MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VERSLO IR EKONOMIKOS INSTITUTAS

INGA DILIENĖ

ASMENS DUOMENŲ NUTEKĖJIMO PRIVAČIAME SEKTORIUJE RPEVENCIJA

Magistro baigiamasis darbas

Vadovas:
prof. dr. Marius Laurinaitis

VILNIUS, 2024

MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VERSLO IR EKONOMIKOS INSTITUTAS

INGA DILIENĖ

ASMENS DUOMENŲ NUTEKĖJIMO PRIVAČIAME SEKTORIUJE RPEVENCIJA

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Konsultantas

Atliko:

KSVvmis 22-1 gr. stud.:
I. Dilienė

_____
(parašas)

2024 05

Recenzentas

Vadovas:
prof. dr. Marius Laurinaitis

_____
(parašas)

2024 05

VILNIUS, 2024

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

Magistro baigiamojo darbo tema – „Asmens duomenų nutekėjimo privačiame sektoriuje prevencija".

Magistrinio darbo išplėstinis planas pateikiamas 1 priede.

Magistro baigiamojo darbo vadovas – prof. dr. Marius Laurinaitis.

ĮVADAS

Temos aktualumas. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau - Bendrasis duomenų apsaugos reglamentas) buvo suvienodintas ir iki šiol stiprinamas asmens duomenų apsaugos reguliavimas Europos ekonominėje erdvėje.

Europos sąjungos narės vieningai sutaria, kad kibernetinės atakos inicijuojamos ne tik prieš pačias valstybes nares, kritinę infrastruktūrą, viešąjį sektorių, tačiau ir prieš mažo ir vidutinio dydžio privataus sektoriaus įmones (toliau – MVĮ), atakų taikiniu pasirenkant asmens duomenis, finansinę informaciją, verslo informaciją, darbuotojų bei klientų asmens duomenis bei intelektinę nuosavybę. Pasak Cartwright A., Cartwright E. ir kt.. teigia, kad „MVĮ yra patrauklūs taikiniai kibernetiniams nusikaltėliams dėl suvokiamo pažeidžiamumo, išteklių apribojimų ir kartais netinkamų kibernetinio saugumo priemonių. Šios įmonės, spręsdamos kibernetinio saugumo klausimus, susiduria su unikaliais iššūkiais, joms trūksta didesnių partnerių išteklių ir kompetencijos, kad galėtų veiksmingai kovoti su kibernetinėmis grėsmėmis. Nepaisant jų dydžio, MVĮ nėra atleistos nuo kibernetinių išpuolių ir vis dažniau tampa kibernetinių nusikaltėlių, siekiančių pasinaudoti sistemos pažeidžiamumu, taikiniais. Be to, MVĮ, teikdamos įvairias paslaugas, dažnai pasikliauja trečiųjų šalių pardavėjais ir partneriais, todėl dėl tiekimo grandinės pažeidžiamumo kyla papildoma kibernetinio saugumo rizika.“.[1] EY kibernetinio saugumo rizikų tyrime nustatyta, kad „kibernetinių atakų skaičiaus augimas 75% per penkerius metus rodo tiek pačių programišių suaktyvėjimą, tiek nepakankamą organizacijų dėmesį saugumui“[2]. Ypatingai svarbu užtikrinti saugumą, nes šiuolaikiniame skaitmeniniame amžiuje duomenys tapo vienu vertingiausiu įvairaus dydžio įmonių nematerialiuoju turtu. Įmonės nuolat renka ir analizuoja didelius kiekius duomenų, kad galėtų numatyti vartotojų elgseną, rinkos tendencijas bei vidinius procesus, todėl didėjant duomenų rinkimui ir dalinimuisi, duomenų saugumo prevencinių priemonių svarba taip pat didėja. Pasak Cheng L. ir kt. (2017) „duomenų kiekiui eksponentiškai augant, o duomenų

[1] Cartwright A., Cartwright E., Edunc E. S. *Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies*. 2023.
[2] Verslo žinios. *Kibernetinių atakų skaičius auga sparčiai: lemia ir geopolitika, ir nesutvarkytas IT ūkis*. 2024.

pažeidimams vykstant vis dažniau nei bet kada anksčiau, duomenų praradimo aptikimas ir prevencija tapo viena iš svarbiausių įmonių saugumo problemų“[3]. Netinkamo duomenų saugumo pasekmės gali būti sunkios, įmonės gali patirti finansinių nuostolių, reputacijos praradimų ar atsirasti kitų teisinių įsipareigojimų. Pasak Toldino J., Venčkausko A ir kt. „kibernetinės atakos ir kibernetinio saugumo rizika smarkiai išaugo naujose technologijose, tokiose kaip debesų kompiuterija, debesų kompiuterija, kraštinė kompiuterija ir daiktų internetas (IoT)“[4]. Šie išpuoliai gali prasiskverbti į su kompiuterių tinklais susijusias aplinkas ir debesimis pagrįstas paslaugas bei padaryti finansinės ir reputacijos žalos. Cartwright A., Cartwright E. ir kt. (2024) autoriai taip pat akcentuoja kibernetinių nusikaltimų poveikį reputacijai: „MVĮ vis labiau integruoja skaitmenines technologijas į savo veiklą, kad sustiprintų konkurencingumą, jos susiduria su vis didesne grėsme: kibernetiniais nusikaltimais. Kibernetinio saugumo pažeidimai ne tik atskleidžia neskelbtinų duomenų konfidencialumą, vientisumą ir prieinamumą, bet ir daro didelį poveikį MVĮ veiklos ir finansiniam stabilumui, taip pat jų reputacijai“.

Pažymėtina, kad „šiandien kompiuterinės programos ir programos kuriamos dideliu greičiu. Kenkėjiška programinė įranga atsirado ir auga įvairiais formatais ir tampa vis sudėtingesnė. Kompiuteriniai nusikaltėliai juos naudoja kaip įrankį įsiskverbti, pavogti ar klastoti informaciją, darydami didžiulę žalą asmenims, įmonėms ir net keliantys grėsmę nacionaliniam saugumui“[5].

2023 m. „Eurostat“ statistinės ataskaitos duomenimis, net 22 proc. ES įmonių patyrė kibernetinio saugumo incidentų per 2021 m.[6]. Valstybinės duomenų apsaugos inspekcijos 2022 metų veiklos ataskaitos duomenimis 60 proc. asmens duomenų saugumo pažeidimų kyla dėl žmogiškosios klaidos, o likusi dalis – dėl kibernetinių atakų. Pasak Chang L., Coppel N. (2020), „kibernetinė klaida“, tai yra, kibernetiniai nusikaltimai ir kibernetinio saugumo pažeidimai, sukelti žmogaus klaidų ar elgesio, tapo pagrindine kibernetinio saugumo problema[7]. Remiantis Valstybinės duomenų apsaugos inspekcijos 2022 metų asmens duomenų apsaugos priežiūros Lietuvoje apžvalgos duomenimis, Valstybinės duomenų apsaugos

[3] Cheng L., Liu F., Yao D. *Enterprise data breach: causes, challenges, prevention, and future directions*. (2017).
[4] Toldinas J, Venčkauskas A., Damaševičius R., Grigaliūnas Š., Morkevičius N., Baranauskas E. *A novel approach for network intrusion detection using multistage deep learning image recognition*.// Electronics. Basel : MDPI. ISSN 2079-9292. 2021, vol. 10, iss. 15, art. no. 1854, p. 1-21. DOI: 10.3390/electronics10151854.
[5] Damaševičius R., Venčkauskas A., Toldinas J. Grigaliūnas Š.. *Ensemble-based classification using neural networks and machine learning models for windows pe malware detection*.// Electronics. Basel: MDPI. ISSN 2079-9292. 2021, vol. 10, iss. 4, art. no. 485, p. 1-23. DOI: 10.3390/electronics10040485.
[6] Eurostat news. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1.
[7] Chang L., Coppel N. *Kibernetinio saugumo supratimo ugdymas besivystančioje šalyje: pamokos iš Mianmaro*. 2020.

inspekcijos gaunamų pranešimų dėl įvykusių asmens duomenų saugumo pažeidimų kasmet daugėjo iki 2023 metų (2018 m. – 100, 2019 m. – 175, 2020 m. – 181, 2021 m. – 239, 2022 m. – 304).[8]. Pagal asmens duomenų apsaugos pažeidimų pobūdį Lietuvoje statistiškai dominuoja konfidencialumo pažeidimai - 2022 m. net 269 asmens duomenų saugumo pažeidimų atvejais buvo prarastas asmens duomenų konfidencialumas, 21 atvejis buvo susijęs su duomenų prieinamumo pažeidimais, 19 atvejų buvo prarastas duomenų vientisumas. Dažniausiai pažeidžiami asmens tapatybę patvirtinantys asmens duomenys – iš viso per 2022 metus nustatyta 210 tokių atvejų, prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai – 74 atvejai, specialiųjų kategorijų asmens duomenys – 31 atvejis bei kiti asmens duomenys. Šių kategorijų asmens duomenys dažniausiai panaudojami neteisėtai prieigai prie informacinių sistemų, interneto svetainių ir tolesnei neteisėtai veiklai, pvz., kenkimo programinės įrangos platinimui, sukčiavimui, susijusiam su el. prekyba ar pinigų pervedimu ir pan. „Globalus elektroninės erdvės pobūdis ir specifinės jos savybės leidžia teisės pažeidėjams veikti gana saugioje aplinkoje, nukreipti savo veiksmus bet kuria linkme ir veikti bet kurioje vietoje, veikas atlikti labai plačiu mastu, visiškai nepaisant valstybių sienų ir jurisdikcijos“[9] (Štitilis, 2011). Pažymėtina, kad Valstybinė duomenų apsaugos inspekcija 2023 m. pastebėjo įvykusių asmens duomenų saugumo pažeidimų, susijusių su kibernetinėmis atakomis mažėjimą. Valstybinės duomenų apsaugos inspekcijos 2023 metų veiklos ataskaitos duomenimis[10], 2023 metais kibernetiniai incidentai sudarė tik 15 proc. visų 2023 metais įvykusių pažeidimų. Tačiau Valstybinė duomenų apsaugos inspekcija pastebi, kad daugėja asmens duomenų saugumo pažeidimų, kilusių dėl žmogiškosios klaidos: „2023 m. 72 proc. asmens duomenų saugumo pažeidimų įvyko dėl žmogiškosios klaidos (2022 m. tokių asmens duomenų saugumo pažeidimų buvo 60 proc.)“.

Pažymėtina, kad „MVĮ yra pakankamai naivios, susidūrusios su elektroniniais nusikaltimais, nes gali manyti, kad jos nėra tikėtini kibernetinių išpuolių taikiniai. Ši trumparegiška perspektyva lemia mažas investicijas į kibernetinį saugumą, tačiau tikrovė rodo, kad 40 proc. MVĮ dėl šių kibernetinių nusikaltimų patiria kibernetinį poveikį (GOV.UK, 2023).“ (Cartwright A., Cartwright E. ir kt. 2024). ENISA (2020) įvardina šiuos pagrindinius nusikaltimus prieš įmones: „finansinė nauda, įmonių šnipinėjimas, paslaugų sutrikimas,

[8] Valstybinė duomenų apsaugos inspekcija. *Apklausa. Ką galvoja Lietuvos gyventojai?* 2024.
[9] Štitilis, D. (2011). Elektroniniai nusikaltimai. Metodinė priemonė. Vilnius: Mykolo Romerio universitetas. P. 89.
[10] Valstybinė duomenų apsaugos inspekcija. *Valstybinės duomenų apsaugos inspekcijos veiklos ataskaita* 2023.

duomenų pažeidimas, politiniai motyvai, vidinės grėsmės tyčia arba netyčia sukeltos darbuotojų, turto prievartavimas“[11].

Pasak Kuklytės J., Ūso A. (2017) „vienas iš didžiausių iššūkių, su kuriais susiduria informacinė visuomenė, ne tik informacinių ir komunikacinių technologijų įvairovė, bet ir yra kibernetinio saugumo užtikrinimas ir teisinis kibernetinių nusikaltimų reglamentavimas, prevencija, nustatymas“[12]. Vadovaujantis Nacionalinio kibernetinio saugumo 2022 m. ataskaitos duomenimis, iš visų subjektų, patyrusių kibernetinių nusikaltimų poveikį, juridiniai asmenys sudarė 12 proc. 2022 m. iš juridinių asmenų, patyrusių kibernetinių atakų poveikį, dominavo prekybos subjektai (3 proc.). Kitos 2022 m. akivaizdžiau matomos kibernetinės atakos buvo prieš informatikos ar telekomunikacijos paslaugų subjektus, apdirbamosios pramonės subjektus ir transportavimo paslaugų subjektus. 2022 m. kibernetinių atakų prieš juridinių asmenų informacines sistemas dažniausi padariniai – ūkinės veiklos duomenų užšifravimas ar kitoks sugadinimas (29 proc.), taip pat el. pašto adreso pakeitimas ir susirašinėjimo perėmimas (25 proc.), duomenų stebėjimas ar pasisavinimas (19 proc.), duomenų pakeitimas (10 proc.). Duomenų nutekėjimas gali sukelti rimtas pasekmes įmonei, įskaitant finansinius nuostolius bei baudas, reputacijos praradimą, teisines pasekmes ir klientų pasitikėjimo sumažėjimą, todėl MVĮ sektoriuje itin svarbu skirti dėmesį duomenų apsaugai ir prevencijos priemonėms. Pasak Cartwright A., Cartwright E. ir kt. (2024), „nė vienas sektorius nėra apsaugotas nuo kibernetinių grėsmių, pradedant oportunistiniais ir beatodairiškais išpuoliais ir baigiant sudėtingomis ir labai selektyviomis kampanijomis prieš konkrečius subjektus“.

Mokslinis naujumas / teorinis reikšmingumas. „Kibernetinis saugumas tapo rimtu iššūkiu verslui visame pasaulyje, tačiau nepaisant svarbos, kibernetinio saugumo tyrimai, konkrečiai MVĮ kontekste, vis dar yra labai riboti“[13](Tam T. 2021). Europos Sąjungos kibernetinio saugumo agentūra (toliau – ENISA), siekdama aukšto kibernetinio saugumo lygio visoje Europoje kasmet teikia grėsmių aplinkos ataskaitas (angl. *ENISA Threat Landscape,* ETL), kuriose įvardijamos pagrindinės grėsmės, svarbiausios pastebėtos tendencijos, susijusios su grėsmėmis, grėsmės subjektai ir išpuolių metodai, taip pat aprašomos atitinkamos rizikos mažinimo priemonės[14], tačiau pagrindinis dėmesys skiriamas grėsmių poveikiui, o ne prevencijai. Mykolo Romerio universiteto Žmogaus ir visuomenės studijų mokslininkai taip

[11] ENISA 2020. *Threat Landscape*.
[12] Kuklytė J., Ūsas A.. *Informacinės visuomenės iššūkiai: kokios yra kibernetinių nusikaltimų formos? Mokslinių straipsnių rinkinys. Visuomenės saugumas ir viešoji tvarka*. 2021.
[13] Tam, T., Rao, A., & Hall, J. (2021, 109, 102385.). *The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security*.
[14] ENISA. 2021. *Threat landscape.*

pat pripažįsta problemos aktualumą bei teorinį ir praktinį reikšmingumą. 2019 m. balandžio 28-29 d. Mykolo Romerio universitete vyko Erasmus+ strateginės partnerystės tarptautinio projekto "TeBelSI - Informacinio saugumo kompetencijų įgytų neformaliuoju mokymosi būdu sertifikavimas"[15]. Šiuo projektu siekiama sukurti įrankius, suteikiančius asmenims, dirbantiems socialinėse įstaigose, mažose ir vidutinėse įmonėse su informacijos saugumu ir asmens duomenų apsauga savarankiškai įsivertinti savo kompetencijas duomenų apsaugos informacijos saugumo srityje bei esant poreikiui tobulinti turimas kompetencijas bei įgyti naujų būtinų kompetencijų (taip pat bus parengta mokymų programa). Atsižvelgiant į tai, kad įvyko dar tik pirmas susitikimas, galima daryti prielaidą, kad asmens duomenų nutekėjimo privačiame sektoriuje problema vis dar nepraranda aktualumo. Asmens duomenų sampratą bei teisinius asmens duomenų aspektus nagrinėjo Kiškis M., Petraukas R., Rotomskis ir kt. (2006), Štitilis D. (2011), Civilka M., Šlapimaitė L. (2015), Zaleskis J. (2019) ir kiti, tačiau asmens duomenų nutekėjimo prevencija privataus sektoriaus įmonėse dar nėra pilnai išnagrinėta.

Pažymėtina, kad Valstybinė duomenų apsaugos inspekcija teikia visuomenei pranešimus apie įvykusius incidentus bei rengia gaires, rekomendacijas ir prevencines priemones, susijusias su incidentų valdymu, tačiau pasak Šidlausko (2021), „priežiūros institucijų rekomendaciniai dokumentai kritikuojami dėl pernelyg bendro pobūdžio ir dėmesio sutelkimo į teisės teoriją"[16]. Todėl šio magistro darbo tyrimo rezultatai gali būti pritaikyti siekiant vystyti privataus sektoriaus mažų ir vidutinių įmonių gebėjimą užtikrinti asmens duomenų nutekėjimo prevenciją.

Mokslinė problema. Kaip turėtų būti užtikrinama asmens duomenų apsaugos nutekėjimo prevencija Lietuvos mažose ir vidutinėse įmonėse?

Tyrimo objektas: Lietuvos privataus sektoriaus mažo ir vidutinio dydžio įmonės.

Tyrimo dalykas: asmens duomenų nutekėjimo prevencijos aktualumas Pasvalio ir Pakruojo privataus sektoriaus mažo ir vidutinio dydžio įmonėse.

Tyrimo tikslas: identifikuoti kibernetinės brandos lygį Pasvalio ir Pakruojo miestų mažose ir vidutinėse įmonėse.

Uždaviniai:

1. Aptarti asmens duomenų nutekėjimo prevencijos teorinius aspektus.
2. Išryškinti privataus sektoriaus mažų ir vidutinių įmonių pasirengimo asmens duomenų nutekėjimo prevencijos tendencijas.

[15] Mykolo Romerio universitetas. *Įvyko tarptautinio projekto pirmas partnerių susirinkimas*.
[16] Šidlauskas A. *Valstybinės duomenų apsaugos inspekcijos administracinių baudų skyrimo praktika ES šalių kontekste*. 2021. P. 160.

3. Ištirti Pasvalio ir Pakruojo miestų mažo ir vidutinio dydžio privataus sektoriaus įmonių asmens duomenų nutekėjimo prevencijos pajėgumus.
4. Pateikti rekomendacijas privataus sektoriaus mažoms ir vidutinėms įmonėms bei priežiūros institucijoms dėl geriausių praktikų asmens duomenų nutekėjimo prevencijai užtikrinti.

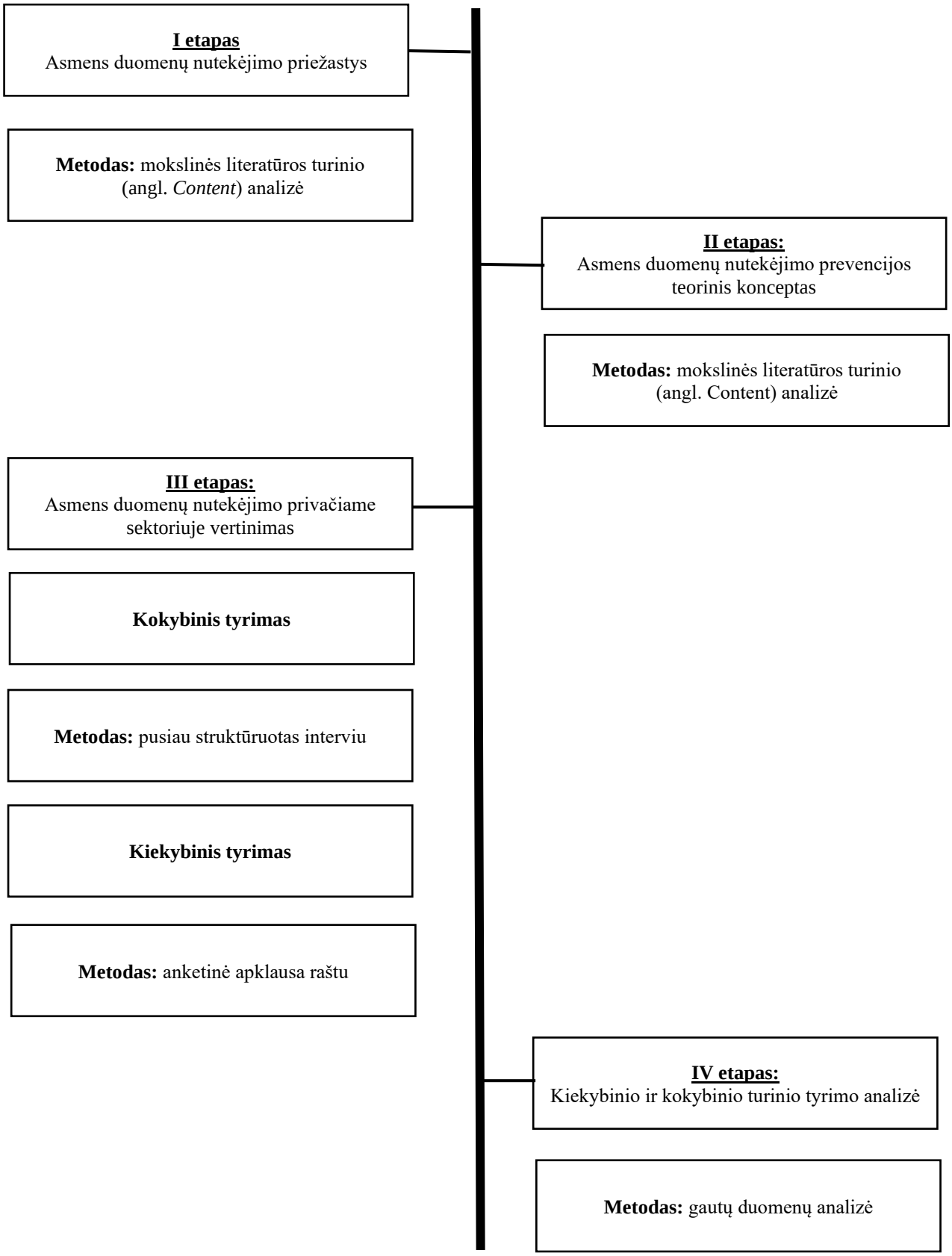
Duomenų rinkimo metodai:

1. Mokslinės literatūros analizė. Metodas atliekamas pagal K. Kardelį (2016), kuris teigia, jog mokslinės literatūros analizė yra neatsiejama darbo dalis, kuri tęsiasi viso mokslinio tyrimo metu.
2. Lyginamoji literatūros analizė. Analizuojant ir interpretuojant duomenis buvo atsižvelgiama į skirtingas autorių pateikiamas įžvalgas siekiant atskleisti įvairias perspektyvas.
3. Duomenų vizualizacijos metodas. Darbe šis metodas naudojamas pateikiant schemas, teiginius, lenteles.
4. Pusiau struktūrizuotas interviu.
5. Apklausa raštu.

Duomenų analizės metodai:

1. Kiekybinė turinio analinė
2. Pusiau struktūrizuoto interviu kokybinė turinio (anglų k. *Content*) analizė ir interpretavimas.
3. Lyginamoji gautų duomenų analizė.

Darbo struktūra. Darbas sudarytas iš 3 dalių. Pirmojoje dalyje nagrinėjami asmens duomenų nutekėjimo privačiame sektoriuje prevencijos aspektai, apžvelgiant asmens duomenų saugumo pažeidimų metodus bei galimas pasekmes. Antrojoje dalyje nagrinėjamas asmens duomenų nutekėjimo prevencijos teorinis konceptas, kuriame aptariama asmens duomenų nutekėjimo prevencija taikant prevencijos priemones ir kt. Trečiojoje dalyje aprašomas kokybinis ir kiekybinis tyrimai. Kokybiniu tyrimu siekiama išsiaiškinti kaip mažo ir vidutinio dydžio įmonių atsakingi už asmens duomenų saugumą asmenys vertina savo darboviečių prevencinį pasirengimą asmens duomenų nutekėjimo atvejams. Kiekybinio tyrimo tikslas išsiaiškinti kaip mažo ir vidutinio dydžio privataus sektoriaus įmonių darbuotojai supranta asmens duomenų saugumo reikalavimus bei su asmens duomenų tvarkymu susijusias rizikas, kaip dažnai yra vykdomi darbuotojų asmens duomenų apsaugos bei kibernetinio saugumo mokymai. Darbo struktūros loginė schema pavaizduota 1 paveiksle.



1 pav. Darbo struktūros loginė schema

Teorinė dalis:

1. ASMENS DUOMENŲ NUTEKĖJIMO PRIVAČIAME SEKTORIUJE TEORINIAI ASPEKTAI

1.1. Asmens duomenų valdymas privačiame sektoriuje

Vadovaujantis visuotine lietuvių enciklopedija, „privatus sektorius – tai šalies ūkio sudėtinė dalis, kuri apima fizinių ir juridinių asmenų ekonominę veiklą, tenkinančią jų privačius interesus – gauti pelno ar pajamų. Privataus sektoriaus pagrindas yra gamybos priemonių ir kitų ekonominių išteklių privati nuosavybė. Lietuvoje privačiame sektoriuje 2018 sukurta daugiau kaip 75 % BVP, dirbo 69,2 % visų darbuotojų“[17]. Privataus sektoriaus įmonės gali būti labai įvairios, pradedant mažomis savarankiškomis verslo įmonėmis ir baigiant didelėmis tarptautinėmis korporacijomis. Lietuvos Respublikos smulkiojo ir vidutinio verslo plėtros įstatymo 3 straipsnyje nurodyta, kad „labai maža įmonė – įmonė, kurioje dirba mažiau kaip 10 darbuotojų ir kurios finansiniai duomenys atitinka bent vieną iš šių sąlygų: įmonės metinės pajamos neviršija 2 mln. Eurų ir (arba) įmonės balanse nurodyto turto vertė neviršija 2 mln. eurų. Maža įmonė – įmonė, kurioje dirba mažiau kaip 50 darbuotojų ir kurios finansiniai duomenys atitinka bent vieną iš šių sąlygų: įmonės metinės pajamos neviršija 10 mln. Eurų ir (arba) įmonės balanse nurodyto turto vertė neviršija 10 mln. eurų. Vidutinė įmonė – įmonė, kurioje dirba mažiau kaip 250 darbuotojų ir kurios finansiniai duomenys atitinka bent vieną iš šių sąlygų: įmonės metinės pajamos neviršija 50 mln. eurų ir (arba) įmonės balanse nurodyto turto vertė neviršija 43 mln. eurų“[18]. Nepriklausomai nuo įmonės dydžio, įmonei tvarkant fizinių asmenų (toliau – duomenų subjektai) asmens duomenis, tokios įmonės bus laikomos asmens duomenų valdytojais. Vadovaujantis Bendrojo duomenų apsaugos reglamento nuostatomis, duomenų valdytojas – „fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise“[19]. Siekiant įgyvendinti Bendrojo duomenų apsaugos reglamento 5 straipsnio 2 d. numatytą atskaitomybės principą, būtent duomenų valdytojui tenka prisiimti didžiausią atsakomybę, nes jis turi laikytis visų duomenų apsaugos principų ir kitų Bendrojo duomenų apsaugos reglamento reikalavimų, bei įrodyti, kad jų laikosi. Didžiosios Britanijos

[17] Visuotinė lietuvių enciklopedija. *Straipsnis. Privatus sektorius*.
[18] Lietuvos Respublikos smulkiojo ir vidutinio verslo plėtros įstatymo Nr. VIII-935 pakeitimo įstatymas. 2017 m. sausio 12 d. Nr. XIII-192.
[19] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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).

informacijos ir duomenų apsaugos institucija (ICO) nurodo, kad „jei maža organizacija tvarko ir naudoja žmonių asmeninę informaciją, vykdydami įprastinę verslo veiklą, tai jie bus laikomi asmens duomenų valdytojais. Bendrasis duomenų apsaugos reglamentas taikomas nuo tada, kai renkami asmens duomenys ir tai apima įvairaus dydžio įmones, nuo individualių prekybininkų ir sau dirbančių asmenų iki didelių pasaulinių korporacijų“[20]. Įmonės dažniausiai renka vartotojų bei darbuotojų vardą, pavardę, elektroninio pašto adresą, paso bei tapatybės kortelės duomenis, sveikatos duomenis, buvimo vietos duomenis, telefono numerį, atvaizdą bei daugelį kitų asmens duomenų kategorijų, todėl būtina užtikrinti asmens duomenų nutekėjimo prevenciją „siekiant skaitmeniniame amžiuje stiprinti pagrindines asmenų teises ir sudaryti palankesnes sąlygas vykdyti verslo veiklą, nustatant aiškesnes bendrojoje skaitmeninėje rinkoje įmonėms ir viešojo sektoriaus institucijoms taikomas taisykles“[21](Šidlauskas A. 2021).

Pasak Civilkos M., Šlapimaitės L (2015) „asmens duomenys tapo ir elektroninio verslo dalimi“. Bendrovės vartotojų apsilankymo svetainėse metu renka kompiuterio naudotojo duomenis (pvz. IP adresas, nustatyta kalba, laiko zona, programinė įranga, slapukai ir kt.), kuriuos siunčia kelioms skirtingose valstybėse veikiančioms rinkodaros, reklamos ir kita veikla besiverčiančioms bendrovėms. Direktyvoje 95/46/EB pateikiama ganėtinai plati asmens duomenų apibrėžtis: „Asmens duomenys reiškia bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais“[22]. Europos Komisijos interneto svetainėje pateikiama, kad „asmens duomenys yra bet kokia informacija, susijusi su gyvu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta. Skirtinga informacija, kuri surinkta kartu gali atskleisti konkretaus asmens tapatybę, taip pat yra asmens duomenys. Asmens duomenys, iš kurių pašalinta asmeninė informacija, kurie yra užšifruoti ar kuriems yra suteikti pseudonimai, bet kuriuos galima panaudoti iš naujo nustatant asmens tapatybę, išlieka asmens duomenimis ir jiems taikomas Bendrasis duomenų apsaugos reglamentas. Asmens duomenys, kurių anonimiškumas užtikrintas taip, kad asmens tapatybė negali arba nebegali būti nustatyta, nebelaikomi asmens duomenimis. Kad asmens

[20] Didžiosios Britanijos duomenų ir informacijos apsaugos institucija (ICO).
[21] Šidlauskas A. *Valstybinės duomenų apsaugos inspekcijos administracinių baudų skyrimo praktika ES šalių kontekste*. 2021. P.154.
[22] 29 straipsnio duomenų apsaugos darbo grupė. *Nuomonė 4/2007 dėl asmens duomenų sąvokos*. 2007.

duomenys būtų iš tiesų anoniminiai, anonimiškumas turi būti užtikrintas negrįžtamai“[23]. Bendrojo duomenų apsaugos reglamento 4 straipsnyje nurodyta, kad asmens duomenys - „tai 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“. Vadinasi, tais atvejais, kai įmonės tvarko ne anoniminius fizinių asmenų duomenis, bei sprendžia dėl šių duomenų tvarkymo tikslų bei priemonių, jie yra laikyti duomenų valdytojais. Pažymėtina, kad „duomenų tvarkymas – tai 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“ (Bendrojo duomenų apsaugos reglamento 4 straipsnio 2 dalis).

