „Problems of Ensuring Public Security: Theoretical and Practical Aspects"*, 20th-22th of October, 2020.
5. Šidlauskas, A. **Consent as a Lawful Basis for Processing Personal Data under the GDPR**, *INTED20: 14th International Technology, Education and Development Conference*, Valencia, Spain. 2-4, 2019.

CURRICULUM VITAE

Personal information
Name, surname: Aurimas Šidlauskas

Education
2019 – 2023 Doctoral Student in Management, Mykolas Romeris University
2016 – 2018 Master of Cyber Security Management, Mykolas Romeris University
2013 – 2015 Master of Electronic Business Management, Mykolas Romeris University
2005 – 2011 Master of Business Law, Kazimieras Simonavicius Universitety

Work experience
From 2023 UAB „Adwisery“, Head of Cyber Security Group
2021 – 2023 UAB „Adwisery“, Information Security Management Expert
2019 – 2021 UAB „Delfi“, Copywriter and Creator of other Content
2018 – 2020 Lithuanian National Radio and Television, Information Security Officer
2018 – 2020 Lithuanian National Radio and Television, Data Protection Officer
2011 – 2016 Bakkavor Group plc, Quality Controller
2010 – 2011 UAB „Allianz“, Finance Consultant

Associations
From 2023 ISC2 Association Member
From 2021 ISACA Lithuania Association Member
2020 – 2022 Member of the Association of Lithuanian Data Protection Officers

Šidlauskas, Aurimas

ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE SISTEMOS MODELIS: daktaro disertacija. – Vilnius: Mykolo Romerio universitetas, 2024. P. 240.

Bibliogr. 159-181 p.

Sparti technologinė plėtra dėl skaičiavimo galios progreso, padidėjusių duomenų saugojimo kiekių ir pažangesnio tinklo technologijos leidžia organizacijoms rinkti ir apdoroti vis didesnius duomenų kiekius. Netinkamas asmens duomenų tvarkymas organizacijoms kelia finansinę, teisinę ir reputacijos riziką. Asmens duomenų apsauga yra aktuali ir svarbi šiandienos problematika, todėl tinkamų saugumo priemonių taikymas svarbus tiek teorine, tiek praktine prasme. Apibendrinus apžvelgtos literatūros šaltinius ir empirinio tyrimo metu gautus rezultatus yra sukurtas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis. Sukurtas asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis leis organizacijoms numatyti ir sumažinti galimas asmens duomenų apsaugos ir kibernetinio saugumo rizikas.

Rapid technological developments caused by advances in computing power, increased amounts of data storage and more advanced networking technology are enabling organisations to collect and process ever larger amounts of data. The protection of personal data is a topical and important issue today, and the application of appropriate security measures is important both in theory and in practice. After summarizing the reviewed literature and the results obtained during the empirical research, a model for a system for the secure management of personal data in cyberspace was created. The created model for a system for the secure management of personal data in cyberspace will allow organizations to anticipate and mitigate potential risks to the protection of personal data and cyber security.

Aurimas Šidlauskas
ASMENS DUOMENŲ SAUGAUS VALDYMO ELEKTRONINĖJE ERDVĖJE SISTEMOS MODELIS

Daktaro disertacija
Socialiniai mokslai, vadyba (S 003)

Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas roffice@mruni.eu
Tiražas 20 egz.

Parengė spaudai Martynas Švarcas

Spausdino UAB „Šiaulių spaustuvė“
P. Lukšio g. 9G, 76200 Šiauliai
El. p. info@dailu.lt
https://siauliuspaustuve.lt