Apibendrinant galima teigti, kad skaitmeniniame amžiuje mažo ir vidutinio dydžio įmonės tvarko vis daugiau asmens duomenų, todėl šioms įmonėms, kaip duomenų valdytojams kyla pareiga užtikrinti asmens duomenų nutekėjimo prevenciją.

1.2. Asmens duomenų nutekėjimo samprata

Asmens duomenų nutekėjimo sąvoką galime prilyginti asmens duomenų konfidencialumo pažeidimo sąvokai. Vadovaujantis Bendrojo duomenų apsaugos reglamento 4 straipsnio 12 punktu[24], asmens duomenų saugumo pažeidimas – „tai saugumo pažeidimas, dėl kurio netyčia ar neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga“. Siekiant išsiaiškinti konfidencialumo pažeidimo sąvoką, būtina apžvelgti mokslinę bei metodinę literatūrą. Pasak S. Jastiugino, „dauguma informacijos saugumo apibrėžčių jau daugiau kaip dvidešimt metų remiasi trimis informacijos saugumo tikslais (CIA triada). Pagal CIA triadą, įvardijama, kad informacijos saugumo tikslas – užtikrinti informacijos

[23] Europos komisija. *Kas yra asmens duomenys*?
[24] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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).

konfidencialumą (*confidentiality*), vientisumą (*integrity*) ir prieinamumą (*availability*)“[25]. Pasak Maximiano A., Pinto G. (2021), „konfidencialumo pažeidimus galime laikyti informacijos saugumo pažeidimais. Konfidencialumas, vientisumas ir prieinamumas, kurie dar vadinami CIA triada, yra projektavimo modelis, skirtas apibrėžti organizacijų informacijos saugumo politiką. Kadangi duomenys yra susiję su daugeliu organizacijos viduje atliekamų operacijų, jų konfidencialumas yra pagrindinis rūpestis, todėl organizacijoje turi būti taikomos tam tikros procedūros ir taisyklės, siekiant apibrėžti, kas ir kam turi prieigą prie duomenų ir informacijos. Vientisumas ir prieinamumas yra susiję su duomenų patikimumu ir tikslumu, kuriuos gali pasiekti įgalioti asmenys. Taigi informacijos saugumo standartai ir sistemos yra pagrįsti politikos ir kontrolės įgyvendinimu, siekiant valdyti saugumą ir riziką organizaciniu lygmeniu“[26].

Vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 7 straipsnio nuostatomis, „Valstybinė duomenų apsaugos inspekcija stebi, kaip laikomasi asmens duomenų apsaugos reikalavimų“[27]. Valstybinės duomenų apsaugos inspekcijos direktorius, siekdamas padėti duomenų valdytojams atlikti pareigą pranešti apie asmens duomenų saugumo pažeidimus Valstybinei duomenų apsaugos inspekcijai, vadovaudamasis Bendrojo duomenų apsaugos reglamento 33 straipsniu bei Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo 29 straipsniu, 2018 m. rugpjūčio 29 d. parengė įsakymą dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo[28], kuriame nustatė, kad duomenų valdytojai ir (ar) tvarkytojai, teikdami informaciją apie įvykusį asmens duomenų apsaugos pažeidimą turi nurodyti asmens duomenų saugumo pažeidimo tipą. Formoje yra pateikiami trys asmens duomenų saugumo pažeidimų tipai: „asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas), asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas), asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)“. Pažymėtina, kad asmens duomenų konfidencialumo praradimas nebūtinai siejamas su kibernetinio saugumo pažeidimais, tačiau asmens duomenų nutekėjimo atvejai tapatinami su kibernetinių saugumo priemonių netaikymu

[25] Jastiuginas. S (2012). *Integralus informacijos saugumo valdymo modelis*. P. 8..
[26] Maximiano A., Pinto G. *Informacijos saugumas ir kibernetinio saugumo valdymas: atvejo tyrimas su MVĮ Portugalijoje.* 2021.
[27] 1996 m. birželio 11 d. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas Nr. Nr. I-1374 (Suvestinė redakcija nuo 2024-01-01).
[28] 2018 m. rugpjūčio 29 d. *Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas „Dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“ Nr. Nr. 1T-82(1.12.E).*

ir (arba) netinkamu taikymu. Saugumo garantijų principas yra pagrindinis privatumo principas, nustatytas 1980 m. bei 2013 m. peržiūrėtose Ekonominio bendradarbiavimo ir plėtros organizacijos (EBPO) gairėse, reglamentuojančiose privatumo apsaugą. Šio pagrindinio privatumo principo esmė: „asmens duomenys turi būti apsaugoti pagrįstomis saugumo priemonėmis nuo tokių pavojų kaip duomenų praradimas ar neteisėta prieiga, sunaikinimas, naudojimas, keitimas ar atskleidimas)“.

1.3. Asmens duomenų nutekėjimo prevencijos samprata

Visuotinės lietuvių enciklopedijos duomenimis[29], prevencija (lot. *praeventio*) – išankstinis kelio užkirtimas, užbėgimas už akių kokiam nors neigiamam reiškiniui ar įvykiui. „Plačiąja prasme nusikaltimų prevencija – visa tai, kas padeda palaikyti teisėtvarką. Nusikaltimų prevenciją traktuojant plačiąja prasme, ši veika išskaidoma į daugelį socialinių procesų, todėl negalima išskirti jos specifinių bruožų. Kiti autoriai traktuoja prevenciją siaurąja prasme. Tokio požiūrio pagrindas – ryškus kryptingumas, kai prevencinėmis priemonėmis pripažįstamos tik tos priemonės, kurios užkerta kelią nusikaltimams. Pagrindinis nusikaltimų prevencijos tikslas – saugoti tokias svarbias socialines vertybes, kaip valstybės, visuomenės ir piliečių interesai“ (Štitilis, 2011, p. 88). Siekiant išsiaiškinti asmens duomenų nutekėjimo prevencijos sampratą, būtina aptarti kibernetinio saugumo politikos įtaką asmens duomenų nutekėjimo prevencijai.

Lietuvoje kibernetinio saugumo politika formuojama vienu pagrindinių įstatymų – Lietuvos kibernetinio saugumo įstatymu, kuriuo siekiama palaikyti aukštą kibernetinio saugumo lygį. Šiame įstatyme pateikiama kibernetinio saugumo sąvoka, kuri nusako, kad „kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą. Paprastai tariant, tai yra veiksmai, kurių imamasi norint apsaugoti kibernetinę aplinką. Tai vidinių teisės aktų, organizacinių procesų ir techninių priemonių, leidžiančių išvengti, aptikti ir reaguoti į kibernetinius incidentus, rizikų įvertinimo visuma“[30].

[29] Visuotinė lietuvių enciklopedija. Straipsnis. Prevencija.
[30] Nacionalinis kibernetinio saugumo centras. *Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas?*. 2020.

Nacionalinis kibernetinio saugumo centras verslui skirtame „Vadove“ (2020) pažymi, kad „siekiant užtikrinti kibernetinio saugumo prevenciją, būtina laikytis konfidencialumo, vientisumo bei prieinamumo principų“[31]. Maži ir vidutiniai verslai taiko minimalias apsaugos priemones, o kartais būdami įsitikinę, kad yra niekam neįdomūs, nesisaugo išvis. Būtent tokių įmonių ir ieško sukčiai. Pažymėtina, kad 93 proc. atakų pagrindinis motyvas – finansinė nauda. Be kita ko, Nacionalinis kibernetinio saugumo centras „Vadove verslui“ (2020) taip pat pažymi, kad „kibernetiniai incidentai gali grėsti visur, o bandymų įsilaužti į įmonių tinklus ar darbuotojų paskyras skaičius tik didėja, ir mažai tikėtina, kad ši tendencija artimiausiu metu keisis. Būtina suvokti, kad kibernetinės atakos auka gali tapti kiekviena įmonė, nepriklausomai nuo jos dydžio, vykdomos veiklos ar naudojamų kibernetinio saugumo priemonių modernumo. Būtina suprasti, kad visos įmonės tam tikru mastu naudoja kibernetinę erdvę ir ja remiasi pateikti mokesčių deklaracijas, bendrauti su klientais el. paštu ir pan.“[32]. Kibernetinių atakų metu įvykus konfidencialumo pažeidimui, nuteka ir klientų, darbuotojų asmens duomenys. Vadovaujantis Valstybinės duomenų apsaugos inspekcijos pranešimų apie asmens duomenų saugumo pažeidimus apžvalga[33], per 2023 m. I pusmetį Lietuvoje gauta apie 130 asmens duomenų saugumo pažeidimų, o paveiktų vartotojų skaičius sudarė 328 929. Net 87 proc. visų pažeidimų sudaro asmens duomenų konfidencialumo pažeidimai. Privatūs juridiniai asmenys (išskyrus ER paslaugų ar tinklų teikėjus) sudaro 40 proc. duomenų valdytojo pobūdžio.

Nacionalinio kibernetinio saugumo centro duomenimis, vienas žymiausių Lietuvoje nustatytų Bendrojo duomenų apsaugos reglamento pažeidimų – įmonei „CityBee“ taikyta 110 tūkst. eurų bauda už įmonės vartotojų duomenų konfidencialumo neužtikrinimą[34]. Šios kibernetinės atakos metu buvo pavogti bei paskelbti 110 tūkst. duomenų subjektų asmens duomenys. Nustatyta, kad įmonė netinkamai įgyvendino technines ir organizacines asmens duomenų saugumo priemones pagal Bendrojo duomenų apsaugos reglamento 24 straipsnį, to pasėkoje įvyko konfidencialumo pažeidimas. Duomenų valdytojai tvarkydami duomenų subjektų asmens duomenis privalo įgyvendinti tinkamas technines ir organizacines duomenų saugumo priemones užtikrinant asmens duomenų nutekėjimo prevenciją.

Siekiant išvengti tokių asmens duomenų pažeidimų, įmonės privalo suprasti, kad duomenų saugumas itin svarbus, kintantis bei nuolatinis procesas, kurį reikia reguliariai stebėti

[31] Nacionalinis kibernetinio saugumo centras. *Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas?*. 2020.
[32] Cartwright A. Cartwright E. *Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers and Security* 131 (2023) 103288. P.5.
[33] Valstybinė duomenų apsaugos inspekcija. „*Asmens duomenų saugumo pažeidimai Lietuvoje 2023 m. I pusmetį.*“.
[34] Nacionalinis kibernetinio saugumo centras. *Svarbiausia Lietuvos kibernetinio saugumo būklės statistika ir tendencijos 2021 m. – 2022 m. I ketv.*.

bei atnaujinti. Pagal šį nustatytą procesą, būtina taikyti parinkti bei taikyti kibernetinio saugumo priemones ir reguliariai atlikti kibernetinio bei asmens duomenų apsaugos auditus, rizikos vertinimus bei imtis prevencinių priemonių atsižvelgiant į auditų bei rizikos vertinimo rezultatus. Nacionalinio saugumo centras bei Valstybinė duomenų apsaugos inspekcija reguliariai teikia rekomendacijas, bei mokymus, kad padidintų verslo įmonių informuotumą apie saugumo priemones, tačiau MVĮ vis dar susiduria su iššūkiais įgyvendinant kibernetinį saugumą. Cartwright A. ir Cartwright E. teigia, kad „apskritai kalbant įrodymai rodo, kad kibernetinio sąmoningumo didinimo kampanijos turi ribotą poveikį elgesiui, o smulkus verslas nėra pakankamai kibernetinis“[35]. Tačiau pasak Vishwanath A., (2020) „kibernetinė higiena reikšmingai prognozuoja žmogaus kibernetinės sąveikos aspektus, kurie yra labai svarbūs kibernetiniam saugumui“[36]. Mokslininkai įžvelgia du kibernetinių mokymų modelius, galinčius padėti užtikrinti asmens duomenų nutekėjimo prevenciją: nuspėjamasis modelis bei prognozavimo modelis. Pasak Barati M., ir kt. (2022) „nuspėjamasis modelis gali būti įžvalgus renkantis savo investicijų ir mokymų kryptį pagal būsimą duomenų pažeidimų tikimybę ir dažnesnių duomenų pažeidimų tipą. Išsamesnių duomenų apie ankstesnius duomenų pažeidimo incidentus prieinamumas kartu su pažeidimų charakteristikomis, tokiomis kaip priežastys, pažeistų duomenų tipas, įmonės išlaidos, reagavimo ir atkūrimo strategijos ir jų veiksmingumas gali suteikti daugiau vertės nuspėjamiesiems modeliams, pridedant pasiūlymų dėl reagavimo planų ir išteklių paskirstymo <...> , o tuo tarpu konkrečiam sektoriui skirtų prognozavimo modelių turėjimas gali padėti organizacijoms kompetentingiau pasirengti kibernetiniams incidentams ir sumažinti bendrą riziką“[37].

Pažymėtina, kad Verslo žinių atliktame EY kibernetinio saugumo rizikų tyrime nurodoma, kad „įmonės turi per daug komunikacijos platformų ir sistemų, kurios kenkėjams leidžia pasiekti įvairius duomenis. Todėl įmonės raginamos įvertinti ir optimizuoti savo IT ūkį, investuodamos į technologijų plėtrą, nuosekliai įgyvendinti integruotus saugumo sprendimus“[38]. Saugumo sprendimų įgyvendinimas neatsiejamas nuo darbuotojų sąmoningumo bei kibernetinės higienos laikymosi.

Atkreiptinas dėmesys, kad tvarkomų asmens duomenų auditai bei savalaikis rizikų įvertinimas, gali padėti išvengti nuostolių, skatinti kibernetinio saugumo sąmoningumą, gebėti

[35] Cartwright A. Cartwright E. *Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies*. Computers and Security 131 (2023) 103288. P.2.
[36] Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. *Cyber hygiene: The concept, its measure, and its initial tests*. 2020.
[37] Barati M., Yankson B., *Predicting the Occurrence of a Data Breach*. 2022
[38] Verslo žinios. *Kibernetinių atakų skaičius auga sparčiai: lemia ir geopolitika, ir nesutvarkytas IT ūkis*. 2024.

įsivertinti ir žinoti galimus pažeidžiamumus bei jiems taikomas saugumo priemones. Taigi, galime išskirti du rizikų analizės tipus:

- „Išankstinis įvertinimas – vykdomas prieš tai, kai dar neįvyko incidentas;
- Pavėluotas įvertinimas – vykdomas jau po incidento“ (Štitilis, 2011, p. 89).

Vadovaujantis Bendrojo duomenų apsaugos reglamento 32 str. 1 d. d. p., turi būti ne tik įgyvendinamos saugumo priemonės, tačiau taip pat turi būti užtikrintas reguliarus duomenų saugumo priemonių tikrinimo, vertinimo ir veiksmingumo vertinimo procesas. „Informacijos saugumas yra vienas didžiausių iššūkių, su kuriuo susiduria organizacijos ir institucijos. Pastaraisiais metais elektroninių nusikaltimų dažnis ir mastas išaugo – kasdien atsiranda naujų būdų pavogti, keisti ir sunaikinti informaciją arba išjungti informacines sistemas“[39] (Damaševičius R., Venčkauskas A. ir kt.. 2021). Pasak Romansky R. P. ir Noninska I. S., (2020). Informacijos saugumas ir asmens duomenų apsauga yra nuolat besikeičiančios sritys. Joms pokytį daro nuolatinė technologijų pažanga. Todėl duomenų valdytojams tenka nuolat ieškoti naujų asmens duomenų prevencijos metodų bei būdų. Pasak Zaleskio J. (2019) „ketvirtosios pramonės revoliucijos pasaulis ištrins ribą tarp virtualios ir fizinės realybės, bus generuojami dideli duomenų, įskaitant asmens duomenis kiekiai, ko pasėkoje duomenys gali virsti religija ir ideologija – *dataizmu*. Bet kokia pažanga kelia pavojų, galimybės kelia riziką, todėl pavojų ir rizikos valdymas – neišvengiama pažangos dalis“[40].

1.4. Informacijos saugumo ir duomenų apsaugos struktūrų organizavimas

Technologijų naudojimo rizika bei asmens duomenų apsaugos pažeidimai didėja eksponentiškai, todėl ypatingai svarbu aptarti ir įvertinti pagrindinius asmens duomenų saugumo organizavimo principus.

Privatumas – tai pagrindinė vertybė, kuri saugoma tarptautiniuose ir regioniniuose dokumentuose. „Asmens teisės į privatumą turinį sudaro keturi savarankiški ir tarpusavyje susiję elementai:

- *Informacinis privatumas* – yra susijęs su duomenų apie asmenį tvarkymu ir vadinamas asmens duomenų apsauga: t. y. kai asmuo pats gali disponuoti savo asmens duomenimis, žinoti apie savo asmens duomenų tvarkymą, susipažinti su savo asmens duomenimis, reikalauti ištaisyti duomenis ir pan.;

[39] Damaševičius R., Venčkauskas A., Toldinas J. Grigaliūnas Š.. „*Ensemble-based classification using neural networks and machine learning models for windows pe malware detection* „// Electronics. Basel : MDPI. ISSN 2079-9292. 2021, vol. 10, iss.4, art. no. 485, p. 1-23. DOI: 10.3390/electronics10040485.

[40] Julius Zaleckis. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. 2019. Monografja. P.18.

- *Fizinis privatumas* (kūno neliečiamumas), t. y. žmogui nesutikus, jam negali būti atliekami jokie medicininiai ar moksliniai bandymai (pavyzdžiui, priverstinai atliekami narkotikų testai ir pan.);
- *Komunikacinis privatumas*, t. y. asmens susirašinėjimo, pokalbių telefonu, telegrafo pranešimų ir kitokio susižinojimo neliečiamumas;
- *Teritorinis privatumas*, t. y. asmens būsto arba teritorijos neliečiamumas“ (Kiškis M. ir kt., 2006)”.

„Privatumas – tai asmens dar asmenų grupės gebėjimas apsaugoti privatų gyvenimą ir privačią aplinką, įskaitant informaciją apie save“ (Radi P. Romansky, ir Irina S. Noninska). Privatumo sritis iš dalies sutampa su asmeninės informacijos konfidencialumu ir jos apsauga (prieiga, naudojimas, platinimas, perdavimas ir pan.), dėl šios priežasties kiekvienas asmuo turi teisę į asmens duomenų apsaugą. Pasak Zaleckio J.(2019), „duomenų apsaugos teisėje pirmiausia reikėtų skirti privatumo ir teisės į privatumą sąvokas. Žodis „privatumas“ įvardija asmens teisės objektą, t. y. gėrį, kurį saugo teisė. Teisė į privatumą (arba privataus gyvenimo apsaugą) reiškia asmens subjektyvią teisę tą gėrį apsaugoti ir šios teisės turinį“.

Europos Komisijos pateikimas informacijos saugumo apibrėžimas – „tai tinklų ir informacinių sistemų apsauga nuo žmogaus klaidų, stichinių nelaimių, techninių gedimų ar kenkėjiškų atakų“, apimanti visas informacines ir ryšių technologijas bei informacinių technologijų paslaugas skaitmeniniame amžiuje. Mokslininkai teigia, kad „pastaruoju metu atlikta nedaug tyrimų, susijusių su „Informacijos turto“ sritimis ir veiksmingo jos valdymo gerinimas įvairiose aplinkose ir sistemose gali būti valdomas daugiausia per žmonių sąmoningumą“[41] (Pawar ir Palivela H.. 2023). ICDPPC (2019) taip pat iškelia žmogiškųjų klaidų bei darbuotojų sąmoningumo lygio problemą bei konferencijos metu pateikia sprendimą dėl žmogiškųjų klaidų valdymo: „skatinti tinkamas saugumo priemones, kad būtų išvengta žmogiškųjų klaidų, dėl kurių gali būti pažeisti asmens duomenys, įskaitant:

- Kurti darbo vietų kultūrą, kurioje privatumas ir asmens duomenų saugumas yra organizacijos prioritetai, be kita ko, periodiškai įgyvendinant darbuotojų mokymo, švietimo ir informavimo programas apie jų privatumo ir saugumo įsipareigojimus bei grėsmių asmens duomenų saugumui aptikimą ir pranešimą apie jas;
- Sukurti patikimą ir veiksmingą duomenų apsaugos ir privatumo praktiką, procedūras ir sistemas, įskaitant privatumo didinimą kuriant, eksploatuojant ir valdant sistemas ir investicijų didinimą į bendro saugumo padėties gerinimą, atsižvelgiant į žinomą saugumo riziką, ir

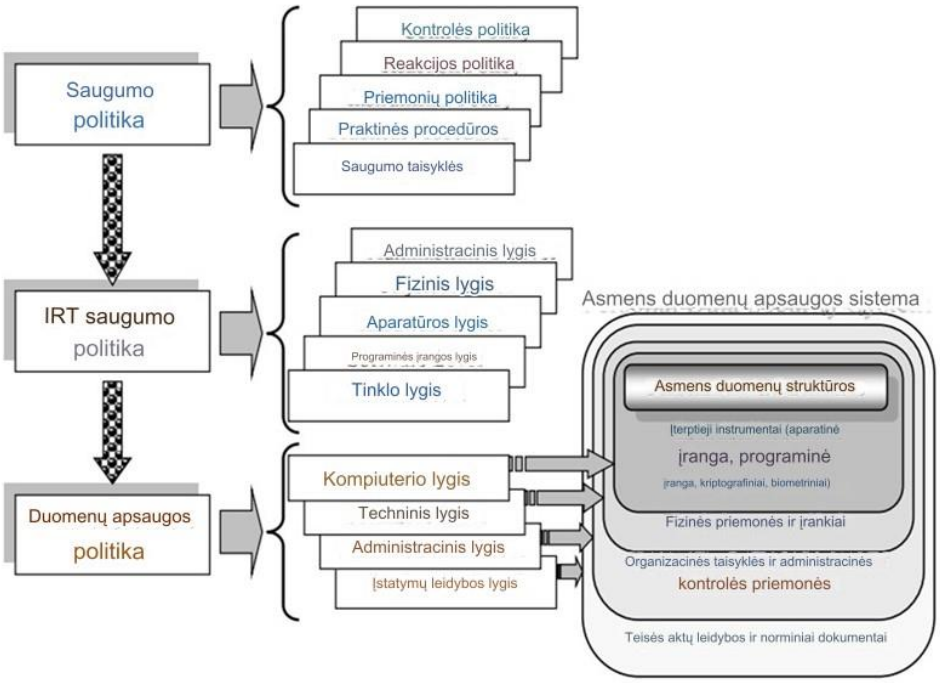
[41] Pawar ir Palivela H.. LCCI: *A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)*. (2023). P. 8.

naudotojo lygmeniu diegiant technologijas, papildančias naudotojų švietimą, siekiant sumažinti kredencialų pažeidimo ir netyčinio asmens duomenų atskleidimo neteisėtiems gavėjams riziką“[42] (ICDPPC, 2019).

Siekiant vykdyti patikimą ir veiksmingą duomenų apsaugos ir privatumo praktiką, būtina suprasti terminus. Informacinių išteklių apsaugoje Romansky R. P. ir Noninska I. S. (2020) išskiria šiuos specifinius terminų skirtumus:

- „*Informacijos saugumas* – tai informacijos apsauga visomis įmanomomis formomis (elektronine, spausdinta ar kitomis);
- *Kompiuterių sauga* apima kompiuterinių sistemų ir tinklų funkcionavimą bei jų apdorojamą informaciją;
- *Informacijos apsauga* apima rizikos valdymo praktiką, susijusią su informacijos apdorojimu, saugojimu ir perdavimu, įskaitant tam tikslui skirtas sistemas ir procesus, kurių pagrindinis tikslas yra užkirsti kelią duomenų praradimui kritinėse situacijose“.

Asmens duomenų apsauga nustato asmenų ir visuomenės santykius, kuriuos pristato valdžios institucijos, įmonės, viešosios ir privačios organizacijos bei kiti subjektai, tvarkantys asmens duomenis. Pasak Romansky R.P, ir Noninska I.S (2020), visi duomenų valdytojai privalo parengti ir taikyti aiškią duomenų apsaugos politiką kaip Informacijos saugumo politikos ir Saugos politikos apskritai dalį. Žr. 2 pav.:

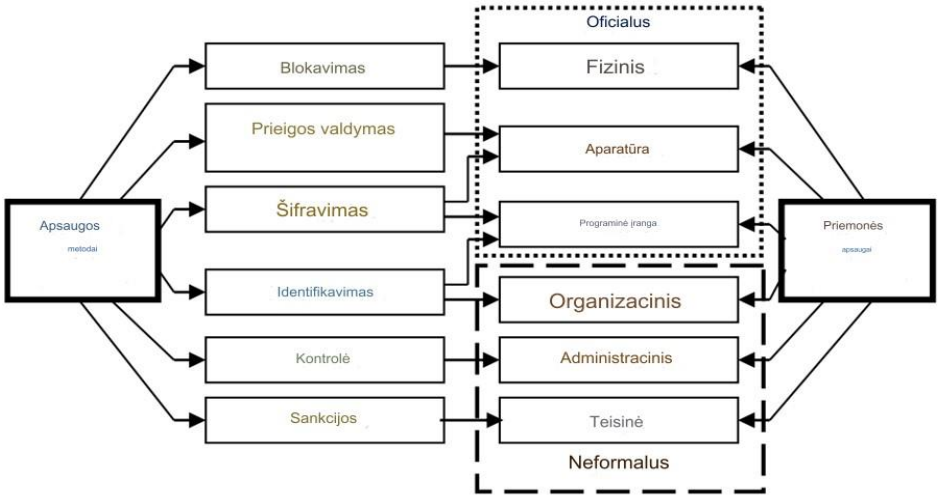


Šaltinis: Romansky R.P. ir Noninska I. S. (2020)

2 pav. Duomenų apsaugos politikos organizacinė struktūra

[42] ICDPPC. *Resolution to address the role of human error ir personal data breaches*. 2019.

Autoriai Romansky R.P. ir Noninska I.S. (2020) taip pat pateikia informacijos ir duomenų apsaugai naudojamų metodų ir priemonių santrauką bei jų ryšį organizuojant asmens duomenų apsaugos sistemą, žr. 3 pav.



Šaltinis: Romansky R. P. ir Noninska I. S. (2020)

3 pav. Duomenų apsaugos organizavimo metodai ir priemonės

Autoriai išskiria šiuos metodus:

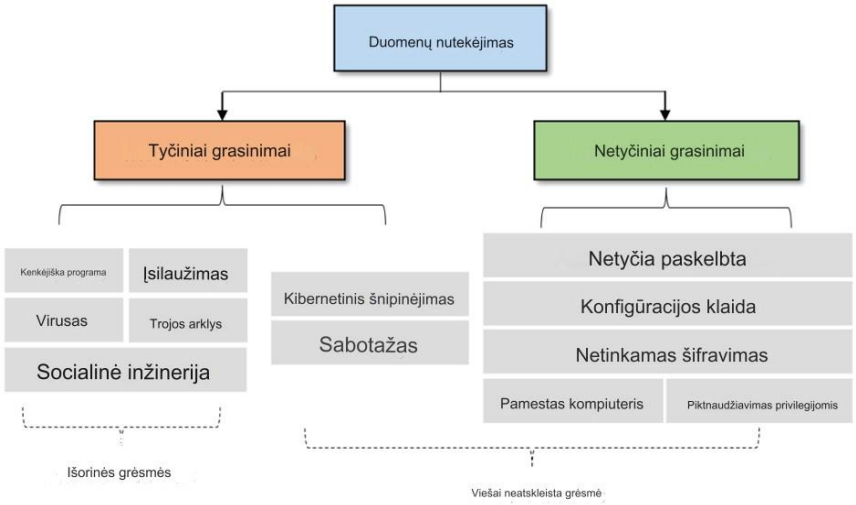
- *„Blokavimas* – neleidžia neteisėtam vartotojui patekti į patalpas, kuriose saugomi duomenys;
- *Prieigos valdymas* – užtikrina saugų visų informacinių išteklių naudojimą ir visų sistemos resursų naudojimą, patikrinant kiekvienam vartotojui iš anksto nustatytas prieigos teises;
- *Šifravimas* – suteikia galimybę naudoti kriptografinius algoritmus duomenims užšifruoti, kad jie būtų nesuprantami neteisėtam vartotojui;
- *Identifikavimas* – personalo ir atskirtų sistemos komponentų, kurie yra užregistruoti kaip teisėti vartotojai ir kuriems nustatytos prieigos teisės identifikavimas;
- *Kontrolė* – metodai, apsaugantys duomenis nuo teisėtų vartotojų neteisėtos veiklos;
- *Sankcijos* – apsaugos programoje aprašomos vidinės informacijos tvarkymo ir naudojimo taisyklės bei vartotojų atsakomybė pagal teisės normas ir įstatymus“.

Apibendrinant galima teigti, kad informacijos saugumo valdymas apima visą saugumo priemonių diegimą visoje įmonėje, aprėpiant technines, organizacines bei žmogiškųjų išteklių perspektyvas.

1.5. Asmens duomenų nutekėjimo priežastys

1.5.1. Išorinės bei vidinės priežastys

Pasak Cheng L., ir kt. (2017), „duomenų nutekėjimą gali sukelti tyčinis ir išorinis informacijos pažeidimas (pvz., duomenų vagystė arba sabotažas, kurį atlieka viešai neatskleista informacija) arba netyčia (pvz., darbuotojų ir partnerių netyčia atskleista jautri informacija). Viešai neatskleistų išpuolių motyvai yra įvairūs, įskaitant įmonių šnipinėjimą, siekį pakenkti darbdaviui ar išpirkos reikalavimus. Atsitiktiniai asmens duomenų nutekėjimai dažniausiai atsiranda dėl netyčinės veiklos prastai organizuojant verslo procesus, pvz., netinkamų prevencinių technologijų ir saugumo politikos taikymo arba darbuotojų nepriežiūros“[43]. Cheng L. ir kt. (2017) pateikia duomenų nutekėjimo grėsmių klasifikaciją, kuri sudaryta taikant išorės bei vidaus grėsmių klasifikacijos metodą, žr. 4 pav.. Šis metodas pagrįstas duomenų nutekėjimo priežastimis. Vienas klasifikavimo metodas nurodo tyčia ar netyčia nutekinami duomenys, o kitas – šalių identifikavimu. Autoriai išskiria, kad šalys gali būti vidinės (darbuotojai) arba išorinės (pašaliniai asmenys/tiekėjai). Išorinius duomenų pažeidimus paprastai sukelia kenkėjiškos programos, įsilaužimai, virusai, socialinė inžinerija. Ypatingai atkreipiamas dėmesys į socialinę inžineriją, kurios atakos (pvz. sukčiavimo) tampa vis sudėtingesnės, darbuotojams neatpažįstamos, todėl jie perduoda vertingus įmonių duomenis kibernetiniams nusikaltėliams. Tuo tarpu vidinis duomenų nutekėjimas dažniausiai gali atsirasti dėl darbuotojų tyčinių veiksmų (pvz. šnipinėjimo už atlygį ir pan.) arba dėl netyčinių klaidų, netinkamų duomenų saugumo užtikrinimui skirtų prevencinių priemonių taikymo.



Šaltinis: Cheng L. , Liu F., Yao D. (2017).

4 pav. Duomenų nutekėjimo grėsmių klasifikacija

[43] Cheng L. , Liu F., Yao D. *Enterprise data breach: causes, challenges, prevention, and future directions*. 2017.

Vadovaujantis Bendrojo duomenų apsaugos reglamento 32 str. 1 d., „sprendžiant dėl duomenų saugumo priemonių įgyvendinimo, turi būti atsižvelgiama į technines galimybes, įgyvendinimo sąnaudas, duomenų tvarkymo aprėptį, aplinką ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms“ (Zaleskis. J. 2019). Mažos įmonės gali neturėti galimybių įdiegti pažangesnių saugumo priemonių, pvz. įsibrovimo aptikimo sistemų arba saugos informacijos ir įvykių valdymo sistemų, kurios galėtų aptikti sudėtingesnes atakas ir į jas reaguoti. MVĮ taip pat gali trūkti išteklių, kad galėtų teikti nuolatines darbuotojų mokymo ir informavimo programas, skirtas užkirsti kelią socialinės inžinerijos atakoms. Be tinkamo mokymo, darbuotojai gali netyčia pakenkti įmonės sistemų saugumui, tapdami šių atakų aukomis. Pasak Osborn ir Simpson (2017), „maži ištekliai ir pinigų išleidimo būdai riboja kibernetinio saugumo gerosios praktikos ir atsparumo priemonių įgyvendinimo mastą. Mažos žinios taip pat yra tam tikra išteklių apribojimo forma, tačiau sprendimus priimančių asmenų supratimas apie didėjančias klaidų kainas gali paskatinti daugiau investicijų į saugumą nukreipti į žmogiškuosius išteklius mažose organizacijose“[44].

Profesinių paslaugų bendrovės EY paskelbtas naujausias kibernetinio saugumo rizikų tyrimas rodo, kad „iššūkius organizacijose lemia darbuotojų, kurie ne iš IT srities, žinių stygius – darbuotojai turi per mažai patirties ir supratimo, kaip vyksta kibernetiniai incidentai, nesugeba nuo jų apsisaugoti ir identifikuoti laiku“[45]. MVĮ taip pat gali trūkti išteklių reguliariai tikrinti pažeidžiamumą ir skverbties testus, kurie gali padėti nustatyti ir pašalinti galimus saugumo trūkumus. „Mažai organizacijų gali sau leisti išvystyti apsaugą, kuri apsaugotų jų kompiuterių sistemas nuo bet kokios rizikos (jeigu tokia apsauga išvis galima). Tai daug kainuoja. Dažnai sulyginama apsaugos kaina su rizika. Saugumo lygis, su kuriuo organizacija sutinka, vadinamas prieinama rizika“ (Štitilis, 2011, p. 88).

Pasak Pawar ir Palivela H. (2023), įvairių tyrimų metu nustatyta, kad MVĮ susiduria su įvairiais iššūkiais kai kalbama apie kibernetinio saugumo įgyvendinimą, t. y. „finansų trūkumas, nesugebėjimas jiems rasti tinkamų kibernetinio saugumo kontrolės priemonių ir kvalifikuotų išteklių trūkumas“[46]. Taip pat MVĮ įmonėse trūksta informacinių technologijų specialistų, duomenų apsaugos pareigūnų, todėl duomenų apsaugos nutekėjimo incidentai gali likti nepastebėti. Dėl šių incidentų, gali būti pažeidžiami darbuotojų bei klientų (bendrai -

[44] Osborn M., Simpson A. *Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study.* 2017. P.491.
[45] Verslo žinios. *Kibernetinių atakų skaičius auga sparčiai: lemia geopolitika, ir nesutvarkytas IT ūkis*. 2024.
[46] Pawar ir Palivela H.. *LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs).* 2023. P. 3.

duomenų subjektai) asmens duomenys, dėl kurių gali būti pažeista įmonės reputacija ir patiriami finansiniai nuostoliai. Kai kuriais atvejais MVĮ gali neturėti finansinių išteklių atsigauti po duomenų pažeidimo, todėl verslas gali bankrutuoti. Pasak Swani K., Labrecque L. ir kt. (2024),„įmonių išlaidos dėl duomenų saugumo pažeidimų atsiranda ne tik dėl prevencinių veiksmų, tokių kaip aptikimas, pranešimas, būsimos kompensacijos, baudos ir reagavimo po pažeidimo priemonės, bet ir dėl būsimo verslo praradimo. Konkrečiai, būsimo verslo praradimas yra labai svarbus, nes duomenų pažeidimai gali sukelti verslo sutrikimus, pajamų praradimą ir pakenkti prekės ženklo reputacijai, o tai galiausiai gali lemti klientų praradimą“[47].

MVĮ dažnai susiduria su dideliais iššūkiais, kai kalbama apie duomenų saugumą. Pagrindiniai iššūkiai yra riboti finansiniai ištekliai saugumo priemonėms įsigyti bei specialistų trūkumas, be kita ko, pasak Uddin M. R. (2024), „nors įmonės imasi iniciatyvų kontroliuoti duomenų pažeidimo poveikį, tokias pastangas dažnai apsunkina kintantis grėsmių pobūdis“[48]. MVĮ įmonės dažnai įgyvendina tik pagrindines saugumo priemones, tokias kaip antivirusinė programinė įranga, ugniasienės ir slaptažodžių politika, tačiau pažangesnės priemonės lieka neįgyvendintos, neužtikrinamas įmonės saugos brandos lygis. Pasak Arranz A., Arroyabe D., (2023) „atsižvelgiant į tai, kokie veiksniai turi įtakos investicijoms į kibernetinio saugumo sistemas, tai rodo, kad organizacijos investuoja į kibernetinį saugumą remdamosi savo kibernetinio saugumo galimybėmis ir patyrusiomis kibernetinėmis atakomis“[49]. Be tinkamų darbuotojų mokymų, nuolatinės stebėsenos ir reagavimo į incidentus planų, mažoms įmonėms gali kilti didesnė asmens duomenų pažeidimų bei su tuo susijusių finansinių nuostolių rizika. Mokslininkai teigia, kad „organizacijos turėtų naudoti vieningą saugos platformą visoms saugos priemonėms ir atsižvelgti į vidines grėsmes kurdamos su kibernetiniu saugumu susijusias organizacines procedūras. Teisinėje literatūroje atkreipiamas dėmesys į du pagrindinius ateities rūpesčius: mažos ir vidutinio dydžio įmonės taps pagrindinėmis kibernetinių atakų aukomis, o žmogiškosios klaidos yra didžiausias kibernetinių atakų sėkmės veiksnys. Atsižvelgiant į tai, kad naudotojas yra silpniausia kibernetinio saugumo grandis, į žmogų orientuotų technologijų kūrėjai turėtų ne tik mokyti darbuotojus nuo kibernetinių incidentų, bet ir kurti į žmogų orientuotus dizainus“[50] (Poehlmann C. N., Caramancion K. M. ir kt. 2021).

[47] Swani K., Labrecque L., Markos E.. *Are B2B data breaches concerning? Consequences of buyer's or firm's data loss on buyer and supplier related outcomes.* 2024. P. 43-61.
[48] Uddin M. R.. *Developing a data breach protection capability framework in retailing*. 2024.
[49] Arranz A., Arroyabe D.. *Kibernetinio saugumo pajėgumai ir kibernetinės atakos kaip investicijų į kibernetinio saugumo sistemas varikliai: JK 2018 ir 2019 m.*. 2023.
[50] Poelhman N., Caramancion K. M. *The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review*. 2021.

Taip pat Poehlmann C. N., Caramancion K. M. ir kt. (2021) teigia, kad „kibernetinis saugumas yra ne tik gynybinis manevras, bet ir strateginis sprendimas, galintis padidinti organizacijos konkurencinį pranašumą prieš potencialius konkurentus. Todėl tai reikš, kad investicijos į kibernetinį saugumą yra organizacijos sprendimas, kuriame dalyvauja visi įmonės lygiai, o įmonės vyresnieji vadovai turi didelę reikšmę priimant sprendimą“.

Pasak Cheng L. ir kt. (2017) „iššūkis yra suprasti grėsmes, o dar svarbiau – įvairių prevencijos ir aptikimo sprendimų saugumo galimybes ir apribojimus, kad administratoriai galėtų priimti pagrįstus saugumo sprendimus ir praktikoje“[51]. Nacionalinis kibernetinio saugumo centras yra sukūręs kibernetinio saugumo informacinį tinklą (toliau – KSIT). Tai saugi, uždara įrankių, kibernetinio saugumo grėsmių stebėjimo ir informacijos apsikeitimo platforma, tačiau šis tinklas yra skirtas tik kibernetinio saugumo subjektams, todėl nėra atvira kitiems juridiniams asmenims. Susipažinus su viešojoje erdvėje pateikiamais KSIT privalumais kibernetinio saugumo subjektams, šie privalumai, būtų nepakeičiama pagalba ir mažoms bei vidutinio dydžio įmonėms, kurios neturi finansinių bei žmogiškųjų išteklių užtikrinti kibernetinį saugumą bei parinkti tinkamas prevencijos priemones ir metodus. Nacionalinio kibernetinio saugumo centro svetainėje pateikiama, kad „prie KSIT prisijungę naudotojai gali saugiai ir realiu laiku: dalintis su Nacionaliniu kibernetinio saugumo centru ir kitais KSIT nariais informacija apie kibernetinius incidentus, kenkėjiškus veiksmus; pranešti apie kibernetinius incidentus; automatizuoti kibernetinių incidentų aptikimą; nemokamai naudotis kai kuriais komerciniais produktais; suteikti savo organizacijos specialistams asmeninę prieigą prie reikiamų įrankių, nesijungiant prie visos KSIT platformos; bendrauti su kitais KSIT nariais ir kt.“[52].

1.5.2. Darbuotojų kibernetinio saugumo kultūros įtaka asmens duomenų nutekėjimui

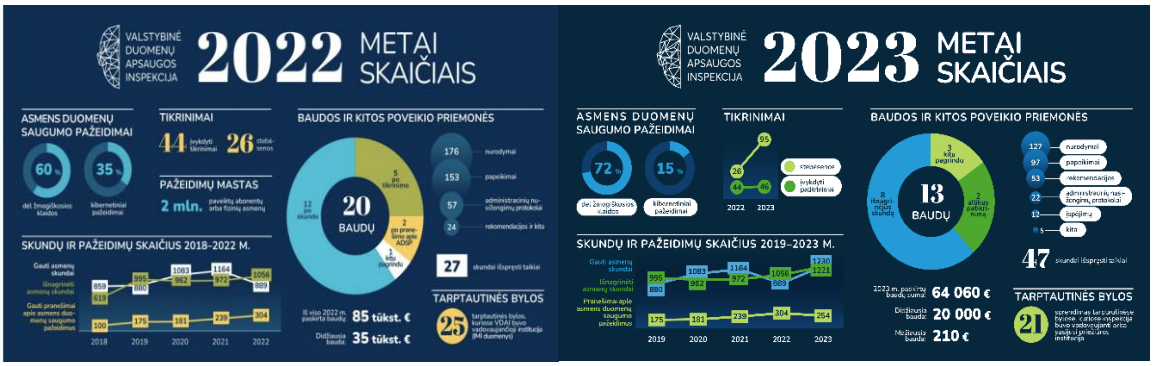
Ypatingą svarbą MVĮ įmonių saugumo formavime užima darbuotojai. Pasak Cheng L. ir kt. (2017) „siekiant išvengti netyčinio ar tyčinio duomenų nutekėjimo, be technologinių priemonių, labai svarbu didinti darbuotojų supratimą apie saugumą darbo vietoje“[53]. Netyčia darbuotojų nutekinta jautri informacija gali sukelti itin dideles neigiamas pasekmes bet kokio dydžio įmonei. Tokios klaidos gali būti kritinės ir sukelti didelę žalą tiek pačiai įmonei, tiek jos duomenų subjektams. Daugeliu atveju šie nelaimingi atsitikimai įvyksta dėl to, kad darbuotojams trūksta tinkamų mokymų ar įmonės politikos suvokimo. Net ir taikant pačias

[51] Cheng L., Liu F., Yao D. *Enterprise data breach: causes, challenges, prevention, and future directions*. 2017.
[52] Nacionalinis kibernetinio saugumo centras. *KSIT*.
[53] Cheng L., Liu F., Yao D. *Enterprise data breach: causes, challenges, prevention, and future directions*. 2017.

sudėtingiausias kibernetinio saugumo priemones, užtenka vieno neatsargaus darbuotojo, kad įvyktų konfidencialumo pažeidimas.

EBPO (2019) priėmė rezoliuciją dėl asmens duomenų saugumo pažeidimų prevencijos, daugiausia dėmesio skiriant saugumo priemonėms, kurių reikia imtis, kad būtų išvengta daugelio asmens duomenų saugumo pažeidimų – žmogiškųjų klaidų[54].

Valstybinės duomenų apsaugos inspekcijos duomenimis, per 2022 metus Lietuvoje net 60 proc., o 2023 metais net 72 proc. asmens duomenų saugumo pažeidimų įvyko dėl žmogiškosios klaidos, žr. 5 pav.:



Šaltinis. Valstybinė duomenų apsaugos inspekcija (2022-2023)

5 pav. Valstybinės duomenų apsaugos inspekcijos priežiūros veiklos rodikliai

Duomenų apsaugos procedūrų nesilaikymas yra viena dažniausių saugumo pažeidimų priežastis. Darbuotojai dažnai palieka nešiojamus kompiuterius ar mobiliuosius įrenginius be priežiūros viešose vietose, pamiršta užrakinti savo darbo vietą kai pasitraukia iš jos, naudoja darbui skirtą kompiuterį nesilaikant minimalios kibernetinės higienos reikalavimų ir kt.. Siekdamos išvengti tokių klaidų, įmonės turi darbuotojams pateikti aiškias gaires, kaip tvarkyti jautrius duomenis ir kokių veiksmų reikia imtis, kad užtikrintų jų apsaugą.

Asmeninių įrenginių naudojimas darbo tikslais yra dar viena iš atsitiktinių asmens duomenų pažeidimų priežastis. Kai darbuotojas naudoja savo asmeninį įrenginį, kad galėtų pasiekti su darbu susijusius dokumentus ar el. laiškus, jis tampa pažeidžiamas kibernetinių atakų. Taip nutinka todėl, kad įmonės neturi galimybių kontroliuoti darbuotojų asmeninius įrenginius, todėl jie yra mažiau saugūs nei įmonei priklausantys įrenginiai. Šiuose įrenginiuose dažnai trūksta būtinų saugos protokolų, kad būtų apsaugota jautri informacija.

Vienas iš pagrindinių reguliarių mokymų ir informavimo programų pranašumų yra tai, kad jos padeda darbuotojams neatsilikti nuo naujausių duomenų apsaugos praktikos ir

[54] International Conference of Data Protection & Privacy Commissioners (ICDPPC). *Resolution to address the role of human error in personal data breaches. 41st International Conference of Data Protection and Privacy Commissioners*. 2019.

reikalavimų. Tai gali apimti tokias temas kaip slaptažodžių valdymas, saugaus naršymo praktika ir duomenų šifravimas. Informuodamos darbuotojus apie naujausias tendencijas ir geriausią praktiką, kurdamos saugumo kultūrą, nustatydamos galimas rizikas ir pažeidžiamumą bei gerindamos darbuotojų moralę ir pasitenkinimą darbu organizacijos gali užtikrinti, kad jų duomenys išliktų saugūs bei apsaugoti nuo neteisėtos prieigos ar atskleidimo. Pasak Uddin M. R.. (2024), „organizacijos gebėjimas puoselėti informuotumo apie saugumą kultūrą gali geriau apsaugoti asmenis ir organizaciją nuo duomenų saugumo pažeidimo grėsmių“[55].

Siekiant sumažinti kibernetinių nusikaltimų skaičių bei užtikrinti asmens duomenų nutekėjimo prevenciją, būtina sumažinti žmogaus inicijuojamų saugumo pažeidimų skaičių, įpareigojant darbuotojus laikytis kibernetinės higienos. Pasak Neigel A. R. ir kt. (2020), „kibernetinė higiena yra adaptyvios žinios ir elgesys, siekiant sušvelninti rizikingą veiklą internete, dėl kurios kyla pavojus asmens socialinei, finansinei ir asmeninei informacijai - tai pavojus, kuris žymiai padidėja aptariant riziką ištisoms šalims, o ne vienam asmeniui“[56]. Nacionalinis kibernetinio saugumo centras 2024 metų pradžioje paskelbė apie galimybę stiprinti Lietuvos organizacijų ir jų darbuotojų kibernetinį atsparumą bei sukūrė naują nemokamą nuotolinę Kibernetinės higienos platformą. Pasak Nacionalinio kibernetinio saugumo centro - „Organizacijos, siekdamos užtikrinti savo kibernetinį saugumą, dažniausiai pagrindinį dėmesį skiria techninėms apsaugos priemonėms. Jos padeda, tačiau silpniausia kibernetinės gynybos dalis yra žmogus. Įvairių tyrimų duomenimis, net 80-90 proc. visų kibernetinių incidentų įvyksta dėl žmogiškosios klaidos, todėl darbuotojų švietimas ir mokymai privalo tapti kiekvienos organizacijos kasmetine rutinine veikla“[57]. Šiame informaciniame pranešime taip pat teigiama, kad „į mokymus savo darbuotojus gali registruotis visos ypatingos svarbos infrastruktūrą valdančios organizacijos, taip pat viešojo sektoriaus įstaigos“. Taigi, iki šiol Lietuvoje nėra platformos, leidžiančios ir mažo biudžeto įmonėms suteikti savo darbuotojams nemokamus mokymus. Tuo tarpu Uddin M. R.. (2024) pabrėžia platformų, valdymo bei darbuotojų pajėgumų svarbą, teikdamas, kad platformos būtinos tam, kad „įmonės galėtų sutelkti ir perkonfigūruoti „mikro“ pamatinių išteklių derinius bei sukurtų duomenų apsaugos nuo pažeidimų pajėgumus - dinamišką pajėgumą, palengvinantį reaktyvų ir aktyvų atsaką į duomenų pažeidimo grėsmes“[58].

[55] Uddin M. R.. *Developing a data breach protection capability framework in retailing*. 2024.
[56] Neigel A. R., Claypoole V.L., Waldfogle G. E., Acharya S., Hancock G. M. *Holistic cyber hygiene education: Accounting for the human factors*. (2020).
[57] Nacionalinis kibernetinio saugumo centras. *Nauja nemokama kibernetinių mokymų platforma*..
[58] Uddin M. R.. *Developing a data breach protection capability framework in retailing*. 2024

Apibendrinant galima teigti, kad MVĮ gali pagerinti kibernetinį saugumą suteikiant darbuotojams įrankius ir metodus tobulėti, tačiau, pasak Uddin M. R.. (2024), „per didelis spaudimas atitikties užtikrinimo veiklai gali išprovokuoti darbuotoją. Darbuotojams turi būti paprasta laikytis saugumo taisyklių“. Darbuotojų kibernetinio saugumo kultūros formavimas sumažina saugumo klaidų tikimybę atliekant kasdienines užduotis.

2. TVARKOMŲ ASMENS DUOMENŲ RIZIKOS VERTINIMAS BEI KITOS ASMENS DUOMENŲ NUTEKĖJIMO PREVENCIJOS PRIEMONĖS

Kibernetinio saugumo bei asmens duomenų apsaugos reikalavimų įgyvendinimu siekiama užkirsti kelią asmens duomenų nutekėjimui ir įdiegti tinkamas prevencijos priemones, padėsiančias apsisaugoti nuo galimų asmens duomenų nutekėjimo incidentų. Pasak Cheng L. ir kt. (2017) „duomenų nutekėjimo ir aptikimo sistemų tikslas yra nustatyti, stebėti ir užkirsti kelią netyčiniam ar neapgalvotam jautrios informacijos atskleidimui įmonės aplinkoje. Duomenų nutekėjimo ir aptikimo sistemos naudoja įvairius techninius metodus nutekėjimo priežastims pagrįsti“[59]. Zaleskio J. (2019) teigimu, duomenų saugumo principo laikymasis užtikrinamas įgyvendinant konkrečias duomenų saugumo priemones. Duomenų valdytojai ir tvarkytojai turėtų rinktis iš gausios duomenų saugumo priemonių sistemos. Autorius taip pat išskiria kelias duomenų saugumo priemonių rūšis. Pasak Zaleskio J. (2019), „pagal duomenų saugumo priemonių pobūdį, galima skirti technines ir organizacines duomenų saugumo priemones. Pagal teisinį sureguliavimą, galima skirti tas duomenų saugumo priemones, kurios yra nustatytos, ir tas, kurios nenustatytos teisės norminiu reguliavimu“.

„2023 m. I pusmetį asmens duomenų saugumo pažeidimų metu išryškėjo prieigos kontrolės valdymo organizacijų kompiuterių tinkluose spragos, kai suteikiant prieigą nėra taikomi apribojimai ir tinklo segmentavimas, nesilaikoma „mažiausių teisių privilegijos“ ir „būtina žinoti“ principų, netaikomas dviejų ir daugiau veiksnių autentifikavimas aukštesnes teises turintiems, nuotoliniu būdu besijungiantiems ir virtualų privatų tinklą naudojantiems vartotojams“ (Valstybinė duomenų apsaugos inspekcija. 2023).

Siekiant užtikrinti duomenų nutekėjimo prevenciją bei parinkti tvarkomų asmens duomenų apimtį atitinkančias saugumo priemones, MVĮ būtina atlikti rizikos vertinimą. „Elektroninių nusikaltimų prevencijos įgyvendinimas betarpiškai susijęs su rizikos analize“ (Štitilis, 2011, p. 88). Pažymėtina, kad Lietuvoje vis dar nėra vieningos sistemos kaip atlikti kibernetinio saugumo ir tvarkomų asmens duomenų apsaugos rizikos vertinimus. Stasytytė V.

[59] Cheng L. , Liu F., Yao D. *Enterprise data breach: causes, challenges, prevention, and future directions*. 2017.

ir Aleksienė L. (2015) teigia, kad „MVĮ dažnai neturi jokio rizikos valdymo mechanizmo, dažnai rizikos apskritai nėra valdomos, nėra vertinamas jų poveikis ir tikimybė“. Pasak autorių, procesų ir rizikos valdymo priemonės priklauso nuo įmonės dydžio ir brandos: „brandos lygis diktuoja, kokį rizikos valdymo metodą pradėti taikyti įmonės veikloje. Vienas iš galimų rizikos valdymo būdų, tinkamų MVĮ, yra rizikų portfelio sudarymas. Šis metodas leidžia kompleksiškai analizuoti ir vertinti įmonės patiriamas rizikas bei efektyviai numatyti atitinkamas atsako į rizikas priemones“[60]. „Kompleksinė apsauga verčia sukurti vieningą sistemą, kuri galėtų atremti visas galimas atakas, nukreiptas į kompiuterių sistemą – nuo durų išlaužimo ir aparatinės įrangos pavogimo iki informacinės vagystės iš kompiuterių sistemos“ (Štitilis, 2011, p. 101).

Įvertinę su asmens duomenų tvarkymu susijusias rizikas, MVĮ privalo užtikrinti tinkamo lygio duomenų apsaugą. „Duomenų valdytojai ir duomenų tvarkytojai turi neapsiriboti Bendrojo duomenų apsaugos reglamento tiesiogiai įvardintų duomenų saugumo priemonių įgyvendinimu. Turi būti įgyvendintos visos tinkamos techninės ir organizacinės priemonės, kurių, duomenų valdytojų ir tvarkytojų pagrįsta nuomone, reikėtų užtikrinti asmenims tinkamą saugumą (Bendrojo duomenų apsaugos reglamento 32 str. 1 d.)“[61].

2.1. Kibernetinio saugumo rizikos vertinimo aspektai

Dėl dažnų kibernetinių atakų, sukčiavimų, valstybės bei Bendrojo duomenų apsaugos reglamento reikalavimų, įmonės privalo užtikrinti asmens duomenų tvarkymo atskaitomybę. Asmens duomenų nutekėjimo prevencija gali būti užtikrinama tik kartu su kibernetinio saugumo priemonių įgyvendinimu. Dėl to įmonėse formuojasi tam tikra kibernetinio saugumo kultūra. Vienas iš pagrindinių kibernetinio saugumo kultūros elementų yra saugumo politika (saugos nuostatai). Tai oficialus taisyklių ir dokumentų rinkinys, kurį išleidžia įmonė, siekdama užtikrinti, kad jo darbuotojai bei duomenų tvarkytojai, kuriems suteikta prieiga prie technologijos ir informacijos išteklių, laikytųsi taisyklių ir gairių, susijusių su informacijos saugumu. Kibernetinio saugumo politikos pagalba, įmonės apibrėžia vieningus ir veiksmingus kibernetinio saugumo valdymo principus, vadovybės poziciją, kibernetinio saugumo atžvilgiu bei užtikrina efektyvų valdymo proceso įgyvendinimą. Siekiant tinkamo politikos įgyvendinimo, įmonės politiką turi reguliariai peržiūrėti, dokumentuoti. Ši politika nusako, kokios sistemos turėtų būti įdiegtos kritinių, svarbiausių duomenų apsaugai. Be to, saugumo

[60] Stasitytė S. Aleksienė L. *Įmonės veiklos rizikos vertinimas ir valdymas mažose ir vidutinėse įmonėse*. (2015).
[61] Julius Zaleskis. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė.* 2019. Monografja. P.133.

dokumentai informacinių technologijų personalui bei administracijos darbuotojams nurodo, kaip jie turi saugoti įmonės duomenis ir kas yra atsakingas už jų apsaugą.

Valstybės informacinės sistemos valdytojai privalo, o privataus sektoriaus įmonės turi teisę vadovautis gerąja praktika ir savarankiškai įsidiegti pagal Lietuvos Respublikos Vyriausybės nutarimu „Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir saugos dokumentų turinio gairių aprašo parvirtinimo“ Saugos dokumentų turinio gaires parengtus saugos dokumentus:

- „Informacinės sistemos duomenų saugos nuostatus;
- Saugaus elektroninės informacijos valdymo taisykles;
- Informacinės sistemos veiklos tęstinumo valdymo planą;
- Informacinės sistemos naudotojų administravimo taisykles“.

Kibernetinio saugumo dokumentai rengiami remiantis standartais ir Lietuvos Respublikos Vyriausybės dokumentais: „Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu“, taip pat siekiant užtikrinti kibernetinį saugumą, įmonės turėtų vadovautis 1 lentelėje pateikiamu standartu bei „gerosios praktikos“ rekomendacijos ir metodikomis:

1 lentelė. Kibernetinio saugumo standartas, „gerosios praktikos“ rekomendacijos ir metodikos.

Kibernetinio saugumo standartas	
Bendrasis duomenų apsaugos reglamentas (angl. General Data Protection Regulation, GDPR)	Tai yra Europos Sąjungos standartas, kuris apibrėžia visų vartotojų duomenų apsaugą. Pagal šį standartą įmonė turi įsitikinti, kad duomenų subjektų duomenys yra saugūs ir negali būti prieinami be tinkamo leidimo. Šis standartas daugiausiai dėmesio skiria vartotojų duomenų saugai, kai jie dalinasi jais su bet kuria iš organizacijų, kurios laikosi šio reglamento.
„Gerosios praktikos“ rekomendacijos ir metodikos	
ITIL (angl. Information Technology Infrastructure Library)	Pagrindinis ITIL standarto ir metodikos tikslas – IT paslaugų valdymo įgyvendinimas. Tai geriausių pavydžių, naudojamų siekiant šio tikslo, rinkinys. ITIL gali padėti įmonei pasiekti informacijos apsaugos politikoje numatytų tikslų ir gali būti naudojamas kartu su ISO 27001/27002 standartais.

1 lentelės tęsinys kitame puslapyje

1 lentelės tęsinys

COBIT (angl. Control Objectives for Information and related Technology)	Tai audito kompanijų organizacijos ISACA parengta metodika, kartu ir gerosios praktikos rinkinys, kuri turi padėti vartotojams, įmonėms ir auditoriams planuoti, įgyvendinti ir audituoti IT valdymo priemones
ISF (angl. The Information Security Forum Standard of Good Practice)	ISF – tai Informacijos saugumo forumo, kurį sudaro daugiau nei 200 didžiausių pasaulio kompanijų parengtas informacijos apsaugos priemonių rinkinys. Jo pripažinimas ir populiarumas yra mažesnis negu ISO 17799 standarto, tačiau šis rinkinys yra platinamas nemokamai. Minėtas rinkinys yra skirtas padėti organizacijoms, nepriklausomiems rinkos sektoriams vertinti pavojus, susijusius su informacinėmis sistemomis. Tai yra efektyvus įrankis, padedantis gerinti saugumo kontrolės efektyvumą ir patogesnį pritaikymą organizacijai.
CRAMM (angl. CCTA Risk Analysis and Management Methodology)	Tai D. Britanijos Vyriausybės užsakymu sukurta ir visame pasaulyje taikoma informacijos apsaugos rizikų analizės ir valdymo metodika. CRAMM metodika yra nuolat tobulinama jau beveik 20 metų ir yra nepakeičiama priemonė saugumo vadovams ir analitikams. CRAMM – tai laipsniškas ir metodiškas būdas analizuoti ir valdyti tiek techninius (pavyzdžiui, IT techninę ir programinę įrangą), tiek netechninius (pavyzdžiui, fizinius ir žmogiškuosius) informacijos apsaugos aspektu.
CSA CCM	Debesų saugos aljanso (CSA) Debesų rodiklių matrica CCM yra rodiklių rinkinys, skirtas įvertinti informacijos saugumą debesų technologijose. Jame – 133 rodikliai, padalinti į 16 sričių, aprėpiančių visus pagrindinius debesų technologijų aspektus. Matrica duoda organizacijoms gaires, kurios padėtų joms maksimaliai padidinti informacijos saugumą, nepasikliaujant vien debesų teikėjo garantijomis.

Šaltinis: sudaryta autoriaus

Svarbu suprati, kad tinkamas kibernetinio saugumo rizikos valdymas bei tikslingai parinktas ir įdiegtas kibernetinio saugumo standartas ar metodika „ne tik sumažina kibernetinės

grėsmės riziką, bet ir suteikia pripažinimą kaip kibernetinę brandą pasiekusią įmonę“[62] (S. (Pawar ir Palivela H.. 2023) Pažymėtina, kad Alahmaris A., Duncanas B. (2020) nustatė „penkias pagrindines perspektyvas, kurios vaidina pagrindinį vaidmenį MVĮ kibernetinio saugumo rizikos valdyme – atitinkamai grėsmės, elgsena, praktika, informuotumas ir sprendimų priėmimas“[63]. Kadangi „IT infrastruktūra tapo labai svarbiu visos MVĮ veiklos turtu, didėjantis kibernetinis pavojus MVĮ padidino valdybų sąmoningumą apie būtinybę ir svarbą kovoti su rizika, susijusia su bendra verslo priklausomybe nuo informacinių sistemų“[64] (Maximiano A., Pinto G. 2021), 1 lentelėje nurodytos „gerosios praktikos“ rekomendacijos ir metodikos per įmonių vadovų bei valdybų prioritetų kibernetiniam saugumui paskirstymą, kibernetinės kultūros įmonėje modeliavimą, grėsmių atitinkamą įvertinimą gali būti integruotos į įmonių kasdienę veiklą, teigiamai veiktų bendrą įmonių kultūrą, didindamos sąmoningumą apie asmens duomenų svarbą. Pažymėtina, kad mokslininkai įžvelgia problemų, susijusių su standartų taikymu MVĮ, teigiama, kad „standartų yra nedaug ir jie dažniausiai orientuoti į dideles įmones, kurių verslo procesas tam tikru mastu yra gerai struktūrizuotas. Turimi standartai yra pernelyg bendri arba pernelyg specifiniai kai kurioms konkrečioms verslo sritims“ (Maximiano A., Pinto G. (2021), todėl MVĮ tenka ieškoti kitų metodų ir būdų, užtikrinančių aukštą kibernetinės brandos lygį. Rinkoje yra teikiama pakankamai rekomendacijų bei standartų, tačiau MVĮ yra sudėtinga spręsti kibernetinio saugumo klausimus, „nėra specialaus apsaugos personalo, yra daug standartų ir gairių, tačiau sunku susidaryti vaizdą apie tai, kas aktualu konkrečiam kontekstui (įmonės dydis, įdiegtų technologijų rinkinys, rinkos situacija, rinkos profilis), o dar sunkiau objektyviai įvertinti ir pasirinkti konkretų sprendimą ar gaires“[65] (Kern M.. 2023). Pasak Štitilio (2013) vienas iš būdų pasiekti kibernetinį atsparumą – bendradarbiauti tarpusavyje[66]. Viešojo ir privataus sektoriaus bendradarbiavimas bei skirtingų veiklų įmonių dalinimasis informacija, galėtų padėti užtikrinti kibernetinį saugumą.

Duomenų pažeidimai, susiję su reikšmingais asmeninės informacijos praradimais ir finansiniu poveikiu, tampa vis dažnesni. Pažymėtina, kad Valstybinės duomenų apsaugos inspekcijos veikla yra tiesiogiai susijusi su kibernetiniu saugumu, kai tiriami kibernetiniai

[62] Pawar ir Palivela H.. LCCI: *A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)*. (2023). P. 3.
[63] Alahmaris A., Duncanas B. *Kibernetinio saugumo rizikos valdymas mažose ir vidutinėse įmonėse: sisteminga naujausių įrodymų apžvalga*. (2020).
[64] Maximiano A., Pinto G *Informacijos saugumas ir kibernetinio saugumo valdymas: atvejo tyrimas su MVĮ Portugalijoje*. 2021.
[65] Kern M., Landauer M., Weippl E. A logging maturity and decision model for the selection of intrusion detection cyber security solutions. 2024.
[66] Štitilis D. *Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos.* 2013. P.193.

incidentai, susiję su asmens duomenų ir privatumo apsaugos pažeidimais. 2020 m. 24,6 % Valstybinės duomenų apsaugos inspekcijos vertintų asmens duomenų saugumo pažeidimų buvo taip pat ir kibernetiniai incidentai.[67] Bendrojo duomenų apsaugos reglamento baudų sekimo svetainės (angl. *CMS. Law GDPR Enforcement Tracker*) (toliau – CMS) duomenimis, per 2023 metus 26 šalių priežiūros institucijos skyrė 372 baudas įvairioms įmonėms, o tai 139 baudomis daugiau palyginti su 2022 metais. Šiuo metu bendra baudų suma siekia 857 mln. eurų[68]. Dauguma privataus sektoriaus įmonių buvo nubaustos dėl nepakankamos duomenų tvarkymo teisinės bazės, nepakankamo informavimo įsipareigojimo vykdymo ir nepakankamų techninių bei organizacinių priemonių.

Pažymėtina, kad kibernetiniai incidentai daro neigiamą poveikį ne tik duomenų subjektams, kurių duomenys nutekėjo, bet ir pačioms įmonėms. Pasak Zhou F., Huang J. (2024), „literatūroje tarp duomenų pažeidimų poveikio pateikiami didesni audito mokesčiai (Li, No, &; Boritz, 2020; Smith et al., 2019), mažėjančios inovacijos (He, Frost, &; Pinsker, 2020) ir neigiamo įvykio suvokimas paveiktoms įmonėms (Xu ir kt., 2019), kurių atskleidimas sukelia neigiamas rinkos reakcijas (Gwebu ir kt., 2018). Pajamas didinančių pajamų valdymas, kurį dažnai vykdo pažeistos įmonės, siekdamos sušvelninti neigiamas rinkos reakcijas, paprastai lemia blogesnius vėlesnius rezultatus (Xu et al., 2019)“[69].

Vadovaujantis Valstybinės duomenų apsaugos inspekcijos nuomone, labai „svarbi priemonė siekiant išvengti kibernetinių incidentų (duomenų viliojimo atakų ir kt.) yra darbuotojų mokymai. Mokymai apie duomenų apsaugą ir saugumo procedūras (pvz. slaptažodžių naudojimą ir prieigą prie konkrečių IT sistemų) yra svarbūs tinkamam organizacinių ir techninių saugumo priemonių įgyvendinimui ir prevencijai dėl netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų. Žinios apie asmens duomenų tvarkymui keliamus reikalavimus bei atsakomybes yra ypač svarbios tiems asmenims, kurie atlieka didelės rizikos asmens duomenų tvarkymo operacijas“[70]. Siekiant sėkmingo kibernetinio saugumo, ypatingą dėmesį atlieka bet kurios organizacijos, tame tarpe MVĮ darbuotojai. Todėl neužtenka turėti saugumo politikos bei įdiegti technines saugumo priemones, nes darbuotojo elgesys bei veiksmai užtikrinant kibernetinį saugumą yra svarbesni. Tą pažymi ir Pawar ir Palivela H. (2023), teigiant, kad

[67] Valstybinė duomenų apsaugos inspekcija. *2020 metų asmens duomenų apsaugos priežiūros Lietuvoje apžvalga*.
[68] CMS. *Law, tax, future*.
[69] Zhou F., Huang J.. Cybersecurity data breaches and internal control. 2024.
[70] Valstybinė duomenų apsaugos inspekcija. *Asmens duomenų apsaugos pažeidimai Lietuvoje 2023 m. I pusmetį.*

„kibernetinio saugumo suvokimas padeda bet kokiam skaičiui auditorijų ir tai yra veiksmingiausias būdas užkirsti kelią kibernetinėms grėsmėms“[71].

Įvykus asmens duomenų apsaugos pažeidimui, visais atvejais įmonėms tenka patirti materialinę arba reputacijos žalą, tenka atlyginti nuostolius bei komunikuoti su partneriais ar duomenų subjektais, kurių asmens duomenys tapo pažeisti. Tačiau dažnai MVĮ trūksta informacijos, kad būtų galima priimti veiksmingus sprendimus, o tradicinės „perimetro apsaugos“ strategijos nėra pakankamos. Daugumai įmonių taip pat sunku įvertinti rizikos ir rizikos valdymo priemonių poveikį. Pasak Štitilio (2011), „didelė žala atsiranda dėl netinkamo atsako į pažeidimą, o ne dėl paties pažeidimo“[72]. Štitilis (2011) išskiria šiuos kibernetinių saugumo rizikų tipus, žiūrėti į 2 lentelę:

2 lentelė. Kibernetinių saugumo rizikų tipai

Kibernetinė rizika			
Vidinė		Išorinė	
Kenkėjiška	Netyčinė	Kenkėjiška	Netyčinė

Šaltinis: sudaryta autoriaus pagal Štitilį (2011)

Pasak Štitilio (2011) „kibernetinė rizika – tai galimybė patirti bet kokį veiklos sutrikdymą, finansinę žalą ar žalą reputacijai, kylančią iš organizacijos nesugebėjimo apsaugoti savo turimą informaciją, užtikrinti veiklos tęstinumą. Kibernetinės rizikos tipai:

- Vidinė ir kenkėjiška rizika – paprastai tai yra sąmoningas sabotažo ar vagystės veiksmas įmonės viduje. Tai gali būti nepatenkintas darbuotojas, ištrynęs ar pavogęs duomenis iš centrinės sistemos, arba sąmoningas virusų diegimas įmonės kompiuteriuose;
- Vidinė ir netyčinė rizika – atsiranda dėl žmogiškosios klaidos. Net labiausiai sąmoningas darbuotojas gali padaryti klaidų;
- Išorinė ir kenkėjiška – organizacijai nepriklausančio asmens/asmenų tyčinis išpuolis. Tai gali būti įsilaužimas į įmonės vidines sistemas, duomenų bazes nusikalstamais tikslais;
- Išorinė ir netyčinė – atsitiktinis neigiamas poveikis įmonės sistemai. Tai galėtų būti programinės įrangos klaida ar stichinė nelaimė“.

Siekiant valdyti rizikas, būtina atlikti rizikos analizę. Saugumo procesas turi būti nukreiptas į kritinę reikšmę turinčius veiksnius, kurių nepaisant iškyla didelė nesėkmės tikimybė. Rizikos valdymo proceso tikslas – sumažinti riziką iki priimtino lygio. Kibernetinės

[71] Pawar ir Palivela H.. *LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs).* 2023. P. 3

[72] Štitilis, D. (2011). *Elektroniniai nusikaltimai. Metodinė priemonė*. Vilnius: Mykolo Romerio universitetas

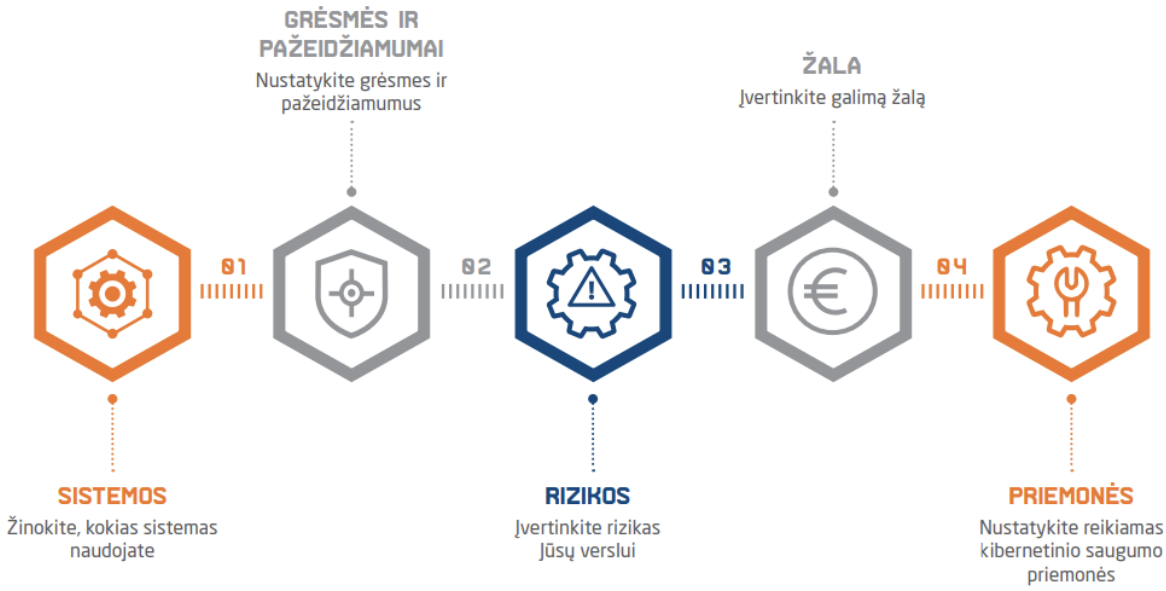
rizikos vertinimas apima kibernetinės rizikos identifikavimą, analizę ir pasekmių įvertinimą. „Į rizikos analizę taip pat įeina ir įvertinimas, kaip gerai organizacija pasiruošusi blogiausiam variantui, kartais vadinamas atsitiktinumų planavimu arba krizės vadovavimu“ (Štitilis, 2011, p. 89). Rizikos analizės rezultatai skirti siekiant rizikos mažinimo procesams įgyvendinti ir jų veiksmingumui įvertinti, pavyzdžiui, atsisakant neveiksnių priemonių, diegiant naujas ir suderinant su esamomis rizikos valdymo priemonėmis. Ypatingas dėmesys turi būti skiriamas iš vadovybės, nes be vadovybės palaikymo, saugos rizikos valdymas nebus veiksmingas, o rizikos analizei esminę reikšmę turi aiškus vaidmenų ir atsakomybės apibrėžimas.

Nacionalinio kibernetinio saugumo centras leidinyje „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas vadovas?“ nurodo, kad „rizika gali būti apibrėžiama kaip bet kokia aplinkybė ar įvykis, galintis turėti neigiamą poveikį ryšių ir informacinių sistemų saugumui“. Teigiama, kad rizikų pašalinimas nėra įmanomas, jos gali būti sumažinamos, pasitelkiant tinkamas prevencijos priemones (technines arba organizacines). Akcentuojamas balansas tarp rizikų bei kontrolės mechanizmų, teigiant, kad rizikos mažinimo priemonės neturėtų kainuoti daugiau nei galimi saugumo pažeidimo padariniai. Vadinasi, kiekviena MVĮ turi nuspręsti kokias organizacines bei technines priemones taikyti ir kokią saugumo keliamą riziką toleruoti. „Rizikos analizė yra procesas, kurio metu atsakoma į klausimus: pirma, apie grėsmes, antra, apie pažeidžiamumą, ir, galiausiai, apie kontrapriemones, kurias panaudojus galima užkirsti kelią pavojui.

- Grėsmė – tai galimas pavojus kompiuterių sistemai. Pavojus gali būti žmogus (vagis, profesionalus nusikaltėlis, hakeris), įvykis (gaisras, žaibas) ir kt. kas gali pakenkti kompiuterių sistemai;
- Pažeidžiamumas – vieta, kur kompiuterių sistema yra jautri pažeidimui. Grėsmė pasireiškia konkrečioje veikoje, kuri išnaudoja sistemos pažeidžiamumą;
- Kontrapriemonės – priemonės kompiuterių sistemų apsaugojimui: slaptažodžiai, durų užraktai“[73] (Štililis, 2011).

Įvertinus rizikas, parenkamos atitinkamos kibernetinio saugumo priemonės, kurios padeda būti pasiruošusiems galimoms grėsmėms. Rizikos vertinimo bei prevencijos užtikrinimo procesas pateikiamas pav. Nr. 6:

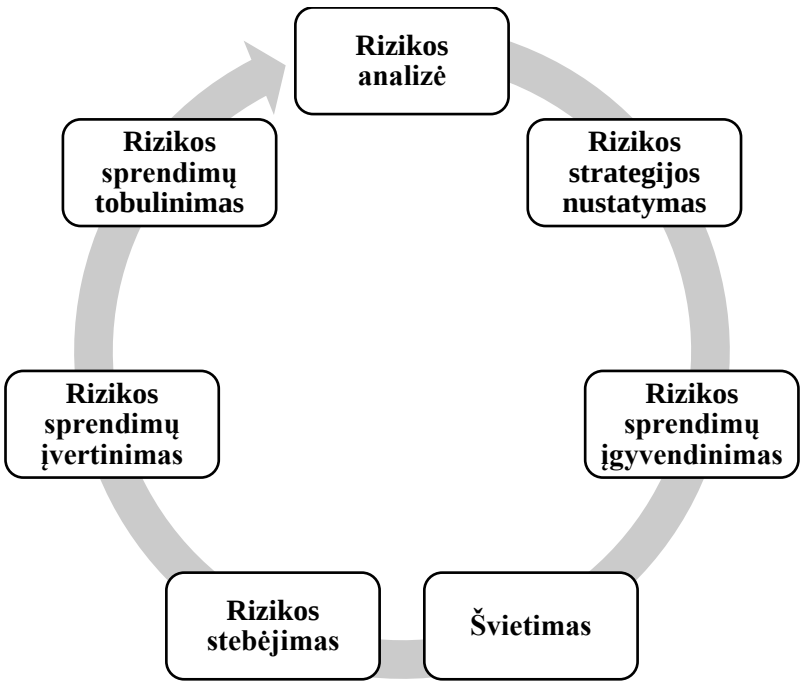
[73] Štitilis, D. (2011). *Elektroniniai nusikaltimai. Metodinė priemonė. Vilnius: Mykolo Romerio universitetas*. P. 89.



Šaltinis: Nacionalinio kibernetinio saugumo centras. Vadovas verslui

6 pav. Rizikos vertinimo bei prevencijos užtikrinimo procesas

Rizikos valdymas – tai potencialios rizikos nustatymo, šios rizikos poveikio ir planavimo, kaip reaguoti, jei rizika taptų realybe, nenutrūkstamas procesas (žr. 5 pav.). Kiekvienai įmonei, nepriklausomai nuo dydžio ar veiklos, svarbu parengti kibernetinio saugumo rizikos planą.



Šaltinis: sudaryta autoriaus

7 pav. Rizikos valdymo procesas

Privataus sektoriaus įmonės turi teisę pasinaudoti gerąją praktika ir atlikti informacinių sistemų rizikos analizę bei grėsmių ir pažeidžiamumų vertinimą pagal Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“ bei Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus (LST ISO/IEC 27001:2013). Vadovaujantis šia gerąja praktika, informacinių sistemų rizikos analizės ir vertinimo metu turi būti atlikta:

- „Vertinamos sistemos visų posistemių kritiškumo nustatymas;
- Grėsmių ir jų tikimybės nustatymas;
- Esamų pažeidžiamumų ir kontrolės priemonių, mažinančių grėsmių rizikas, nustatymas;
- Rizikos lygio nustatymas;
- Priimtos rizikos nustatymas;
- Nepriimtos rizikos valdymo būdo parinkimas;
- Likutinės rizikos paskaičiavimas;
- Ataskaitos parengimas ir pateikimas“[74].

Toliau nustačius galimas grėsmes ir pažeidžiamumus, galinčius turėti įtakos kibernetiniam saugumui, turi būti atliekamas vertinimas. Informacinių sistemų technologinio pažeidžiamumo, galinčio turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, įvertinime ir galimų grėsmių bei pažeidžiamumų poveikio duomenų veiklai sričių nustatymo metu turi būti atlikta:

- „Vidinio tinklo (LAN) infrastruktūros saugos patikrinimas;
- Tarnybinių stočių saugumo patikrinimas;
- Kompiuterizuotų darbo vietų saugumo patikrinimas;
- Slaptažodžių auditas;
- Duomenų bazių valdymo sistemų patikrinimas;
- Tinklo įrangos auditas;
- Bevielio tinklo įrangos auditas;
- Interneto svetainių patikrinimas;
- Ataskaitos kartu su trūkumų šalinimo planu parengimas ir pateikimas“.

Apibendrinant galima teigti, kad „atsižvelgiant į didėjantį dėmesį informacijos saugumo valdymo teorijai šiuolaikinėje informacinių sistemų literatūroje (Ou et al., 2022) ir rizika pagrįstų metodų populiarumą šioje srityje (Barati, 2022), duomenų pažeidimo atsiradimo

[74] Lietuvos Respublikos Vidaus reikalų ministerija. *Rizikos analizės vadovas*. 2005.

tikimybės supratimas ir kiekybinis įvertinimas, kuris yra pagrindinis indėlis į rizikos vertinimo sistemas, galėtų būti vertingas indėlis tiek į teoriją, tiek į praktiką“[75] (Barati M. 2022).

2.2. Asmens duomenų tvarkymo rizikos vertinimo aspektai

Bendrasis duomenų apsaugos reglamentas nėra techninis informacinių technologijų duomenų saugumo reguliavimo dokumentas. „Pagrindiniuose teisės aktuose nėra nustatytų konkrečių techninių standartų, atskleidžiančių kas konkrečiai laikoma tinkamu techniniu duomenų saugumu. Galimi aktualūs ir konkretūs duomenų saugumo standartai pateikiami „soft law“ kompetentingų institucijų, pvz. ES tinklų ir informacijos saugumo agentūros, priimtuose šaltiniuose“ (Zaleskis J. 2019). Vadovaujantis Bendrojo duomenų apsaugos reglamento 24 bei 32 straipsniais, MVĮ privalo atsižvelgti į „duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus ir riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms“[76] atlikti tvarkomų asmens duomenų rizikos vertinimą. Atlikus rizikos vertinimą, MVĮ kuria (diegia) bei vertina turimas organizacines ir technines saugumo priemones atsižvelgiant į rizikos vertinimo rezultatus.

Valstybinė duomenų apsaugos inspekcija parengė tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gaires[77], kurios skirtos „padėti duomenų valdytojams ir duomenų tvarkytojams, kurie priskiriami prie smulkiojo ir vidutinio verslo subjektų įvertinti aktualius pavojus asmens duomenų saugumui ir įgyvendinti tinkamas saugumo priemones“. Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams (toliau – gairės) parengtos remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA. 2018) ir ISO standartais LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ bei ISO/IEC 27701:2019 „Saugumo metodai – ISO/IEC 27001 ir ISO/IEC 27002 papildymas dėl privatumo valdymo – Reikalavimai ir gairės“. Valstybinė duomenų apsaugos inspekcija prie organizacinių bei techninių asmens duomenų saugumo priemonių gairėse išvardintų priemonių, taip pat pateikia nuorodą į susijusį informacijos saugumo valdymo standarto LST ISO/IEC 27001:2017 reikalavimą ir jį papildantį privatumo užtikrinimo reikalavimą pagal ISO/IEC 27701:20192.

[75] Barati M., Yankson B., *Predicting the Occurrence of a Data Breach*. 2022.
[76] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB. 24-32 str.
[77] Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*. 2020-06-18. 3 versija.

Paaiškinimai pateikti atsižvelgiant į Bendrąjį duomenų apsaugos reglamentą. Pažymėtina, kad Bendrajam duomenų apsaugos reglamentui būdingos abstrakčios nuostatos, todėl papildomi *soft low* šaltiniai, tokie kaip gairės, rekomendacijos ir geriausios praktikos pavyzdžiai, nors ir neturėdami formaliai privalomos teisinės galios, padeda suteikti daugiau teisinio apibrėžtumo. Pasak Zaleskio J. (2019), „duomenų saugumo srities teisės nuostatos grindžiamos principais, bet ne detaliomis taisyklėmis. Galima skirti šiuos duomenų saugumo teisinio reguliavimo principus: duomenų valdytojų ir tvarkytojų diskrecijos principą, pavojų asmenims grįsto požiūrio (angl. risk *based approach*) principą, duomenų konfidencialumo, vientisumo, prieinamumo ir atsparumo principą, duomenų saugumo priežiūros principą“.

Valstybinė duomenų apsaugos inspekcija gairėse pateikia keturis būtinuosius žingsnius, kuriuos MVĮ, siekdamos įdiegti prevencines asmens duomenų saugumo priemones privalo atlikti, (žr. 8 pav.):

Šaltinis: sudaryta autoriaus pagal Valstybinės duomenų apsaugos inspekcijos gaires (2020)

8 pav. Rizikos vertinimo procesas

Valstybinės duomenų apsaugos inspekcijos pateikiamos rizikos vertinimo proceso dalys (žingsniai) aprašomi 3 lentelėje[78]:

[78] Valstybinė duomenų apsaugos inspekcija. Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams. 2020-06-18. 3 versija.

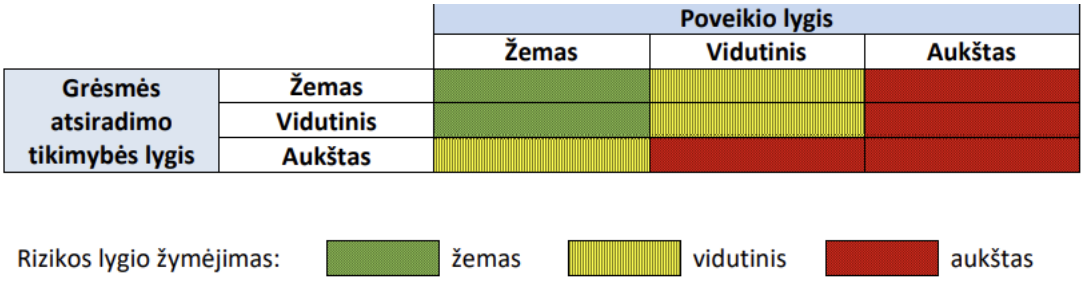
3 lentelė. Rizikos vertinimo proceso dalys

Žingsnis	Proceso dalies pavadinimas	Proceso dalies aprašymas
I	Duomenų tvarkymo operacijų ir jų konteksto nustatymas	„MVĮ privalo nustatyti vertinamų asmens duomenų apimtį ir kontekstą. Vadovaudamasi duomenų tvarkymo etapais (rinkimo, saugojimo, naudojimo, perdavimo, sunaikinimo ir kt.), MVĮ turi atsakyti į klausimus: • Kokios yra įmonės asmens duomenų tvarkymo operacijos? • Kokios kategorijos asmens duomenys yra tvarkomi? • Koks tvarkymo tikslas? • Kokios priemonės naudojamos tvarkyti asmens duomenis? • Kur vykdomas asmens duomenų tvarkymas? • Kokios yra duomenų subjektų kategorijos? • Kas yra duomenų gavėjai?
II	Tvarkomų asmens duomenų poveikio vertinimas	Remiantis pirmo žingsnio analize, MVĮ turi įvertinti fizinių asmenų pagrindinėms teisėms ir laisvėms kylantį pavojų dėl galimo asmens duomenų saugumo pažeidimo. Nagrinėjami trys poveikio lygiai: • **Žemas:** fizinis asmuo gali susidurti su tam tikrais nepatogumais (pvz. sugaištas laikas iš naujo suvedant informaciją, susierzinimas, nepasitenkinimas ir pan.); • **Vidutinis:** fizinis asmuo gali patirti didelių nepatogumų, kuriuos jis galės įveikti nepaisant tam tikrų sunkumų (pvz. papildomos išlaidos, prieigos prie reikalingų išteklių praradimas, stresas, nedideli fiziniai negalavimai ir kt.); • **Aukštas:** fizinis asmuo gali patirti reikšmingas pasekmes ir norint jas ištaisyti, pašalinti reikės susidurti su rimtais sunkumais (pvz. lėšų praradimas, asmens įtraukimas į finansinių institucijų juodąjį sąrašą, turto nuostoliai (žala), darbo vietos praradimas, teisminiai procesai, sveikatos būklės pablogėjimas ir pan.) arba dideles ir negrįžtamas pasekmes, kurių negalės ištaisyti, pašalinti (pvz.

3 lentelės tęsinys kitame puslapyje

		negalėjimas dirbti, ilgalaikiai psichiniai ir fiziniai negalavimai, mirtis ir pan.). Poveikio vertinimas yra kokybinis procesas.
III	Galimų grėsmių nustatymas ir jų atsiradimo tikimybės įvertinimas	Šiame etape MVĮ reikia nustatyti grėsmes, susijusias su visa asmens duomenų tvarkymo aplinka (išorės arba vidaus), ir įvertinti jų atsiradimo tikimybę. Siekiant šį procesą supaprastinti yra pateikiami klausimai, skirti įvertinti MVĮ asmens duomenų tvarkymo aplinką (ji yra tiesiogiai susijusi su grėsmėmis) ir galimas grėsmes. Šie klausimai yra susiję su keturiais pagrindiniais šios aplinkos aspektais (vertinimo sritimis), tai yra: • Tinklo ir techniniai ištekliai; • Procesai ir procedūros, susiję su asmens duomenų tvarkymu; • Duomenų tvarkymo dalyviai; • Veiklos sritys ir duomenų tvarkymo mastai. Kiekvienai vertinamai sričiai gali būti nustatytas grėsmės atsiradimo tikimybės lygis: • **Žemas:** mažai tikėtina, kad grėsmė pasitvirtins; • **Vidutinis:** yra reali galimybė, kad grėsmė pasitvirtins; • **Aukštas:** tikėtina, kad grėsmė pasitvirtins.
IV	Rizikos įvertinimas	Įvertinus asmens duomenų tvarkymo operacijos poveikį ir atitinkamos grėsmės atsiradimo tikimybę, pasinaudojant 9 pav. nurodyta matrica, galima atlikti galutinį rizikos įvertinimą“.

Šaltinis: sudaryta autoriaus pagal Valstybinės duomenų apsaugos inspekcijos gaires (2020).



Šaltinis: sudaryta autoriaus pagal Valstybinės duomenų apsaugos inspekcijos gaires (2020).

9 pav. Rizikos vertinimo matrica

Įgyvendinusi Valstybinės duomenų apsaugos inspekcijos rizikos vertinimo proceso reikalavimus ir nustačiusi tvarkomų asmens duomenų riziką fizinių asmenų teisėms ir laisvėms, MVĮ privalo parinkti atitinkamas „saugumo priemones asmens duomenų saugumui užtikrinti. Duomenų saugumo priemonės skirstomos į dvi plačias kategorijas (organizacines ir technines), kurios toliau skirstomos pagal konkrečias priemonių rūšis ir žymimos spalvomis (žemas – žalia, vidutinis – geltona, aukštas – raudona)“ (Valstybinė duomenų apsaugos inspekcija. 2020). Valstybinė duomenų apsaugos inspekcija pažymi, kad priemonių taikymas konkretiems rizikos lygiams neturėtų būti suprantamas kaip absoliutus, todėl MVĮ turi diskrecijos teisę parinkti ir įgyvendinti papildomas priemones[79].

Organizacijos, užtikrindamos asmens duomenų apsaugą, vadovaujasi šiais modeliais:

- „Reguliavimas bendraisiais įstatymais;
- Sektorinis reguliavimas;
- Savireguliacija;
- Apsauga techninėmis priemonėmis“ [80](Kiškis M ir kt.., 2006).

Siekiant sėkmingos savireguliacijos, net ir nesant teisės aktuose nustatytų pagrindų MVĮ tikslinga savanoriškai skirti duomenų apsaugos pareigūną (toliau – DAP). Įmonės turi teisę DAP funkcijų vykdymui skirti vidinį darbuotoją arba sudaryti išorės paslaugų sutartį. Itin svarbus DAP vaidmuo konsultuojant MVĮ dėl apsaugos priemonių (įskaitant technines ir organizacines) siekiant sumažinti riziką duomenų subjektų teisėms ir laisvėms (29 straipsnio darbo grupė)[81]. Valstybinė duomenų apsaugos inspekcija DAP tikrinimų apibendrinime nurodo, kad „DAP privalo stebėti, kaip laikomasi BDAR, kitų Sąjungos arba nacionalinės duomenų apsaugos nuostatų ir duomenų valdytojo arba duomenų tvarkytojo politikos asmens duomenų apsaugos srityje bei atlieka susijusius auditus (39 straipsnio 1 dalies b punktas). BDAR 39 straipsnio 2 dalyje reglamentuota, kad DAP, vykdydamas savo užduotis, tinkamai įvertina su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus. DAP gairėse yra paaiškinta, kad duomenų apsaugos pareigūnas privalo savo veiklą suskirstyti prioritetais ir daugiausia dėmesio skirti tiems klausimams, kurie kelia didžiausią pavojų duomenų apsaugai“[82].

[79] Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*. 2020-06-18 3 versija;
[80] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. (2006). *Teisės informatika ir informatikos teisė*. Vadovėlis. Vilnius: Mykolo Romerio universitetas. P. 119.
[81] 29 straipsnio darbo grupė. *Duomenų apsaugos pareigūnų gairės*. Priimta 2016 m. gruodžio 13 d.
[82] Valstybinė duomenų apsaugos inspekcija. *Duomenų apsaugos pareigūnų tikrinimo apibendrinimas*. 2023.

2.3. Asmens duomenų apsaugos priemonės

Vadovaujantis Bendrojo duomenų apsaugos reglamento 5 str. 1 d. f p., ET duomenų apsaugos konvencijos 7 str. EBPO privatumo gairių 11 str., įgyvendinant taikant duomenų saugumo principą reikalaujama, kad „duomenys būtų tvarkomi tokiu būdu, jog atitinkamomis techninėmis ir organizacinėmis priemonėmis būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo neturint leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo“.

Bendrajame duomenų apsaugos reglamento 32 str. nustatytas duomenų saugumo principas, o kitaip – vientisumo ir konfidencialumo principas įgalina duomenų valdytojus ir tvarkytojus užtikrinti saugumą ir įgyvendinti tinkamas technines ir organizacines duomenų saugumo priemones. Pasak Zaleskio J. (2019), „duomenų valdytojai ir duomenų tvarkytojai turi diskrecijos teisę bei nuožiūros laisvę neperžengiant reguliavimu nustatytų ribų pasirinkti kokias konkrečias duomenų saugumo priemones įgyvendinti ir kaip tai padaryti, kad pasirinktomis duomenų saugumo priemonėmis būtų užtikrintas tinkamas saugumas, įskaitant konfidencialumą“ (Bendrojo duomenų apsaugos reglamento preambulės 83 p.).

Zaleckio J. (2019) teigimu, nėra įtvirtinto išsamaus konkrečių ir griežtų privalomų duomenų saugumo priemonių sąrašo. Reguliavimu nustatytos kelios konkrečios duomenų saugumo priemonės, tačiau jų įgyvendinimas nėra formuluojamas kaip griežtas imperatyvas. Apibrėžiant MVĮ (duomenų valdytojų ir tvarkytojų) atsakomybę vartojami terminai „tiek, kiek reikia“ (Bendrojo duomenų apsaugos reglamento 32 str. 1 d.) arba „imtis priemonių siekiant užtikrinti“ (Bendrojo duomenų apsaugos reglamento 32 str. 4 d.).

Organizacijose atsakomosios arba saugumo prevencinės priemonės yra kelių rūšių (Štitilis, 2011):

- „Administracinis ir organizacinis saugumas;
- Personalo saugumas;
- Fizinė apsauga;
- Komunikacijų – elektroninis saugumas (ryšių apsauga);
- Programinės įrangos saugumas;
- Procesų saugumas (“Operacijų saugumas”)“[83].

Štitilis (2011) išskiria dvi pagrindines elektroninių nusikaltimų prevencijos priemones: „teisines ir organizacines – technines“. Teisinėms priemonėms priskiriami teisės normų aktai, vidinės organizacijų taisyklės ir kt.

[83] Štitilis, D. (2011). Elektroniniai nusikaltimai. Metodinė priemonė. Vilnius: Mykolo Romerio universitetas. P. 90.

2.3.1. Organizacinės asmens duomenų apsaugos priemonės

Pasak Zaleskio J. (2019), „organizacinės duomenų saugumo priemonės yra susijusios su tuo, kaip organizacija yra įsteigta ir vykdo veiklą. Pavyzdžiui, duomenų saugumą padeda užtikrinti tokios organizacinės priemonės kaip įgaliojimų tvarkyti duomenis paskirstymas, duomenų apsaugos politikos ir procedūrų nustatymas, atsakomybės už duomenų apsaugą paskirstymas organizacijoje“[84].

Valstybinė duomenų apsaugos inspekcija yra pateikusi „10 minimalių organizacinių priemonių, skirtų apsaugoti duomenų subjektų asmens duomenims, tvarkomiems MVĮ: Asmens duomenų saugumo politika ir procedūros;

- Vaidmenys ir atsakomybės;
- Prieigos valdymo politika;
- Išteklių ir turto valdymas;
- Keitimų valdymas;
- Duomenų tvarkytojai;
- Asmens duomenų saugumo pažeidimai ir saugumo incidentai;
- Veiklos tęstinumas;
- Personalo konfidencialumas;
- Mokymai“[85].

Visos organizacinės asmens duomenų saugumo priemonės turi atitikmenį ISO 27001:2017 A priede ir galimus papildomus reikalavimus pagal ISO 27701:2019, o taip pat Bendrajam duomenų apsaugos reglamentui. Visos nurodytos organizacinės asmens duomenų saugumo priemonės yra minimalios bei privalomos siekiant užtikrinti kibernetinį saugumą. Tuo tarpu siekiant įgyvendinti asmens duomenų nutekėjimo prevenciją, ypatingai svarbu užtikrinti duomenų saugumo pažeidimų ir incidentų valdymą, nes 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“ (Bendrojo duomenų apsaugos reglamento 4 straipsnio 12 dalis). Be kita ko, svarbus darbuotojų mokymas bei kibernetinio saugumo kultūros formavimas. Darbuotojai, suprantantys duomenų apsaugos bei kibernetinio saugumo procedūras, gali tinkamai įgyvendinti MVĮ turimas technines bei organizacines asmens duomenų saugumo

[84] Julius Zaleskis. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. 2019. Monografja. P.132.
[85] Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*. 2020-06-18 3 versija.

priemones bei reikšmingai prisidėti prie sėkmingo „netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų“ (Bendrojo duomenų apsaugos reglamento 32 straipsnio 2 dalis) užkardymo. Žinios apie konkrečius duomenų apsaugos bei kibernetinio saugumo reikalavimus, MVĮ veiklos pobūdžiui būtinus saugumo procesus privalomi asmenims, kurie kompiuterizuotose vietose dirba su asmens duomenimis.

Apibendrinant galima teikti, kad „geriausios praktikos organizacijoje yra gyvybiškai svarbios ir yra pagrindinė vidaus informacijos saugumo linija. Kibernetinio saugumo politikos apibrėžimas turėtų būti pirmasis iššūkis siekiant apsaugoti organizacijos duomenis ir apibrėžti procedūras, kurių reikia laikytis. Tikslas yra apibrėžti apsaugos lygį, kad būtų užtikrinta, jog organizacijos duomenys ir tinklai yra saugūs. MVĮ gali neįstengti sau leisti įgyvendinti sudėtingų ir brangiai kainuojančių efektyvių saugumo procedūrų, tačiau organizacinės asmens duomenų saugumo priemonės yra lengviau įgyvendinamos ir kainuoja ženkliai mažiau nei techninės. Šviečiamosios veiklos organizacijoje skatinimas turėtų būti pirmasis žingsnis prisidedant prie bendradarbių informuotumo apie kibernetinį saugumą ir padedant apsaugoti organizacijos duomenis ir veiklą (Maximiano A., Pinto G. 2021)“[86]. Atsižvelgiant į MVĮ specifiką, asmens duomenų apsaugos bei kibernetinės higienos mokymų organizavimas galėtų būti efektyviausia organizacine priemone. Uddin M. R.. (2024) išskiria ne tik darbuotojų mokymus, bet visos įmonės augimo pokytį, siekiant užtikrinti kibernetinio saugumo prevenciją, kadangi „duomenų pažeidimo aplinka yra dinamiška ir greitai kintanti, įmonės turi įgyti nuolatinį mokymosi procesą, orientuotą į aplinkos ir technologinius pokyčius, kad būtų pašalinta duomenų pažeidimo rizika“.

Pasak Chang L., Coppel N. (2020), yra penki veiksniai galėtų padidinti informuotumo apie kibernetinį saugumą kampanijų veiksmingumą bei pagerinti darbuotojų kibernetinės kultūros lygį:

- „Saugumo suvokimas turi būti profesionaliai parengtas ir organizuotas;
- Žmonių baimės sukėlimas nėra veiksminga taktika;
- Saugumo ugdymas turi būti daugiau nei informacijos teikimas vartotojams – jis turi būti tikslingas, veiksmingas, įgyvendinamas ir teikti grįžtamąjį ryšį;
- Kai žmonės nori keistis, reikia mokymų ir nuolatinio grįžtamojo ryšio, kad jie išliktų per pokyčių laikotarpį;

[86] Maximiano A., Pinto G. *Informacijos saugumas ir kibernetinio saugumo valdymas: atvejo tyrimas su MVĮ Portugalijoje*. 2021.

- Kuriant kampanijas būtina pabrėžti skirtingus kultūrinius kontekstus ir ypatybes[87].

2.3.2. Techninės asmens duomenų apsaugos priemonės

Įmonės, veikdami kaip duomenų valdytojai ar tvarkytojai, turi įgyvendinti ne tik organizacines asmens duomenų saugumo priemones, tačiau ir technines: „mechanizmus, įrangą ir įrankius, skirtus užtikrinti informacijos saugumą. Pavyzdžiui, techninėmis duomenų saugumo priemonėmis galima laikyti duomenų pseudonimizavimą ir šifravimą, duomenų atkūrimo priemones kilus fiziniam ar techniniam incidentui“ (Zaleskis. K. 2019).

Valstybinė duomenų apsaugos inspekcija yra pateikusi „10 minimalių techninių priemonių, skirtų apsaugoti duomenų subjektų asmens duomenims, tvarkomiems MVĮ:

- Prieigų kontrolė ir autentifikavimas;
- Techninių žurnalų įrašai ir stebėsena;
- Tarnybinių stočių, duomenų bazių apsauga;
- Darbo vietų apsauga;
- Tinklo ir komunikacijos sauga;
- Atsarginės kopijos;
- Mobilieji, nešiojamieji įrenginiai;
- Programinės įrangos sauga;
- Duomenų naikinimas, šalinimas;
- Fizinė sauga“[88].

Šios techninės asmens duomenų saugumo priemonės taip pat turi atitikmenį ISO 27001:2017 A priede ir galimiems papildomiems reikalavimams pagal ISO 27701:2019 bei Bendrajam duomenų apsaugos reglamentui. Siekiant įgyvendinti MVĮ asmens duomenų nutekėjimo prevenciją, itin svarbu vesti techninius žurnalų įrašus bei vykdyti jų stebėseną. Pasak Valstybinės duomenų apsaugos inspekcijos „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.

[87] Chang L., Coppel N. *Kibernetinio saugumo supratimo ugdymas besivystančioje šalyje: pamokos iš Mianmaro*. 2020.
[88] Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*. 2020-06-18 3 versija.

Svarbu vykdyti tinklo ir komunikacijos saugą, nes 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. Bendrojo duomenų apsaugos reglamento 32 straipsnis numato, kad „<...> atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant *inter alia,* jei reikia:

- pseudonimų suteikimą asmens duomenims ir jų šifravimą;
- gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą <...>“[89].

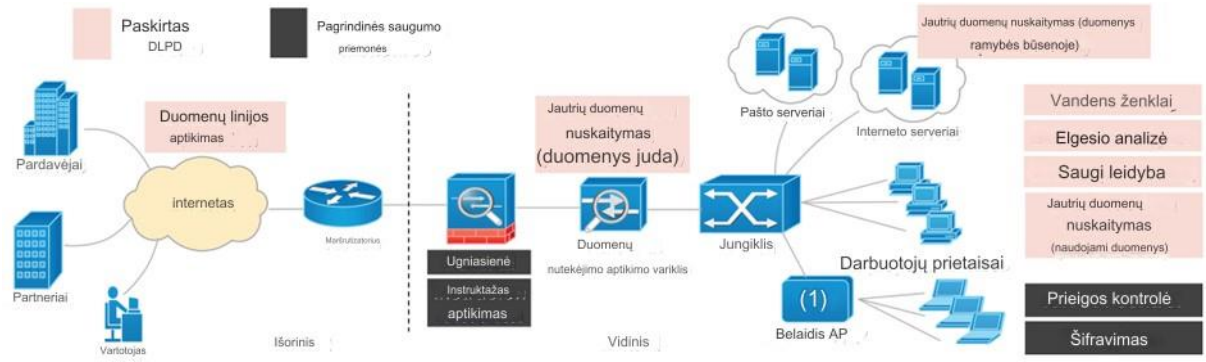
Taip pat asmens duomenų nutekėjimo prevencijai užtikrinti svarbus programinės įrangos saugos įgyvendinimas. Projektuojant ir kuriant naujas programinės įrangos sistemas, kuriose numatoma tvarkyti asmens duomenis, būtina laikytis Bendrojo duomenų apsaugos reglamento 25 straipsnyje (Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga – *angl. Privacy by Design ant Privacy by Default*) numatytų principų.

Pasak Cheng L. ir kt. (2017) „duomenų nutekėjimo prevencijos ir aptikimo metodai skirstomi į pagrindines saugumo priemones ir paskirtus duomenų nutekėjimo metodus“[90]. Pasak šių autorių, skirtingai nuo pagrindinių saugos mechanizmų, tokių kaip ugniasienės, antivirusinės programinės įrangos, įsibrovimų aptikimas, autentifikavimas, prieigos kontrolė bei šifravimas, duomenų nutekėjimo prevencijos ir aptikimo sistemos yra specialiai skirtos kovoti su duomenų nutekėjimo grėsmėmis. Autorių nuomone, „pagrindinė duomenų nutekėjimo prevencijos ir aptikimo sistemų užduotis yra nustatyti, stebėti ir apsaugoti konfidencialią informaciją nuo neteisėtos prieigos, kuri paprastai naudoja faktinį stebimų duomenų turinį arba aplinkinį kontekstą, kad aptiktų galimą nutekėjimą“.

Cheng L., ir kt. (2017) pateikia tipinius metodus (žr. 10 pav.), naudojamus duomenų nutekėjimo aptikimui ir prevencijai bei jų diegimui įmonės sistemoje. Pasak autorių, „pagrindinės saugos priemonės, pvz., saugus duomenų publikavimas, šifravimas ir prieigos prie jautrių duomenų teisių užtikrinimas, apsaugos duomenis ramybės būsenoje, o tai yra

[89] Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams. 2020-06-18 3 versija*.
[90] Cheng L. , Liu F., Yao D. *Enterprise data breach: causes, challenges, prevention, and future directions*. 2017.

pirmoji duomenų nutekėjimo mažinimo linija. Ugniasienės riboja prieigą prie vidinio tinklo. Įsibrovimų aptikimo sistemos stebi kompiuterio ir tinklo veiklą, kad ieškotų neteisėtų įsibrovimų. Antivirusinė programa gali aptikti kenkėjišką programinę įrangą, kuri vagia konfidencialią informaciją prieš nutekinant duomenis, užtikrinant apsaugą nuo vidinių atakų. Įsibrovimo aptikimo sistemos gali padėti aptikti kenkėjišką veiklą, tačiau paprastai ji patiria daug klaidingų teigiamų rezultatų. Nauji mechanizmai, skirti apsaugoti konfidencialius failus kompiuteryje, priklauso nuo virtualios mašinos technologijos“. Autoriai išskiria duomenų nutekėjimo prevencijos ir aptikimo naudojamas technologines priemones į dvi kategorijas į turinio analizę ir kontekstinę analizę. „Turiniu pagrįsti (t. y. jautrių duomenų nuskaitymo) metodai tikrina duomenų turinį, kad apsaugotų nepageidaujamą informacijos poveikį įvairiose būsenose“ (Cheng L. ir kt. 2017). Teigiama, kad šis metodas gali būti veiksmingas siekiant apsaugoti įmonę nuo netyčinio duomenų praradimo, tačiau jis nėra tinkamas apsisaugoti nuo vidinių grėsmių. Pasak autorių, „priešingai, kontekstu pagrįsti metodai daugiausia atlieka kontekstinę metainformacijos, susijusios su stebimais duomenimis arba duomenis supančiu kontekstu, analizę“ (Cheng L., ir kt. 2017).



Šaltinis: sudaryta Cheng L., Liu F., Yao D. (2017)

10 pav. Duomenų nutekėjimo prevencijos metodai

Apibendrinant galima teigti, kad kibernetinio saugumo bei asmens duomenų tvarkymo rizikos vertinimas, organizacinių bei techninių asmens duomenų apsaugos priemonių taikymas sukuria saugumo klimatą, kuris padeda įžvelgti pažeidžiamumus ir saugumo grėsmes bei įgalina pritaikyti tinkamas prevencines saugumo priemones. Pasak Uddin M. R.. (2024), „stiprios saugumo kultūros sukūrimas gali padėti sumažinti duomenų pažeidimus verslo subjekte ir tai yra esminis veiksnys, į kurį reikia atsižvelgti“[91].

[91] Uddin M. R.. *Developing a data breach protection capability framework in retailing*. 2024.

3. ASMENS DUOMENŲ NUTEKĖJIMO PREVENCIJOS PRIVATAUS SEKTORIAUS ĮMONĖSE TYRIMO METODOLOGIJA

3.1. Tyrimo aktualumo pagrindimas, objektas ir tikslas

Siekiant atskleisti asmens duomenų nutekėjimo prevencijos situaciją, pasirinktas mišrus tyrimas: kiekybinis ir kokybinis. Kiekybiniu tyrimu siekiama išsiaiškinti Pakruojo bei Pasvalio rajonų privataus sektoriaus įmonių darbuotojų kibernetinio saugumo kompetencijas bei vertinimą kaip jų darbovietės yra pasirengusios užtikrinti kibernetinio saugumo prevenciją. Kokybinio tyrimo metu siekiama išsiaiškinti Pasvalio bei Pakruojo rajonų privataus sektoriaus įmonių atsakingų už kibernetinę saugą atstovų nuomonę apie darbovietės kibernetinio saugumo rizikas, jų valdymo priemones, formuojamą kibernetinio saugumo politiką. Įvykdžius Lietuvos privataus sektoriaus mažo ir vidutinio dydžio įmonių asmens duomenų nutekėjimo prevencijos tyrimą, bus identifikuoti taikomi kibernetinės saugos metodai.

3.2. Tyrimų metodų pagrindimas ir apibūdinimas

Tyrimui atlikti bus naudojami šie metodai:

- Pusiau struktūrizuotas interviu. Kokybiniam tyrimui pasirinktas struktūrizuotas interviu, kuriuo siekiama surinkti reikiamą informaciją iš specialistų, tiesiogiai susijusių su kibernetinio saugumo įgyvendinimu ir darbuotojų kvalifikacijos kėlimu mažose ir vidutinėse įmonėse;
- Anketinė apklausa. Kiekybiniam tyrimui pasirinkta anketinė apklausa skirta Pasvalio ir Pakruojo mažose ir vidutinėse įmonėse dirbantiems darbuotojams;
- Gautų duomenų analizė. Metodas taikomas siekiant išsiaiškinti specialistų ir darbuotojų nuomonę apie taikomų asmens duomenų nutekėjimo privačiame sektoriuje prevencinių priemonių veiksmingumą. Pasitelkus analizės išvadas buvo rengiamos rekomendacijos siekiant tobulinti mažų ir vidutinių įmonių pasirengimą asmens duomenų nutekėjimo incidentams.

Tyrimo reprezentatyvumas

Kokybinio tyrimo sudarymui pasirinkta tikslinė atranka. Pusiau struktūrizuoto interviu tyrimo dalyviai atrenkami pagal šiuos kriterijus:

1. Įmonė, kurioje dirba specialistas atitinka mažos ir vidutinės įmonės sąvoką;
2. Specialistai tiesiogiai susiję su asmens duomenų nutekėjimo prevencija įmonėje.

Kiekybinio apklausos raštu tyrimo dalyviai atrenkami pagal šiuos kriterijus:

1. Įmonė, kurioje dirba darbuotojas atitinka mažos ir vidutinės įmonės sąvoką;
2. Darbuotojas, dirbantis Pasvalio arba Pakruojo mažoje ar vidutinio dydžio įmonėje.

3.3. Tyrimo dizainas, kurį sudaro trys pagrindiniai etapai:

Pirmasis etapas - tyrimo loginis pagrindimas, remiantis mokslinės literatūros teorinėmis įžvalgomis, kurios atskleidžia asmens duomenų apsaugos sampratą, asmens duomenų nutekėjimo prevencijos teisinio reguliavimo aspektus, identifikuoja asmens duomenų nutekėjimo prevencijos pajėgumų organizacines struktūras, atsakomybes ir užduotis.

Antrame etape pagrindžiama tyrimo organizavimo metodika atliekant tyrimą, taikant kokybinio tyrimo strategiją. Atliekama kokybinė mokslinės literatūros ir dokumentų turinio analizė bei pusiau struktūrizuotas interviu. Tyrimo imčiai taikyta netikimybinė tikslinė atranka. Gauti duomenys yra analizuojami naudojant kokybinio turinio (anglų k. *Content*) metodą.

Trečiame etape naudojantis pusiau struktūrizuoto interviu rezultatais, nustatomi poreikiai asmens duomenų apsaugos prevencijai. Lyginamosios gautų duomenų analizės metodu identifikuojamos privataus sektoriaus mažų ir vidutinių įmonių kibernetinio saugumo užtikrinimo prevencijos galimybės.

Tiriamoji dalis:

4. ASMENS DUOMENŲ NUTEKĖJIMO AKTUALUMO LIETUVOS MAŽO IR VIDUTINIO DYDŽIO PRIVATAUS SEKTORIAUS ĮMONIŲ TYRIMO ANALIZĖ

4.1. Kokybinio tyrimo organizavimas

Kokybinio tyrimo organizavimas. Tyrime buvo atrinktos aštuonios privataus sektoriaus įmonės: keturios įregistruotos bei veikiančios Pasvalio r. ir keturios įregistruotos bei veikiančios Pakruojo r. Tyrimas atliktas balandžio 1-10 dienomis. Kokybinio tyrimo etapų veikla išdėstyta 4 lentelėje.

4 lentelė. Kokybinio tyrimo eiga

Etapas	Etapo veikla	Etapo tikslas
Pasirengimas	Suformuluota tyrimo koncepcija ir tyrimo metodas. Parenkami tyrimo dalyviai remiantis asmenine patirtimi.	Suformuluoti tyrimo koncepciją ir parengti interviu klausimyną.
Tyrimo dalyvių parinkimas	Išsiunčiami el. laiškai su tyrimo aprašymu ir įvardijimu koks yra tyrimo tikslas. Gavus atsakymą bei gavus įmonės vadovo leidimą, susisiekiama tiesiogiai.	Gauti leidimą vykdyti tyrimą iš įmonės vadovybės.

Tyrimo vykdymas	Susisiekiama su tyrimo dalyviais, pristatomas tyrimo tikslas, organizavimo tvarka bei tyrimo etika.	Surinkti informaciją apie asmens duomenų pažeidimų prevencijos priemonių taikymą įmonėje.
Duomenų analizė	Gautų duomenų sisteminimas, apibendrinimas	Vertinti rezultatus, juos interpretuoti ir gauti išvadas.

Tyrimo etika. Kokybinio tyrimo tikslas buvo išsiaiškinti įmonių patirtis kibernetinio saugumo kontekste, todėl iš pradžių buvo gautas vadovų leidimas atlikti tyrimą. Pasirinktų įmonių vadovams (direktoriams) buvo išsiųstas el. laiškas su tyrimo tikslu bei uždaviniais, siekiant gauti leidimą vykdyti tyrimą. Vėliau su vadovais buvo susisiekta telefonu bei vizito metu.

Visi tyrimo dalyviai struktūrizuotame interviu dalyvavo laisva valia. Siekiant išsaugoti tyrimo dalyvių anonimiškumą, tyrime nėra atskleidžiamos įmonės, tyrimų dalyvių vardai, pavardės ar pareigybės, nes daugumoje įmonių šias pareigybes užima vienas žmogus, todėl tyrimo dalyviams yra priskirti kodai, o įmonių pavadinimai neskelbiami (žr. 7 lentelę).

7 lentelė. Tyrimo dalyvių grupė

Kodas	Įmonė
TD1	AB „X“ saugos specialistas
TD2	UAB „X“ saugos specialistas
TD3	UAB „X“ saugos specialistas
TD4	UAB „X“ saugos specialistas
TD5	UAB „X“ saugos specialistas
TD6	UAB „X“ saugos specialistas
TD7	UAB „X“ saugos specialistas
TD8	UAB „X“ saugos specialistas

Tyrimo dalyvių apklausos analizė

Tyrimo dalyviams buvo užduoti 8 klausimai

1. Kaip Jūsų įmonė formuoja ir įgyvendina kibernetinio saugumo politiką, siekdama apsaugoti įmonėje tvarkomus asmens duomenis?
2. Kokias konkrečias kibernetinio saugumo priemones Jūsų įmonė taiko asmens duomenų apaugai užtikrinti ir kaip vertinate jų efektyvumą?

3. Kaip Jūsų įmonė užtikrina, kad visi darbuotojai būtų tinkamai informuoti ir mokomi apie asmens duomenų saugumo svarbą ir praktikas?
4. Kokius procesus Jūsų įmonė turi nustatytais atvejais, kai įvyksta asmens duomenų saugumo pažeidimas?
5. Kaip Jūsų įmonė integruoja naujausias technologijas ir inovacijas į asmens duomenų apsaugos procesus?
6. Kaip Jūsų įmonė užtikrina atitiktį nacionaliniams ir tarptautiniams duomenų apsaugos teisės aktams?
7. Kaip Jūsų įmonė identifikuoja ir valdo rizikas, susijusias su asmens duomenų apsauga?
8. Kaip Jūs bendradarbiaujate su savo partneriais ir tiekėjais, siekdami užtikrinti, kad visoje tiekimo grandinėje būtų laikomasi asmens duomenų apsaugos standartų?

4.2.Kokybinio interviu tyrimo rezultatai

Toliau nagrinėjami kokybinio tyrimo dalyvių atsakymai į klausimus.

1. Kaip Jūsų įmonė formuoja ir įgyvendina kibernetinio saugumo politiką, siekdama apsaugoti įmonėje tvarkomus asmens duomenis?

Trys iš aštuonių tyrimo dalyvių teigia, kad jų įmonėje kibernetinio saugumo politiką formuoja išorės konsultantai, pasirinkti IT paslaugų teikėjai. Respondentai teigia, kad „neturi vidinių resursų bei kompetentingo personalo“, taigi susiduria su žmogiškųjų išteklių trūkumu užtikrinant kibernetinį saugumą. Trys turimo dalyviai teigia, kad „yra pasitvirtinę lokalinius teisės aktus, suteikiančius pareigą darbuotojams bei tiekėjams užtikrinti kibernetinio saugumo politiką“. Dalyvis TD1 teigia, kad jų įmonėje „parengti vidiniai dokumentai (prieigos teisių valdymo tvarkos aprašas, slaptažodžių sudarymo tvarkos aprašas kt.) bei procedūros, formuojančios kibernetinio saugumo politiką“. Du tyrimo dalyviai teigia, kad įmonė „stengiasi dokumentuoti vidiniais teisės aktais esamus kibernetinio saugumo procesus, nustato kai kurias taisykles ir tvarkas darbuotojams, tačiau dar yra „kelyje“ ir ne viską dar užtikrina“. Taip pat du tyrimo dalyviai teigia, kad jų įmonės kibernetinio saugumo politiką „įgyvendina minimaliai, neturi tvarkų ir neveda mokymų darbuotojams“.

Pastebėtina, kad tyrimo dalyviai savo įmonių kibernetinio saugumo politiką vertina kaip nepakankamai išsamią ir nepilnavertiškai užtikrinančią kibernetinį saugumą įmonėje, tačiau galima teigti, kad dalis tyrimo dalyvių suvokia kibernetinio saugumo politikos svarbą bei siekia, kad įmonė planuotų stiprinti įmonės kibernetinio saugumo politiką ateityje.

2. Kokias konkrečias kibernetinio saugumo priemones Jūsų įmonė taiko asmens duomenų apaugai užtikrinti ir kaip vertinate jų efektyvumą?

Tyrimo dalyviai teigia, kad įmonės taiko pagrindines kibernetinio saugumo priemones, tokias kaip: „antivirusines sistemas, ugniasienes, SSL sertifikatą, nereikalinga įranga nenaudojama antriniam panaudojime, vykdoma prieigos kontrolė (darbuotojai gali prisijungti prie sistemų su savo slaptažodžiu), užtikrinama fizinė sauga, operacinė sistema nuolat atnaujinama, daromos atsarginės kopijos, kamerų sistema neprijungta prie interneto, atliekamas tinklo segmentavimas, naudojamas virtualus privatus tinklas (VPN), naudojama tik legali programinė įranga, darbus atlieka profesionalūs darbuotojai“.

Pažymėtina, kad tik vienas tyrimo dalyvis (TD6) teigia, kad „duomenų bazė šifruojama, atliekamas tinklo segmentavimas, daromos rezervinės duomenų kopijos su bandymais atkurti duomenis. Šifruojama pažangiais metodais“.

Atsižvelgiant į klausimyno rezultatus, pastebima, kad dauguma (7/8) tyrimo dalyvių įmonių įgyvendina tik minimalias kibernetinio saugumo priemones.

3. Kaip Jūsų įmonė užtikrina, kad visi darbuotojai būtų tinkamai informuoti ir mokomi apie asmens duomenų saugumo svarbą ir praktikas?

Du iš aštuonių tyrimo dalyvių teigia, kad išorės tiekėjas (IT įmonė) vykdo pirminius asmens duomenų apsaugos ir kibernetinės higienos mokymus. Vienas tyrimo dalyvis teigia, kad „įdarbinant darbuotoją, kartu su darbų saugos instruktažu, keliais sakiniais papasakojama darbuotojui, kad būtina laikytis konfidencialumo įsipareigojimų, su darbuotojais pasirašomi konfidencialumo pasižadėjimai, tačiau asmens duomenų apsaugos ar kibernetinio saugumo mokymai nėra vedami“. Vienas tyrimo dalyvis (TD8) teigia, kad „atsakingiems darbuotojams yra nuperkami išorės tiekėjų mokymai, o po to šie darbuotojai perduoda informaciją ir kitiems darbuotojams, taip atlikdami minimalią informacijos sklaidą“.

Apibendrinant, galima įžvelgti, kad didžioji dalis (6/8) tyrimo dalyvių asmens duomenų apsaugos mokymų darbuotojams neveda. Tyrimo dalyviai, vedantys asmens duomenų apsaugos bei kibernetinės higienos/saugumo mokymus pasitelkia išorės tiekėjus, nesiremia vidiniais žmogiškaisiais resursais. Tyrimo dalyviai neeliminuoja mokymų bei praktinių įgūdžių formavimo svarbos, tačiau šią priemonę palieka ateičiai.

4. Kokius procesus Jūsų įmonė turi nustatytais atvejais, kai įvyksta asmens duomenų saugumo pažeidimas?

Pažymėtina, kad pusė (4/8) tyrimo dalyvių pasirengę Asmens duomenų tvarkymo taisykles arba Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą, kuriuo vadovaujantis yra tiriami asmens duomenų saugumo pažeidimai. Tyrimo dalyvis (TD1) teigia, kad „pažeidimą pastebėjęs darbuotojas informuoja tiesioginį vadovą. Tiesioginis vadovas atlieka tyrimą ir nustato asmens duomenų saugumo pažeidimo poveikio duomenų subjektams lygį. Nustačius

didelį poveikį ir aukštą riziką duomenų subjektui/-ams, ne vėliau nei per 72 val. rengiamas pranešimas Valstybinei duomenų apsaugos inspekcijai (esant poreikiui ir policijai). Taip pat vertinimas pranešimo pateikimo duomenų subjektui, kurio asmens duomenys prarasti/atskleisti būtinumas. Po įvykio rengiamas pažeidimų valdymo planas, kuriuo numatomos papildomos prevencijos priemonės duomenų saugumui užtikrinti“. Tyrimo dalyvis TD2 teigia, kad jų įmonė atlikusi būtinuosius veiksmus pagal iš anksto pasitvirtintas tvarkas, įvykus pažeidimui „imasi priemonių, kad toks įvykis nepasikartotų ateityje“. Tyrimo dalyvis TD8 teigia, kad „esant reikalui, kreipiamasi į teisininkus ar išorės IT paslaugų teikėjus“.

Apibendrinant, pusė tyrimo dalyvių teigia, kad jų įmonės asmens duomenų saugumo pažeidimų valdymui nėra pasiruošusios, procesų neturi, nėra numatytos atsakomybės, planai ir veiksmai, kuriuos būtina atlikti siekiant sumažinti ir (ar) panaikinti asmens duomenų saugumo pažeidimo sukeltas pasekmes. Įvykus saugumo pažeidimui tikimasi, kad darbuotojai praneš direktoriui ar tiesioginiam vadovui, tačiau jie nėra niekaip įpareigoti. Taip pat jie nesupažindinami kas yra laikytina asmens duomenų saugumo pažeidimu, nenumatytas reagavimo laikas bei nenustatyti informavimo būdai.

5. Kaip Jūsų įmonė integruoja naujausias technologijas ir inovacijas į asmens duomenų apsaugos procesus?

Visi tyrimo dalyviai pateikė informaciją, kad neintegruoja naujausių technologijų bei inovacijų į asmens duomenų apsaugos procesus.

6. Kaip Jūsų įmonė užtikrina atitiktį nacionaliniams ir tarptautiniams duomenų apsaugos teisės aktams?

Tyrimo dalyviai pasidalino, kad stengiasi „įgyvendinti technines ir organizacines priemones, užtikrinančias asmens duomenų apsaugą pagal Asmens duomenų teisinės apsaugos įstatymą bei Bendrąjį duomenų apsaugos reglamentą. Įmonė nesaugo perteklinių duomenų, darbuotojai pasirašo konfidencialumo pasižadėjimus, laikosi pagrindinių duomenų kiekio mažinimo, saugojimo trukmės ribojimo principų“. Tyrimo dalyvis TD2 teigia, kad „įmonė užtikrina nacionalinius ir tarptautinius duomenų apsaugos standartus pasitelkdama duomenų apsaugos pareigūną, vykdo reguliarius asmens duomenų apsaugos mokymus, reguliariai atnaujina asmens duomenų apsaugos tvarkų aprašus, veda veiklos įrašus, tikrina gavėjų prašymų teisėtumą, laikosi konfidencialumo principų ir taiko aukštus reikalavimus savo darbuotojams, tvarkantiems asmens duomenis“.

Apibendrinant galima teikti, kad įmonės atitiktį nacionaliniams ir tarptautiniams teisės aktams užtikrina minimaliai. Tik viena įmonė iš aštuonių, įgyvendina reikalavimą vesti veiklos

įrašus, atnaujinti tvarkas ir kt. Vienas tyrimo dalyvis teigia, kad teisiniai įpareigojimai iki galo nėra aiškūs.

7. Kaip Jūsų įmonė identifikuoja ir valdo rizikas, susijusias su asmens duomenų apsauga?

Atsižvelgiant į tyrimo dalyvių atsakymus, nei viena įmonė neidentifikuoja rizikų, susijusių su asmens duomenų apsauga, šių rizikų nevaldo. Taip pat nėra atliekami rizikų vertinimai. Preziumuojama, kad neatliekant rizikų vertinimo, įmonės neturi galimybės identifikuoti galimų grėsmių bei nustatyti šias grėsmes eliminuojančių saugumo priemonių. Netaikant saugumo priemonių, neįgyvendinama asmens duomenų saugumo prevencija.

8. Kaip Jūs bendradarbiaujate su savo partneriais ir tiekėjais, siekdami užtikrinti, kad visoje tiekimo grandinėje būtų laikomasi asmens duomenų apsaugos standartų?

Visi tyrimo dalyviai paminėjo, kad jų įmonės sudarant sutartis su savo partneriais ir tiekėjais, rengia papildomus susitarimus, asmens duomenų tvarkymo sutartis ir pan., kuriomis įpareigoja partnerius ir tiekėjus, tvarkančius asmens duomenis, laikytis asmens duomenų apsaugos standartų. Tyrimo dalyvis (TD2) teigia, kad jų įmonė pasirašydama sutartį su tiekėju, sutarties projektą derina su duomenų apsaugos pareigūnu, vertina tiekėjo teikiamų paslaugų saugumą, prašo pateikti turimus standartus, vertina įmonės amžių bei prisiimtus įsipareigojimus.

Galima teigti, kad visos apklausoje dalyvavusios įmonės, tyrimo dalyvių teigimu įpareigoja partnerius ir tiekėjus laikytis sutartinių įsipareigojimų, tačiau nei vienas tyrimo dalyvis nepaminėjo, kad įmonė atlieka tiekėjo ir (ar) partnerio auditavimą, subtiekėjų vertinimą.

4.3.Kiekybinio tyrimo organizavimas

Kiekybinio tyrimo apklausos modeliavimas. Pasirinktas tyrimo instrumentas – apklausa internetu. Tyrimo dalyviai į klausimus atsakinėjo savarankiškai, jiems tinkamu metu ir patogioje aplinkoje. Tyrimo metu buvo siekiama sužinoti kaip darbuotojai geba identifikuoti kibernetinio saugumo rizikas bei taikyti asmens duomenų nutekėjimo prevencijos priemones. Pagal šiuos tikslus, tyrimo klausimai buvo sugrupuoti į 6 temas (žr. 5 lentelę).

5 lentelė. Tyrimo klausimų grupės ir tikslai

Eil. Nr.	Grupė	Tikslas
1.	Socialiniai – demografiniai tiriamųjų duomenys	Nustatyti tiriamųjų lytį ir gyvenamąją vietovę

2.	Darbuotojų supratimas apie asmens duomenų apsaugą	Išsiaiškinti kaip darbuotojai supranta asmens duomenų apsaugos svarbą
3.	Esamos saugumo priemonės ir procedūros	Išsiaiškinti kokios saugumo priemonės ir procedūros yra taikomos įmonės tvarkomų asmens duomenų nutekėjimo prevencijai užtikrinti
4.	Darbuotojų mokymai ir sąmoningumo lygis	Išsiaiškinti kaip dažnai įmonėje yra vykdomi asmens duomenų apsaugos bei kibernetinio saugumo mokymai ir koks yra darbuotojų sąmoningumo lygis
5.	Asmens duomenų nutekėjimo atvejai	Išsiaiškinti ar įmonėje buvo asmens duomenų nutekėjimo atvejų ir ar yra numatytas asmens duomenų saugumo pažeidimų valdymo planas
6.	Požiūris į privatumo politiką ir reguliavimą	Išsiaiškinti darbuotojų požiūrį į įmonės privatumo politiką bei teisinį reguliavimą.

Tyrimo imtis. Atsižvelgiant į tai, kad tyrimui aktuali populiacija yra baigtinė bei siekiant jog turimo imtis būtų reprezentatyvi, imties tūris apskaičiuojamas pagal Ingos Gaižauskienės ir Svajonės Mikėnės pateiktą formulę (Gaižauskienė ir Mikėnė, 2014, p. 42):

$$n = \frac{t^2 N p(1-p)}{\triangle^2 N + t^2 p(1-p)};$$

Formulės žymėjimų reikšmės:

n – imties tūris;

N – populiacijos dydis;

t – stjudento koeficientas, išreiškiantis patikimumo lygmenį;

p – numatomas pasiskirstymas;

$\triangle$ - paklaida.

Remiantis Statistikos departamento duomenimis, Pasvalio rajono savivaldybėje 2024 metų pradžioje buvo įregistruoti 1217 ūkio subjektų, kuriuose dirbo 586 darbuotojai. Tuo tarpu Pakruojo rajono savivaldybėje 2024 metų pradžioje buvo įregistruoti 791 ūkio subjektai, kuriuose dirbo 465 darbuotojai. Tame tarpe mažų ir vidutinių įmonių skaičius Pasvalio rajone sudarė 489 įmones, o Pakruojo rajone – 324. Pasirinktas 95 procentų patikimumo lygmuo. Pasak Gaižauskienės ir Mikėnės (2014), “tai kompromisinis pasirinkimas, užtikrinantis

toleruotiną patikimumą bei optimalų imties dydį“ (p. 40). Įvertinus galimą respondentų kiekį, buvo pasirinkta 5 procentų paklaida.

Atlikus skaičiavimus pagal aukščiau pateiktą formulę, gautas tyrimo imties dydis – 271 tyrimo dalyvis.

Kiekybinio tyrimo eiga. Siekiant atlikti kiekybinį tyrimą, dalyvių apklausai buvo pasirinktas klausimyno pildymas tiesiogiai internete „Google docs“ formoje. Anketinės apklausos nuoroda buvo pasidalinta socialiniame tinkle „Facebook“ bei pateikiant elektroniniu paštu Pakruojo rajono verslininkų ir darbdavių asociacijai bei Pasvalio verslininkų asociacijai „Verslo žiedas“. Tyrimas buvo vykdomas iki tol, kol buvo surinkti 107 atsakymai į klausimyną ir daugiau nei savaitę nebuvo sulaukta daugiau respondentų, pageidaujančių dalyvauti tyrime. Taigi, tyrime dalyvavo 11,76 % visų respondentų ir tai lemia empirinės dalies ribotumą. Todėl tikėtina, kad tyrimo išvados nebūtinai atitiks generalinės imties poreikius.

Tikėtina, kad mažesnį respondentų dalyvavimą tyrime galėjo lemti šie veiksniai:

1. Ne visų Pasvalio bei Pakruojo mieste dirbančių asmenų darbo vietos yra kompiuterizuotos (pvz. kasininkai, apsaugos darbuotojai, valytojai ir kt.);
2. Nenoras ir/arba baimė atskleisti informaciją apie darbovietę;
3. Praleido galimybę dalyvauti tyrime dėl pamaininio darbo, atostogų, ligos ir pan.;
4. Baimė spausti nuorodas iš svetimų gavėjų.

Elektroniniu būdu pateikiamos anketos kūrimo strategijoje buvo numatyta, kad negalima pateikti atsakymų, jeigu bent vienas klausimas neatsakytas, todėl visos anketos buvo tinkamos tolimesnei analizei. Kiekybinio tyrimo etapai išdėstyti 6 lentelėje.

6 lentelė. Kiekybinio tyrimo eiga

Etapas	Etapo veikla	Etapo tikslas
Pasirengimas	Suformuluojama tyrimo koncepcija ir tyrimo metodas. Parengiamas anketinės apklausos klausimynas, kuris įkeliamas į anketinę platformą.	Parengtas apklausos klausimynas.
Tyrimo vykdymas	Klausimyno nuoroda pasidalinama socialiniame tinkle, taip pat nusiunčiama	Surinkta informacija apie darbuotojų nuomonę dėl kibernetinio saugumo

	Pakruojo rajono verslininkų ir darbdavių asociacijai bei Pasvalio asociacijai „Verslo žiedas“. Vykstama į Pasvalio bei Pakruojo rajonų įmones su atspausdintais klausimynais ir gavus vadovų leidimą, jais pasidalinama.	prevencijos užtikrinimo darbovietėje.
Duomenų analizė	Gautų duomenų sisteminimas bei informacijos apibendrinimas pagal „Google docs“ formatu atliktą apklausą.	Rezultatų interpretavimas, vertinimas bei išvadų gavimas.

Tyrimo etika. Atliekant tyrimą buvo laikomasi Gaižauskienės ir Mikėnės (2014) pateikiamų svarbiausių respondentų gerovę nusakančių principų: „informuotas ir savanoriškas sutikimas dalyvauti tyrime; anonimiškumo ir gautos informacijos konfidencialios informacijos užtikrinimas; žalos respondentams vengimas“ (p. 45). Prieš dalyvaujant tyrime, respondentai buvo supažindinami su tyrimu, jo tikslu bei etikos principų taikymu. Respondentams nebuvo daromas tiesioginis ar netiesioginis spaudimas dalyvauti tyrime. Įgyvendinant anonimiškumo principą, visi pateikti duomenys aprašomi tik apibendrintai, o klausimyno atsakymų rezultatai yra prieinami tik tyrėjui. Klausimyne prašoma pateikti lytį bei kiek laiko darbuotojas dirba įmonėje, tačiau šie duomenys nėra laikomi asmens duomenimis, nes iš pateiktų atsakymų nėra įmanoma identifikuoti fizinio asmens.

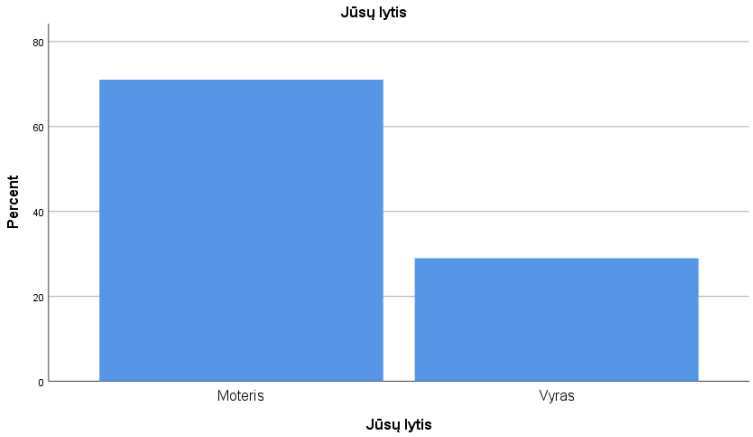
Duomenų analizės metodai. Gautų duomenų analizei bei apdorojimui naudojama statistinės analizės programos SPSS 26.0 versija. Duomenų apipavidalinimui ir grafiniam pateikimui naudojama MS Office paketo programa MS Exel. Siekiant nustatyti ar tarp kintamųjų yra statistinis ryšys, buvo pasirinktas Chi-kvadrato (χ^2) statistinio testo metodas, skirtas nominalių ir ordinalinių kintamųjų bei nominalinių kintamųjų tarpusavio priklausomybei tikrinti.

Duomenų analizei pasirinkta vienoda α=0.05 reikšmingumo lygmens reikšmė.

4.4.Kiekybinės apklausos anketos tyrimo rezultatai

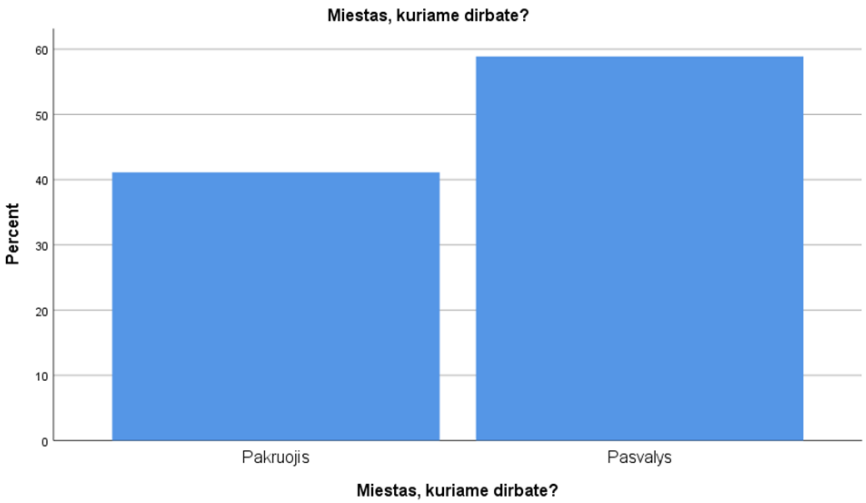
Tyrimo socialiniai demografiniai duomenys.

Tyrime dalyvavo 107 Pasvalio bei Pakruojo mažo ir privataus sektoriaus įmonėse dirbantys darbuotojai. Iš jų 76 (71%) moterų ir 31 (29%) vyrų (žr. 11 pav.).



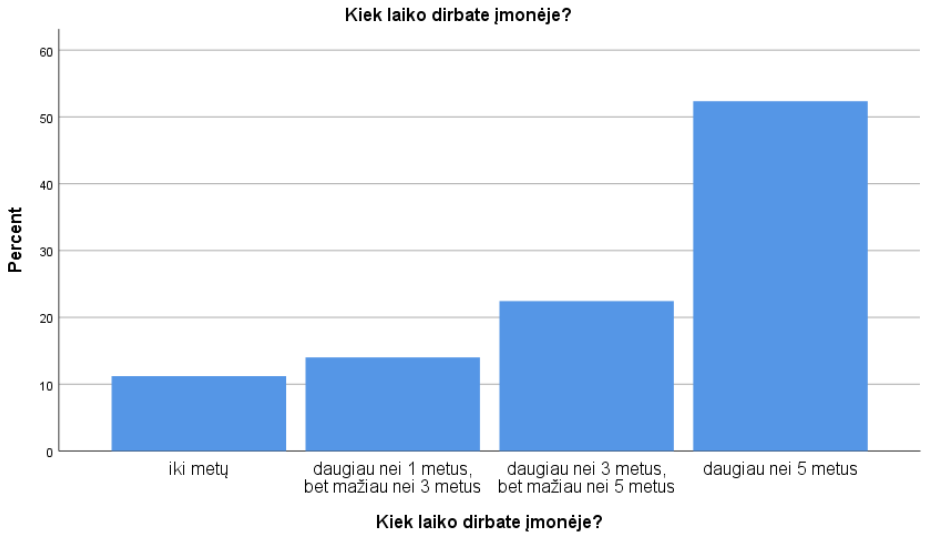
11 pav. Tyrimo dalyvių lytis

Siekiant ištirti kaip skirtingų apskričių (Panevėžio bei Šiaulių) pasirinktuose miestuose mažo ir vidutinio dydžio privačiame sektoriuje dirbantys tyrimo dalyviai vertina savo bei darbovietės pasirengimą asmens duomenų nutekėjimo prevencijai, buvo pasirinkti Pasvalio bei Pakruojo miestai. Tyrime dalyvavo 63 (58,9%) Pasvalio mažo ir vidutinio dydžio įmonėse dirbantys darbuotojai ir 44 (41,1%) Pakruojo mažo ir vidutinio dydžio įmonėse dirbantys darbuotojai (žr. 12 pav.). Tokį santykį galėjo lemti tai, kad Pasvalio mieste yra daugiau (1217 registruotų įmonių) mažo ir vidutinio dydžio įmonių nei Pakruojyje (791 registruota įmonė). Analogiškai Pasvalio mieste dirba daugiau darbuotojų. Pasvalio mieste – 586, o Pakruojo – 324.



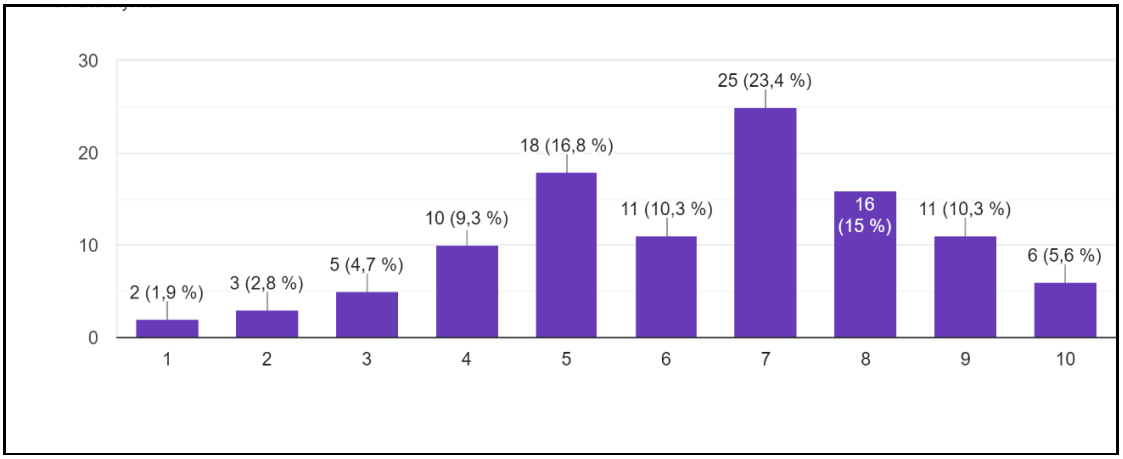
12 pav. Miestas, kuriame dirbate?

Tyrimo dalyviams buvo užduodamas klausimas kiek laiko jie dirba savo darbovietėje. Darbo laiko trukmė buvo suskirstyta į šiuos laikotarpius (žr. 13 pav.): iki metų; daugiau nei 1 metus, bet mažiau nei 3 metus; daugiau nei 3 metus, bet mažiau nei 5 metus; daugiau nei 5 metus. Daugiausia apklaustųjų pažymėjo, kad dirba ilgiau nei 5 metus. Net 56 (52,3%) dirba ilgiau nei 5 metus. 24 (22,4%) tyrimo dalyvių pažymėjo, kad dirba daugiau nei 3 metus, bet mažiau nei 5 metus. Daugiau nei 1 metus, bet mažiau nei 3 metus dirba 15 (14%) tyrimo dalyvių. Mažiausiai tyrimo dalyvių pažymėjo, kad dirba iki metų 12 (11,2%).



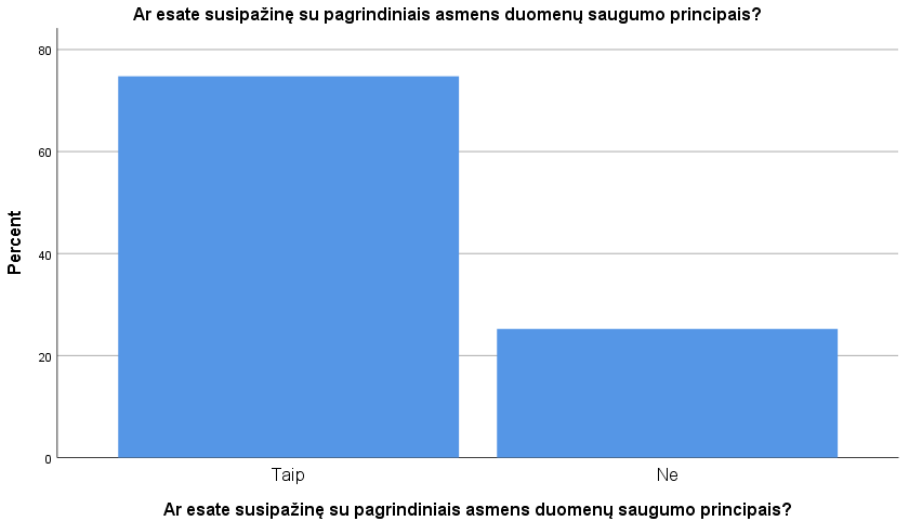
13 pav. Kiek laiko dirbate įmonėje?

Atliekant tyrimą buvo siekiama išsiaiškinti kaip darbuotojai vertina savo žinias apie asmens duomenų apsaugą. 25 (23,4%) tyrimo dalyvių savo žinias vertina 7 balais. Pažymėtina, kad 18 (16,8%) tyrimo dalyvių savo žinias apie asmens duomenų apsaugą vertina 5 balais. Itin aukštai savo žinias vertina ir 10 balų skyrė 6 (5,6%) tyrimo dalyviai. Tuo tarpu itin prastai savo žinias vertina ir tik 1 balą dešimtbalėje skalėje skiria 2 (1,9%) tyrimo dalyviai (žr. 14 pav.).



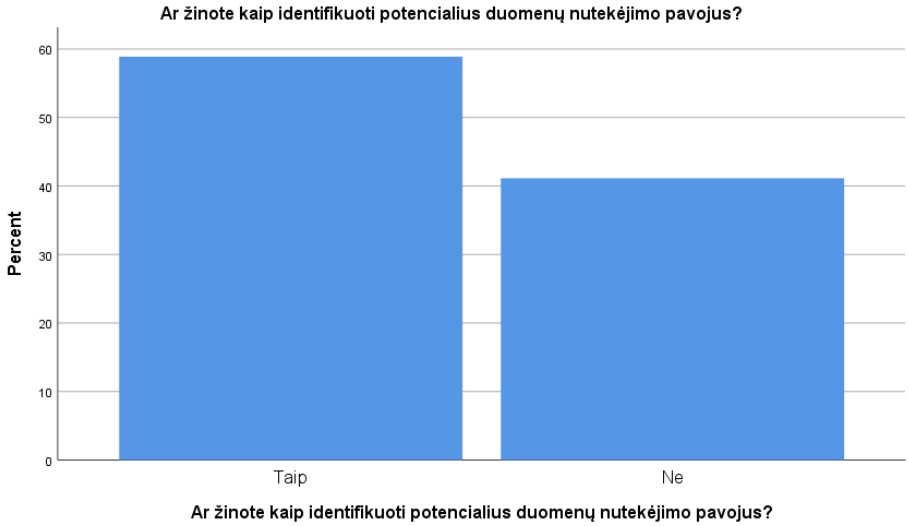
14 pav. Įvertinkite savo žinias apie asmens duomenų apsaugą

Penktuoju klausimu buvo siekiama nustatyti ar tyrimo dalyviai yra susipažinę su pagrindiniais asmens duomenų saugumo principais. 80 (74,8%) respondentų pažymėjo, kad yra susipažinę su pagrindiniais asmens duomenų saugumo principais. Tuo tarpu 27 (25,2%) respondentų pažymėjo, kad nėra susipažinę net su pagrindiniais asmens duomenų saugumo principais (žr.15 pav.).



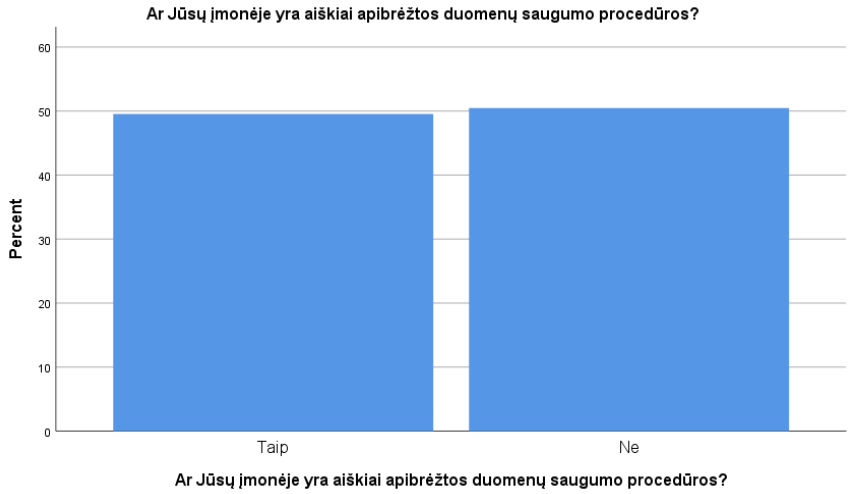
15 pav. Ar esate susipažinę su pagrindiniais asmens duomenų apsaugos principais

Tyrimo dalyvių buvo klausiama ar jie žino kaip identifikuoti potencialius asmens duomenų nutekėjimo pavojus. Atlikus tyrimą buvo nustatyta, kad 63 (58,9%) tyrimo dalyvių žino kaip identifikuoti potencialius asmens duomenų nutekėjimo pavojus, tačiau net 44 (41,1%) respondentų pažymėjo, kad neatpažįsta galimų asmens duomenų nutekėjimo grėsmių (žr.16 pav.).



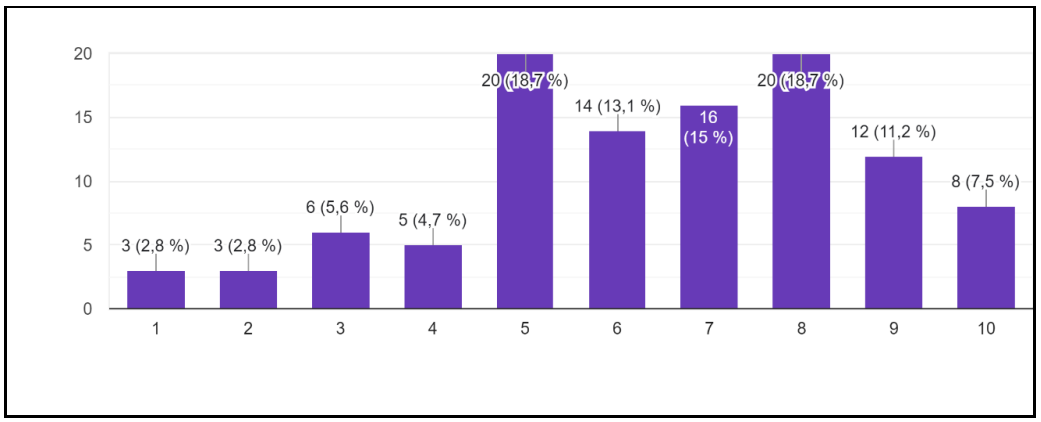
16 pav. Ar žinote kaip identifikuoti potencialius duomenų nutekėjimo pavojus?

Siekiant išsiaiškinti ar mažo ir vidutinio dydžio privataus sektoriaus įmonėse yra parengtos įvairios lokalios tvarkos, politikos bei taisyklės bei nustatytas darbuotojams aiškus asmens duomenų saugumą užtikrinantis darbo procesas, tyrimo dalyvių buvo klausiama ar jų įmonėje yra aiškiai apibrėžtos duomenų saugumo procedūros. Tyrimo dalyvių atsakymai pasiskirstė beveik tolygiai. Net 54 (50,5%) tyrimo dalyvių teigia, kad jų įmonėje nėra aiškiai apibrėžtų duomenų saugumo procedūrų. Dalyje šių įmonių procedūros yra, tačiau darbuotojai nėra su jomis supažindinti. 53 (49,5%) tyrimo dalyviai teigė, kad jų įmonėje yra aiškiai apibrėžtos asmens duomenų saugumo procedūros (žr. 17 pav.).



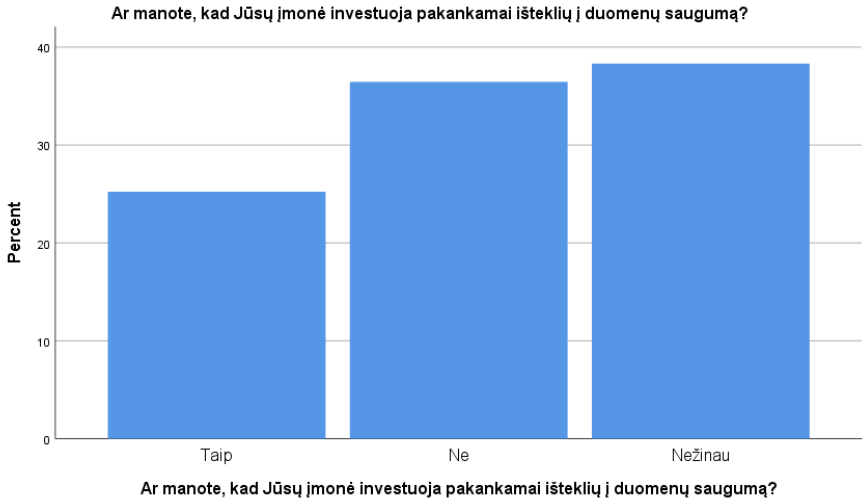
17 pav. Ar Jūsų įmonėje yra aiškiai apibrėžtos duomenų saugumo procedūros?

Tyrimo dalyviai įmonėse taikomas saugumo priemones vertina 5-8 balų lygyje. Stebimas tolygus vertinimo lygio paskirstymas: po 20 (18,7%) tyrimo dalyvių įmonėje taikomas saugumo priemones vertina 5 ir 8 balais. 16 (15%) tyrimo dalyvių taikomas saugumo priemones vertina 7 balais, o 14 (13,1%) – 6 balais. Galima teikti, kad tyrimo dalyviai vidutiniškai taikomas saugumo priemones vertina 6-7 balais (žr. 18 pav.).



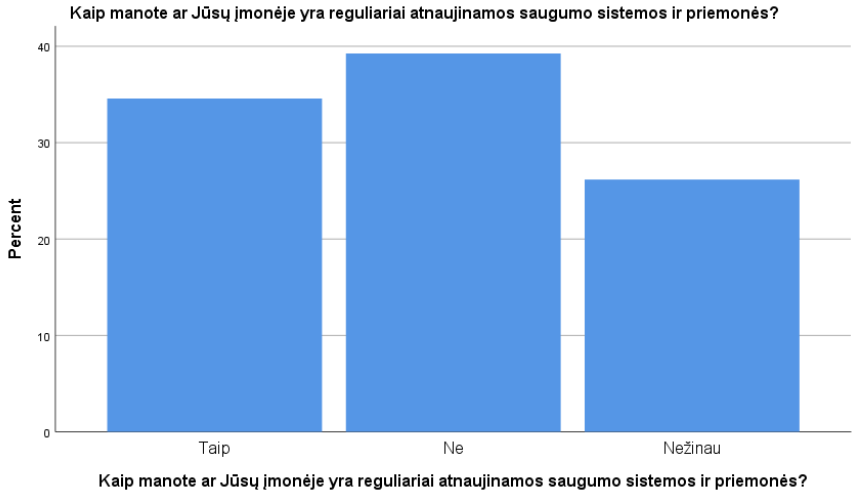
18 pav. Kaip vertinate Jūsų įmonėje esamų saugumo priemonių efektyvumą?

Devintuoju klausimu buvo siekiama nustatyti kaip tyrimo dalyviai vertina ar jų darbovietė pakankamai investuoja į duomenų saugumą. 27 (25,2%) tyrimo dalyviai teigia, kad jų nuomone, įmonė pakankamai investuoja į duomenų saugumą, tačiau 39 (36,4%) tyrimo dalyvių mano, kad įmonė pakankamai neinvestuoja, o 41 (38,3%) teigia, kad nežino. Galima daryti prielaidą, kad darbuotojai pastebėtų investicijas, brangias saugumo priemones, todėl bent dalis įmonių, apie kurių investicijas tyrimo dalyviai nežino, būtų galima priskirti prie įmonių, kurios nepakankamai investuoja į duomenų saugumą (žr.19 pav.).



19 pav. Ar manote, kad Jūsų įmonė investuoja pakankamai išteklių į duomenų saugumą?

Tyrimo dalyvių nuomone, įmonės nepakankamai reguliariai atnaujina saugumo sistemas ir priemones. 42 (39,3) respondentai pažymėjo, kad įmonės neatnaujina saugumo sistemų ir priemonių, o net 28 (26,2%) respondentų nežino apie sistemų bei priemonių reguliarų atnaujinimą (žr. pav. 20).

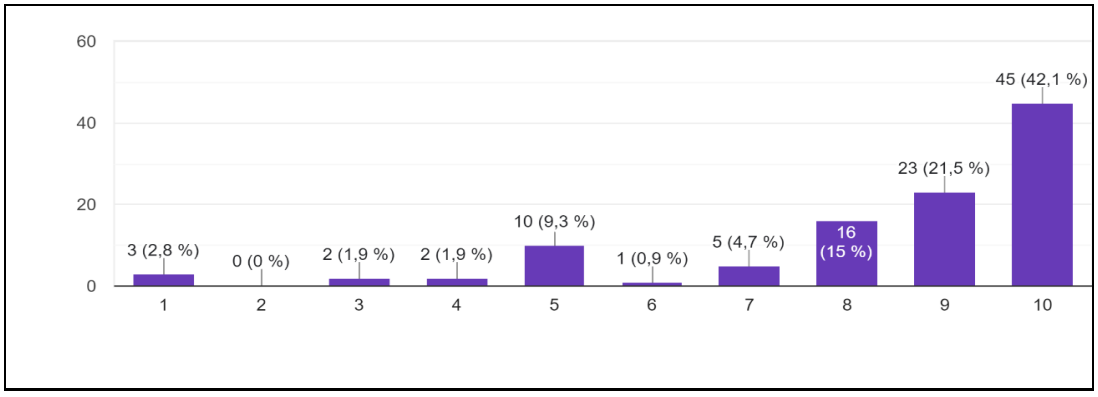


20 pav. Kaip manote, ar Jūsų įmonėje yra reguliariai atnaujinamos saugumo sistemos ir priemonės?

Viena iš svarbiausių organizacinių asmens duomenų saugumo priemonių – darbuotojų mokymai. Ši priemonė yra esminė, siekiant užtikrinti asmens duomenų apsaugos nutekėjimo prevenciją. Pažymėtina, kad 82 (76,6%) tyrimo dalyviai per paskutiniuosius 12 mėnesių nedalyvavo duomenų apsaugos mokymuose (žr. pav.21). Galima daryti išvadą, kad dauguma mažo ir vidutinio dydžio įmonių nevykdo asmens duomenų apsaugos mokymų darbuotojams.

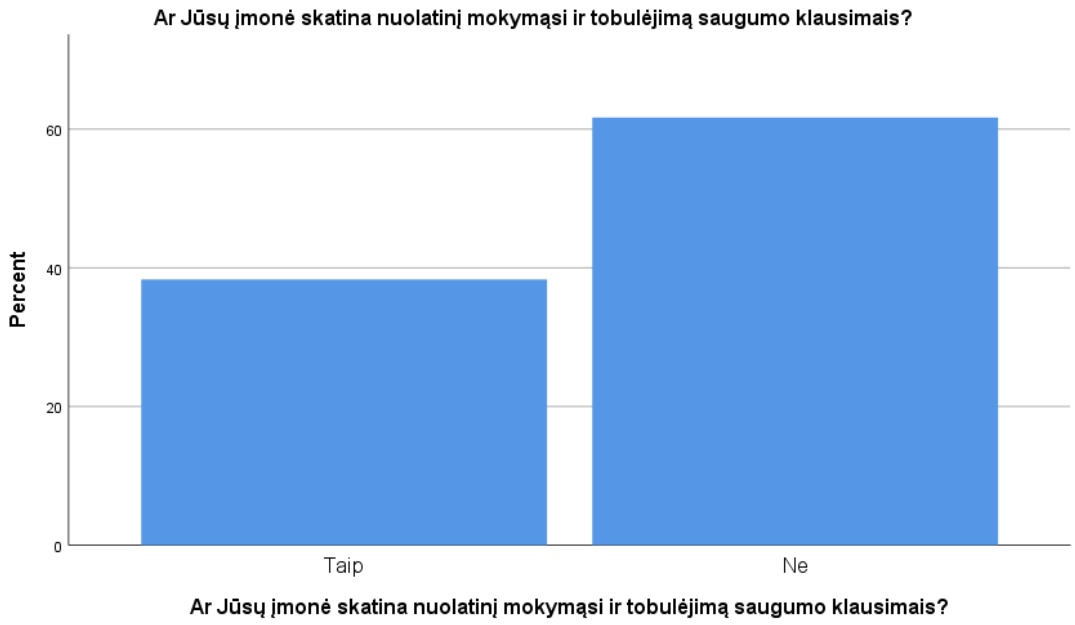
21 pav. Ar per paskutinius dvylika mėnesių dalyvavote duomenų apsaugos mokymuose?

Tyrimo dalyviai vertina, kad duomenų apsaugos mokymų poveikis turi teigiamą įtaką jų sąmoningumui. 45 (42,1%) respondentų dešimtbalėje skalėje pažymėjo 10 balų vertę galimam duomenų apsaugos mokymų teigiamam poveikiui bei kibernetinio saugumo kultūros formavimui. Taip pat 23 (21,5%) bei 16 (15%) skyrė po 9 ir 8 balus (žr. 22 pav.).



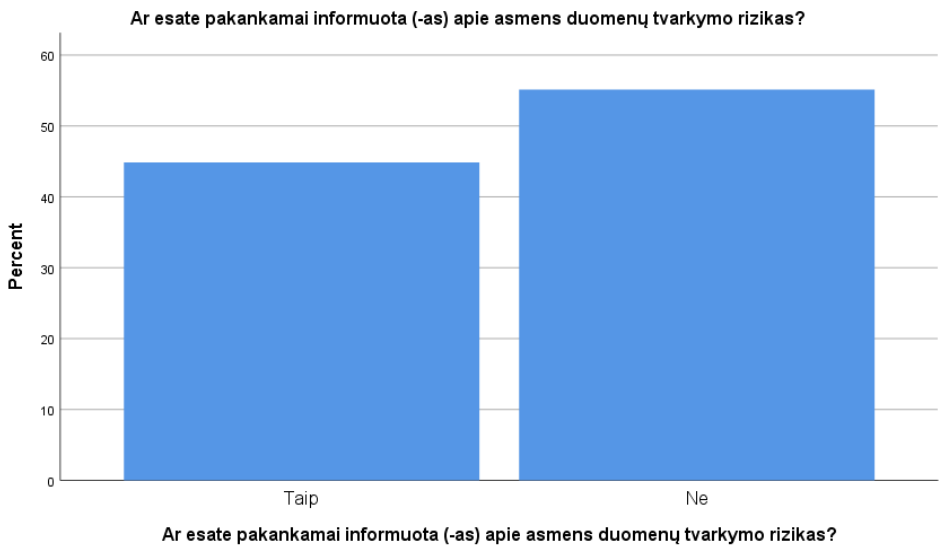
22 pav. Kaip vertinate galimų mokymų poveikį Jūsų sąmoningumui apie duomenų saugumą?

Atliekant tyrimą buvo siekiama išsiaiškinti ar įmonės skatina darbuotojus domėtis asmens duomenų apsaugos bei kibernetinio saugumo temomis, ar teikia įvairias rekomendacijas, atmintines bei kitą informaciją, susijusią su darbuotojų sąmoningumo skatinimu. 66 (61,7%) tyrimo dalyviai pažymėjo, kad jų įmonės neskatina domėtis asmens duomenų apsaugos bei kibernetinio saugumo temomis, neformuoja kibernetinio saugumo kultūros. Atsižvelgiant į tai, kad net 76,6 % tyrimo dalyvių nebuvo apmokyti kaip tvarkyti asmens duomenis, tai galima teigti, kad dalis įmonių (15,9%) nors ir nevykdo mokymų, tačiau skatina darbuotojus duomenų apsaugos praktikomis domėtis savarankiškai (žr. 23 pav.).



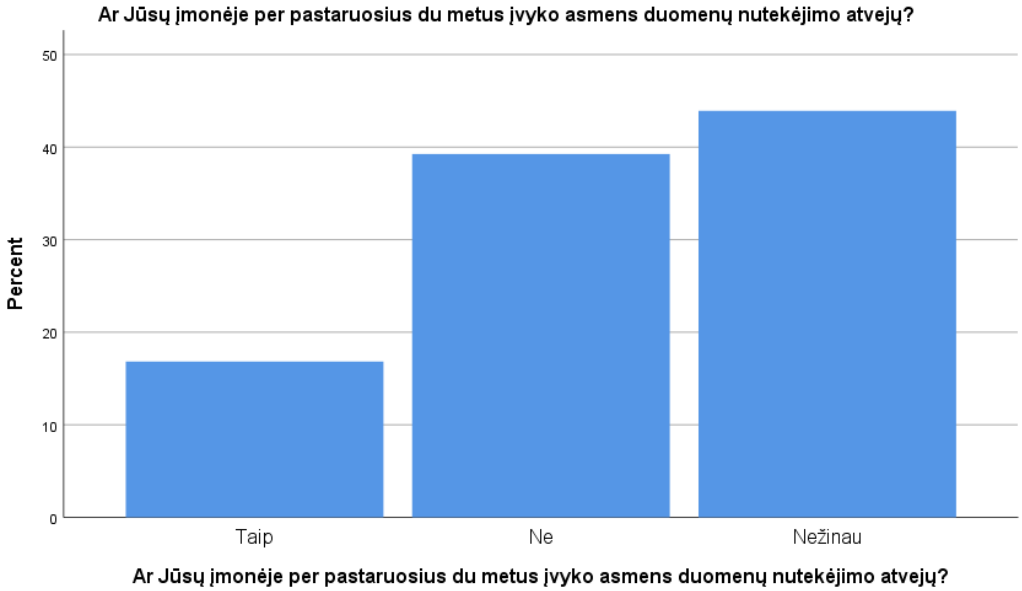
23 pav. Ar Jūsų įmonė skatina nuolatinį mokymąsi ir tobulėjimą saugumo klausimais?

Atsižvelgiant į tai, kad tyrimo dalyvių buvo klausiama ar jie dalyvavo asmens duomenų apsaugos bei kibernetinio saugumo mokymuose per pastaruosius 12 mėnesių, buvo aktualu sužinoti ar tyrimo dalyviai taip pat yra pakankamai informuoti apie duomenų tvarkymo rizikas. Pažymėtina, kad asmens duomenų tvarkymo rizikų žinojimas įgalina darbuotojus priimti tinkamas technines ir organizacines priemones, įvertinti galimas grėsmes. Daugiau nei pusė, 59 (55,1%) tyrimo dalyvių pažymėjo, kad nėra pakankamai informuoti apie duomenų tvarkymo rizikas (žr. 24 pav.). Taip pat buvo nustatyta, kad Pakruojo darbuotojai pozityviau vertina įmonės skatinimą nuolatiniam tobulėjimui saugumo klausimais. Buvo rastas statistiškai reikšmingas skirtumas (p mažesnė už 0,05) tarp grupių – Pasvalio respondentai vertino skatinimą labiau neigiamai.



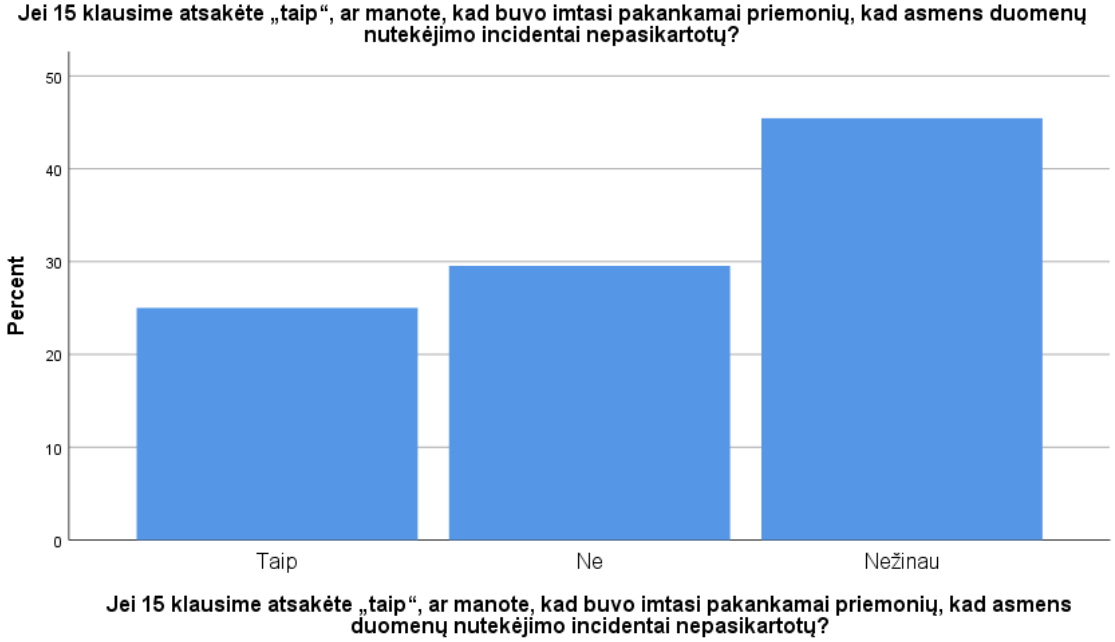
24 pav. Ar esate pakankamai informuota (-as) apie duomenų tvarkymo rizikas?

Tyrimo metu buvo klausima ar tyrimo dalyviai žino apie asmens duomenų nutekėjimo atvejus jų darbovietėse. 18 (16,8%) tyrimo dalyviai pažymėjo, kad jų įmonėse per pastaruosius du metus buvo įvykę asmens duomenų saugumo pažeidimų. 47 (43,9%) neturi žinių apie tokius atvejus (žr. 25 pav.). Ne visos įmonės informuoja darbuotojus apie įvykusius asmens duomenų saugumo pažeidimus bei duomenų nutekėjimo atvejus ir vykdo mokymus bei instruktažus kaip atsakingai ir saugiai tvarkyti asmens duomenis.



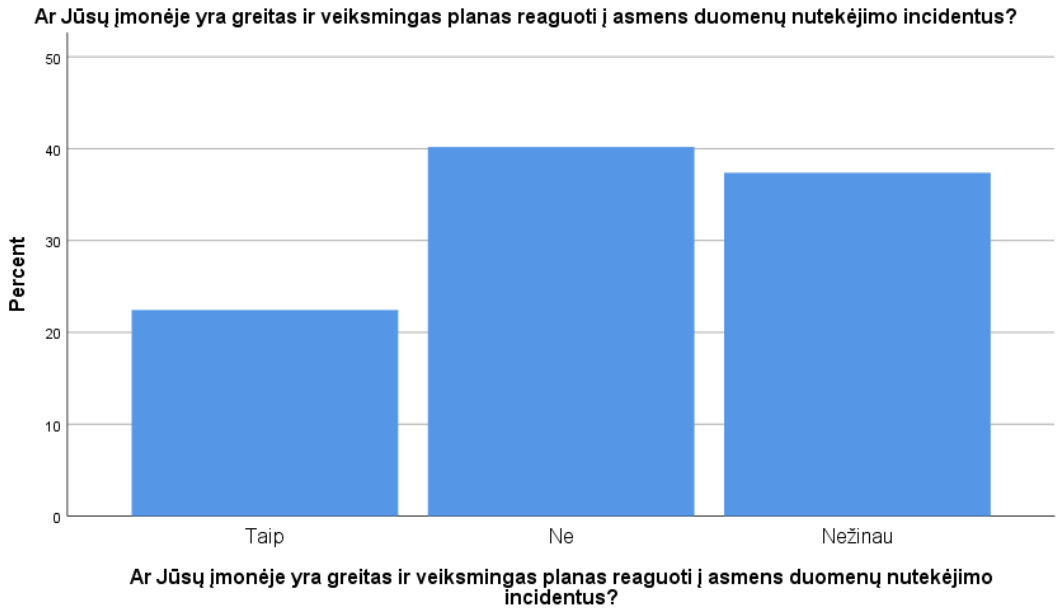
25 pav. Ar Jūsų įmonėje per pastaruosius du metus įvyko asmens duomenų nutekėjimo atvejų?

Tik ketvirtadalis (25%) tyrimo dalyvių mano, kad įvykus asmens duomenų pažeidimui ir duomenų nutekėjimui, įmonė imasi pakankamai saugumo priemonių, kad tokie incidentai nepasikartotų ateityje (žr. 26 pav.).



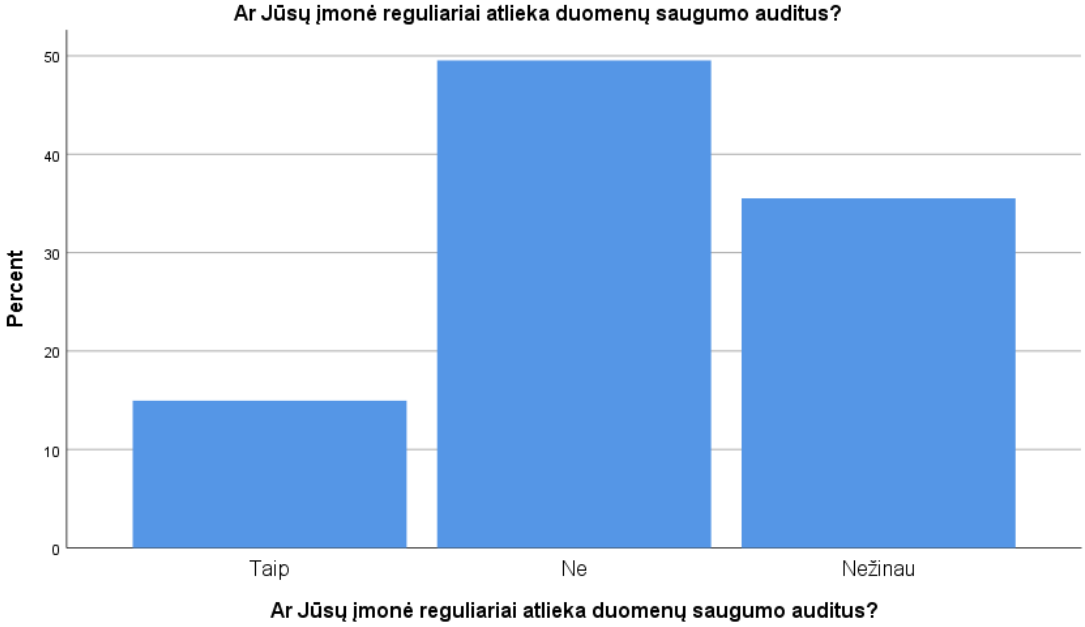
26 pav. Ar manote, kad buvo imtasi pakankamai priemonių, kad duomenų nutekėjimo incidentai nepasikartotų?

Nei viena įmonė ar organizacija negali šimtu procentu užtikrinti saugumo ir pasirengti visiems asmens duomenų nutekėjimo atvejams. Pirmiausia, piktavaliai nuolat sugalvoja vis naujus metodus, o antra, saugumo priemonės kainuoja ženklias sumas. Todėl asmens duomenų pažeidimų valdymas bei gebėjimas greitai identifikuoti bei neutralizuoti duomenų nutekėjimo incidentus tampa itin reikšmingas siekiant kuo greičiau atkurti įmonės veiklą, sumažinti galimus materialius bei reputacijos nuostolius. Siekiant išsiaiškinti ar Pasvalio bei Pakruojo įmonės yra pasirengusios asmens duomenų nutekėjimo tvarkas, planus bei procesus asmens duomenų nutekėjimo incidentams valdyti, tyrimo dalyvių buvo klausiama, ar jų įmonėje yra greitas ir veiksmingas planas reaguoti į duomenų nutekėjimo incidentus. Net 43 (40,2%) tyrimo dalyviai pažymėjo, kad jų įmonėje nėra veiksmingo plano, o 40 (37,4%) tyrimo dalyvių apie tokį planą nežino (žr. 27 pav.). Vadinasi 77,6 % tyrimo dalyvių nėra supažindinti ką daryti įvykus asmens duomenų nutekėjimo atvejui ar kitai grėsmei.



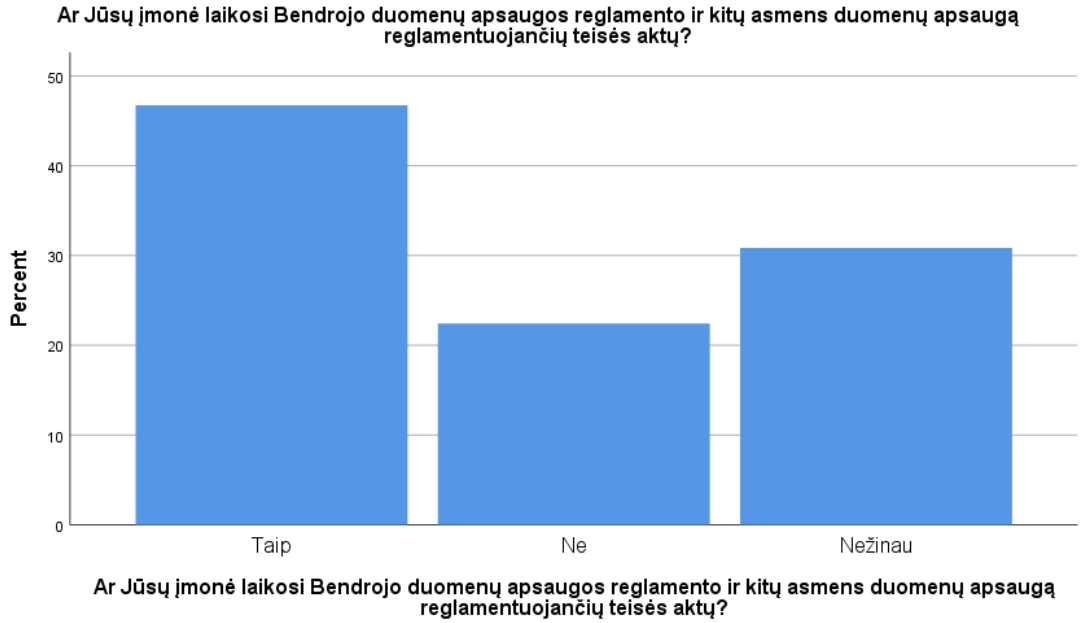
27 pav. Ar Jūsų įmonėje yra greitas ir veiksmingas planas reaguoti į duomenų nutekėjimo incidentus?

Siekiant išsiaiškinti ar įmonės nustato saugumo grėsmes bei parenka atitinkamas prevencijos priemones, tyrimo dalyvių buvo klausiama ar jų įmonė reguliariai atlieka duomenų saugumo auditus. Tik 16 (15%) tyrimo dalyvių pažymėjo, kad jų įmonė reguliariai atlieka duomenų saugumo auditus. 53 (49,5%) tyrimo dalyvių pažymėjo, kad įmonė auditų neatlieka, o 38 (35,5%) tyrimo dalyvių apie saugumo audito atlikimo faktą nežino (žr. 28 pav.). Tokį pasiskirstymą gali lemti kompetencijų bei finansinių išteklių stoka.



28 pav. Ar Jūsų įmonė reguliariai atlieka duomenų saugumo auditus?

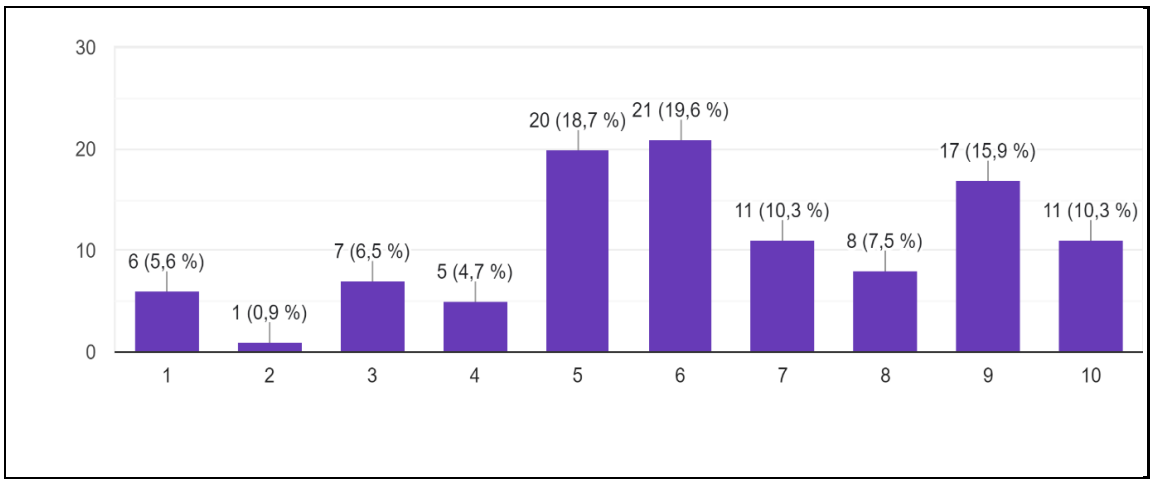
Atsižvelgiant į tai, kad darbuotojai yra įmonės dalis, aktualu išsiaiškinti kaip jie vertina ar jų įmonė laikosi Bendrojo duomenų apsaugos reglamento bei kitų asmens duomenų apsaugą reglamentuojančių teisės aktų. Pažymėtina, kad patys darbuotojai veikia vadovaudamiesi įmonės saugumo politika, tad gali įvertinti ar įmonė laikosi teisės aktų bei rekomendacijų, susijusių su asmens duomenų tvarkymu. 50 (46,7%) respondentų teigia, kad jų nuomone, įmonė laikosi Bendrojo duomenų apsaugos reglamento bei kitų asmens duomenų apsaugą reglamentuojančių teisės aktų. Tuo tarpu 24 (22,4%) respondentų mano, kad jų įmonė Bendrojo duomenų apsaugos reglamento bei kitų asmens duomenų apsaugą reglamentuojančių teisės aktų nesilaiko, o 33 (30,8%) nėra užtikrinti ir nežino (žr. 29 pav.). Kadangi patys darbuotojai įmonėse tvarko asmens duomenis, tad pažymėję, kad nežino apie asmens duomenų apsaugą reglamentuojančių teisės aktų laikymąsi, nėra supažindinti su pagrindiniais asmens duomenų apsaugos reikalavimais, principais, nebuvo dalyvavę mokymuose ir nėra tikri dėl įmonės veiklos atitikties.



29 pav. Ar Jūsų įmonė laikosi Bendrojo duomenų apsaugos reglamento ir kitų asmens duomenų apsaugą reglamentuojančių teisės aktų?

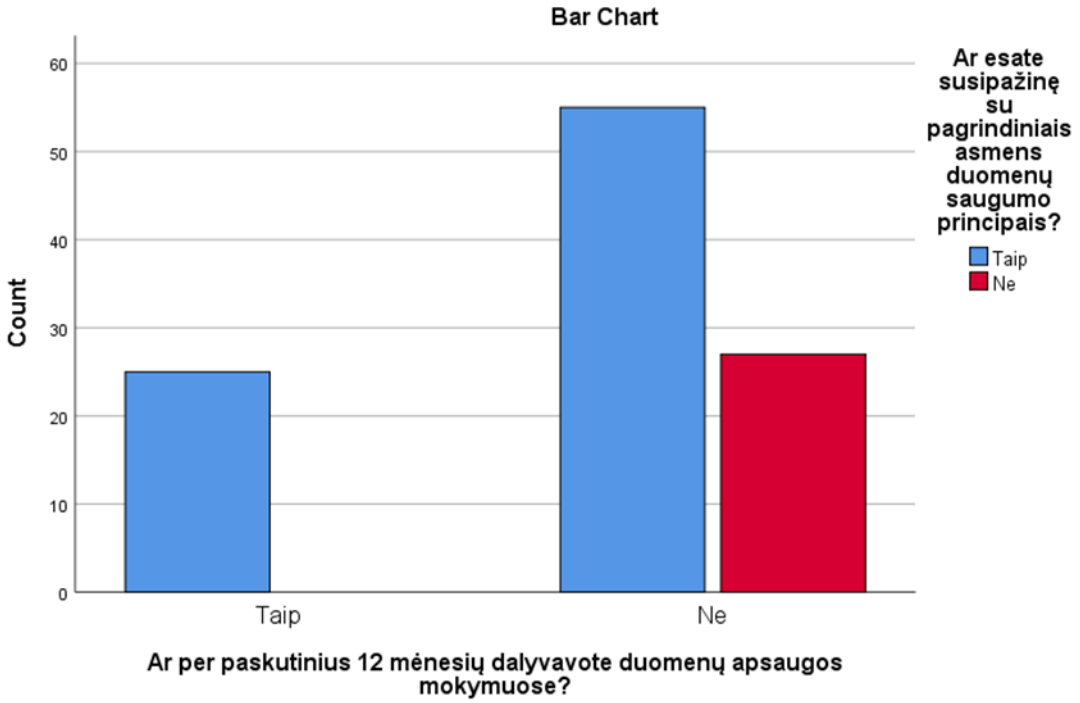
Remiantis tyrimo duomenimis, 21 (19,6%) respondentų įmonės saugumo politikos aiškumą ir prieinamumą vertina 6 balais, 20 (18,7%) vertina 5 balais ir 17 (15,9 %) vertina 9 balais (žr. 30 pav.). Vadinasi didžioji dauguma respondentų įmonės saugumo politikos aiškumą ir prieinamumą vertina vidutiniškai 6 -7 balais. Saugumo politikos aiškumas yra susijęs su tuo, kaip darbuotojui paprasta ir suprantama kalba yra pateikiamos taisyklės, procedūros, praktiškai

paaiškinami saugumo veiksmai. Prieinamumas siejamas su darbuotojo galimybe bet kuriuo jam patogiu metu dar kartą susipažinti su lokaliniais teisės aktais ar gauti patarimą bei rekomendaciją kaip praktiškai tvarkyti asmens duomenis.



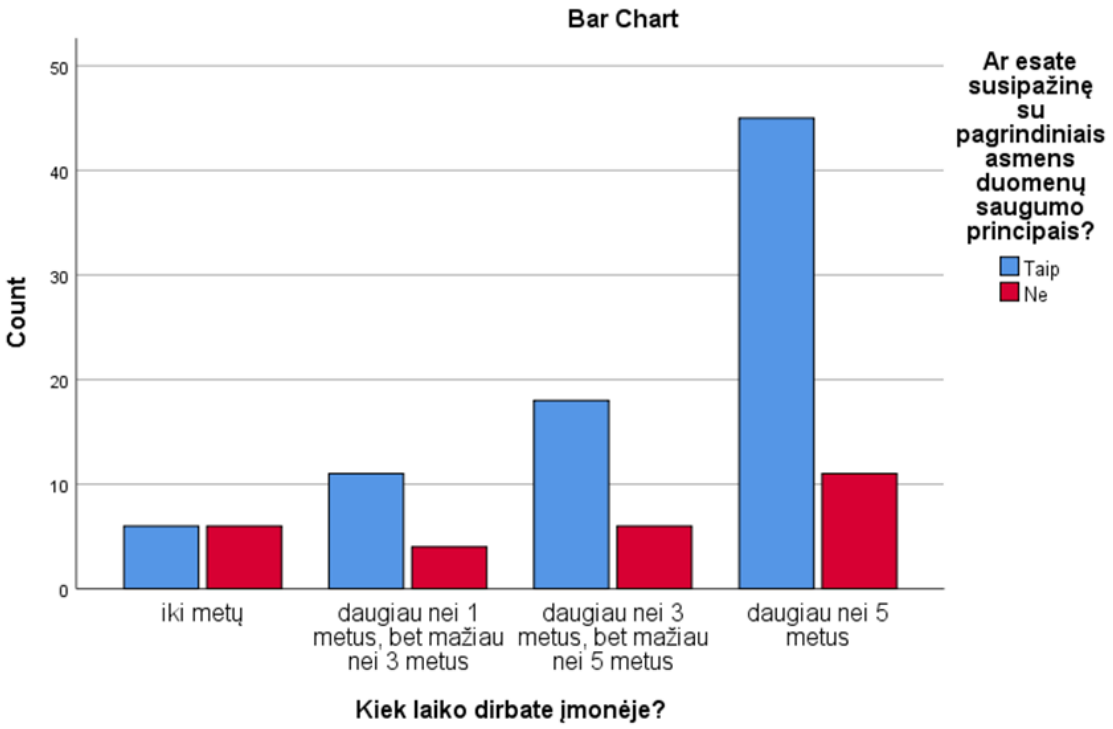
30 pav. Kaip vertinate Jūsų įmonės saugumo politikos aiškumą ir prieinamumą?

Pažymėtina, kad buvo rastas statistiškai reikšmingas skirtumas tarp susipažinimo su asmens duomenų saugumo principais ir mokymų vedimu (p reiškmė mažesnė už 0,05). Visi respondentai, kurie buvo nesusipažinę su šiais principais nebuvo dalyvavę mokymuose (žr. 31 pav.).



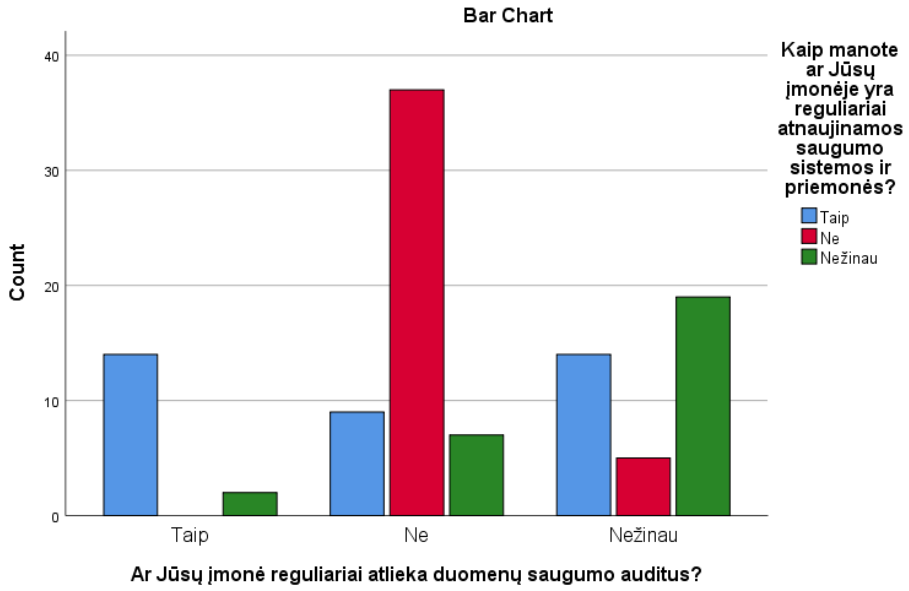
31 pav. Ar yra statistiškai reikšmingas ryšys tarp dalyvavimo duomenų apsaugos mokymuose bei susipažinimo su pagrindiniais asmens duomenų saugumo principais?

Siekiant nustatyti ar darbo stažas koreliuoja tarp susipažinimo su pagrindiniais asmens duomenų saugumo principais, buvo atlikti statistiniai skaičiavimai, kurių metu nustatyta, kad statistiškai reikšmingas skirtumas tarp kintamųjų rastas nebuvo (p reikšmė didesnė už 0,05). Darbo stažas neturi įtakos darbuotojų pagrindinių asmens duomenų saugumo principų žinomumui (žr. 32 pav.).



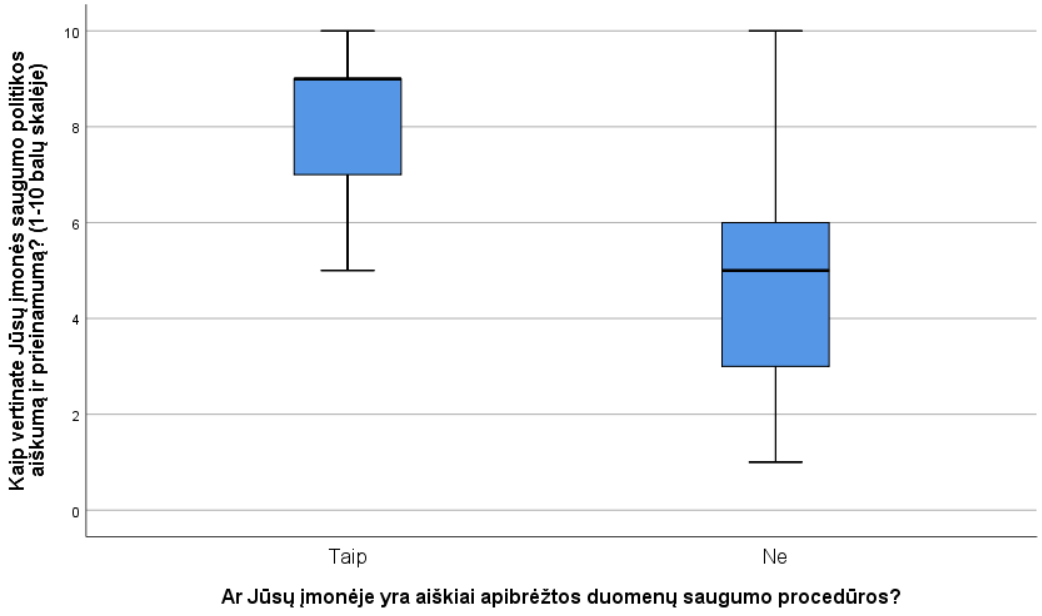
32 pav. Ar yra statistiškai reikšmingas ryšys tarp darbo stažo bei susipažinimo su pagrindiniais asmens duomenų saugumo principais?

Buvo rastas statistiškai reikšmingas skirtumas tarp kintamųjų (p reikšmė mažesnė už 0,05). Svarbu paminėti, kad jeigu įmonėje nebuvo reguliariai atliekamas duomenų saugumo auditas, tai dauguma respondentų manė, jog saugumo sistemų atnaujinimas taip pat nevyksta. Svarbu paminėti, jog visi respondentai, kurių įmonėje reguliariai atliekamas duomenų saugumo auditas nepasirinko atsakymo „Ne“ sistemų atnaujinimo klausime (maža dalis nežinojo, dauguma atsakė „Taip“) (žr. pav. 33).



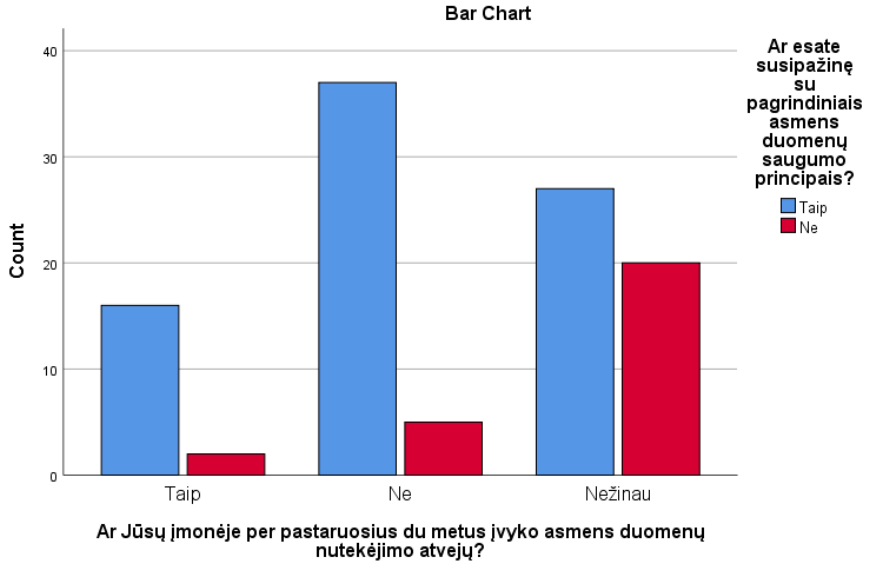
33 pav. Ar yra statistiškai reikšmingas ryšys įmonės reguliariai atliekamų saugumo auditų bei įmonėje reguliariai atliekamų saugumo sistemų ir priemonių?

Siekiant nustatyti darbuotojų koreliaciją tarp įmonės saugumo politikos aiškumo ir prieinamumo bei aiškiai apibrėžtų duomenų saugumo procedūrų, buvo rastas statistiškai reikšmingas skirtumas tarp kintamųjų (p reikšmė mažesnė už 0.05). Galima pastebėti tendenciją, kad respondentai, kurie turėjo aiškiai apibrėžtas duomenų saugumo procedūras vertino įmonės saugumo politikos aiškumą ir prieinamumą pozityviau, nei tie kurie tokio apibrėžtumo neturėjo (žr. 34 pav.).



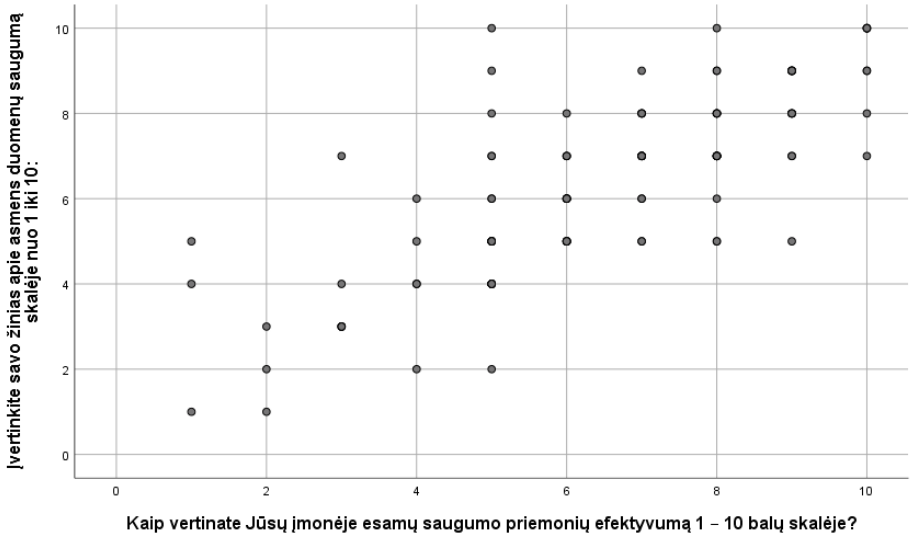
34 pav. Ar įmonės saugumo politikos aiškumas ir prieinamumas koreliuoja su aiškiai apibrėžtomis duomenų saugumo procedūromis?

Atliekant statistinius skaičiavimus nustatant ar respondentai, kurie yra labiau susipažinę su asmens duomenų saugumo principais yra linkę daugiau žinoti apie duomenų nutekėjimo situaciją įmonėje, buvo rastas statistiškai reikšmingas skirtumas (p mažesnė už 0,05) tarp grupių. Respondentai, kurie buvo susipažinę su asmens duomenų saugumo principais buvo linkę turėti daugiau informacijos apie asmens duomenų nutekėjimo atvejus (žr. 35 pav.).



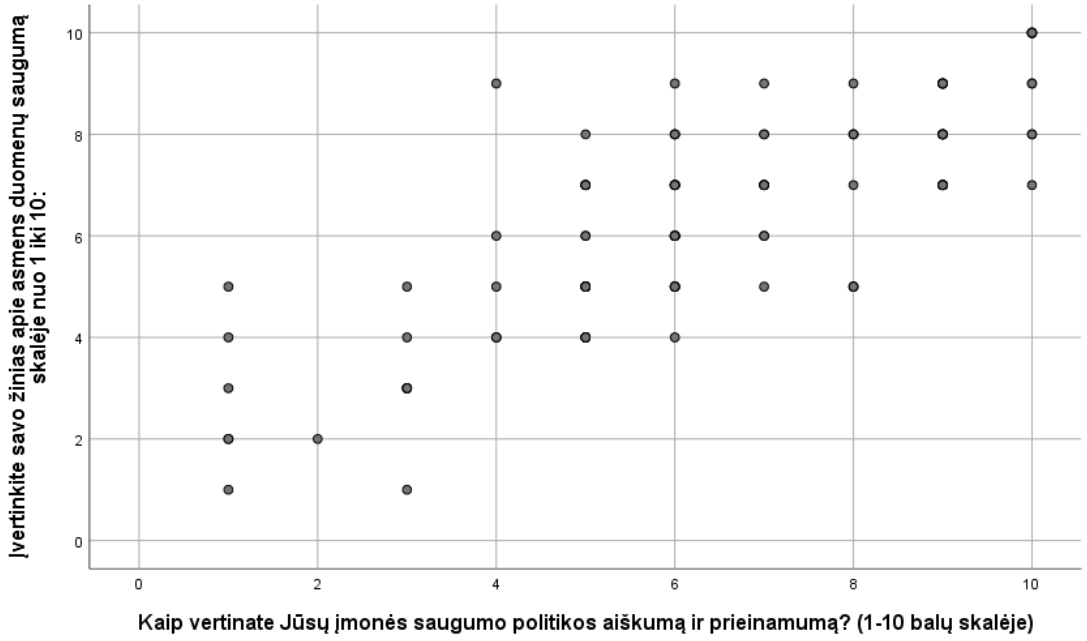
35 pav. Ar respondentai susipažinę su pagrindiniais asmens duomenų saugumo principais turi daugiau informacijos apie įmonės asmens duomenų nutekėjimo atvejus?

Siekiant nustatyti ar respondentai, kurie pozityviau vertina įmonės saugumo priemonių efektyvumą yra linkę labiau vertinti savo žinias apie asmens duomenų saugumą, buvo atlikti statistiniai skaičiavimai, kurių metu rastas statistiškai reikšmingas pozityvus stiprus ryšys tarp šių kintamųjų, todėl galime teigti, jog didėjant vienam vertinimui didės ir kitas (žr. 36 pav.).



36 pav. Ar respondentai pozityviau vertinantys įmonės saugumo priemonių efektyvumą yra linkę labiau vertinti savo žinias apie asmens duomenų saugumą?

Siekiant nustatyti ar respondentai, kurie pozityviau vertina įmonės saugumo politikos aiškumą ir prieinamumą yra linkę labiau vertinti savo žinias apie asmens duomenų saugumą, buvo atlikti statistiniai skaičiavimai, kurių metu buvo rastas statistiškai reikšmingas pozityvus stiprus ryšys tarp šių kintamųjų, todėl galime teigti, jog didėjant vienam vertinimui didės ir kitas (žr. 37 pav.).



37 pav. Ar respondentai pozityviau vertinantys įmonės saugumo politikos aiškumą ir prieinamumą yra linkę labiau vertinti savo žinias apie asmens duomenų saugumą?

Apibendrinant statistinius skaičiavimus, galima teikti, kad egzistuoja pozityvi įtaka tarp mokymų ir geresnių vertinimų, bei papildomų žinių.

IŠVADOS

1. Įmonių skaitmeninė pažanga kelia pavojų, galimybės kelia riziką, todėl pavojų ir rizikos valdymas tampa neišvengiama verslo praktikos dalimi, nepriklausančia nuo jos dydžio, veiklos srities ar naudojamų kibernetinio saugumo priemonių. Informacinių technologijų plėtra nuolat keičia nusistovėjusią praktiką, todėl net mažos ir vidutinės privataus sektoriaus įmonės tampa svarbia nacionalinio kibernetinio saugumo grandies dalimi.
2. Asmens duomenų nutekėjimą gali sukelti tyčinis ir išorinis informacijos pažeidimas arba netyčia darbuotojų ir partnerių atskleista jautri informacija. Išpuolių motyvai yra įvairūs, įskaitant įmonių šnipinėjimą, siekiant pakenkti darbdaviui ar reikalavimus sumokėti išpirką. Atsitiktiniai asmens duomenų nutekėjimo atvejai dažniausiai atsiranda dėl netinkamų prevencinių priemonių naudojimo ir saugumo politikos taikymo bei darbuotojų ir tiekėjų grandinės kontrolės neužtikrinimo.
3. Duomenų saugumas yra ne vienkartinis projektas, o nuolatinis procesas, todėl mažos ir vidutinės įmonės susiduria su dideliais iššūkiais užtikrinant duomenų saugumą. Pagrindiniai mažų ir vidutinių įmonių iššūkiai yra riboti finansiniai ištekliai saugumo priemonėms įsigyti bei specialistų trūkumas, todėl mažos ir vidutinės įmonės įgyvendina tik pagrindines saugumo priemones, tokias kaip antivirusinė programinė įranga, ugniasienės ir slaptažodžių politika. Pažangesnės priemonės neįgyvendinamos, neužtikrinamas įmonės informacinės saugos brandos lygis. Be tinkamų darbuotojų mokymų, nuolatinės stebėsenos, auditų, rizikos valdymo ir reagavimo į incidentus planų, mažoms ir vidutinėms įmonėms gali kilti didesnė asmens duomenų nutekėjimo atvejų bei su tuo susijusių finansinių nuostolių bei reputacijos praradimo rizika.
4. Dėl darbuotojų netyčia nutekintos jautrios informacijos Lietuvoje vyrauja konfidencialumo pažeidimai. Darbuotojams trūksta tinkamų mokymų ir bei informacijos apie įmonės saugumo politikos pokyčius. Net ir taikant pačias sudėtingiausias kibernetinio saugumo priemones, užtenka vieno neatsargaus darbuotojo, kad įvyktų konfidencialumo pažeidimas. Asmens duomenų apsaugos bei kibernetinio saugumo higienos mokymai padėtų darbuotojams neatsilikti nuo naujausių duomenų apsaugos praktikos reikalavimų. Informuodamos darbuotojus apie naujausias tendencijas ir geriausią praktiką, kurdamos saugumo kultūrą, nustatydamos galimas rizikas ir pažeidžiamumą bei gerindamos darbuotojų moralę ir pasitenkinimą darbu, mažos ir vidutinės įmonės galėtų užtikrinti, kad jų valdomi bei tvarkomi asmens duomenys išliktų saugūs bei apsaugoti nuo neteisėtos prieigos ar atskleidimo.

REKOMENDACIJOS

1. Valstybinei duomenų apsaugos inspekcijai rekomenduojama įvesti mažų ir vidutinio dydžio įmonių prevencinės kontrolės mechanizmus, siekiant įvertinti kaip mažo ir vidutinio dydžio įmonės įgyvendina kibernetinio saugumo priemones ir užtikrina asmens duomenų apsaugą. Mažų ir vidutinių įmonių teisinis reguliavimas bei jo įgyvendinimo priežiūra užtikrintų aukštą Lietuvos mažų ir vidutinio dydžio įmonių saugumo brandos lygį.
2. Sisteminis bei savalaikis asmens duomenų apsaugos bei kibernetinės higienos mokymų prieinamumas ne tik viešojo sektoriaus, bet ir privataus sektoriaus darbuotojams formuotų kibernetinę kultūrą visoje Lietuvoje, todėl rekomenduojama valstybiniu lygmeniu sukurti visiems dirbantiems asmenims privalomas, nemokamas mokymų programas, suskirstytas pagal darbo sritį bei kibernetinio saugumo taikymo patirtį.
3. Valstybinei duomenų apsaugos inspekcijai bei Nacionaliniam kibernetinio saugumo centrui rekomenduojama parengti privataus sektoriaus įmonių vadovų mokymų programą bei privalomą kompetencijų patikrinimo sistemą.
4. Valstybinei duomenų apsaugos inspekcijai bei Nacionaliniam kibernetinio saugumo centrui rekomenduojama sudaryti aukštųjų mokymo institucijų, su kibernetiniu saugumu dirbančių specialistų bei tikslinių asociacijų darbo grupę kuriant kibernetinio saugumo technologijas bei inovacijas bei jas pritaikant visuomenės poreikiams, naujų saugumo programų kūrimui.
5. Rekomenduojama valstybiniu lygmeniu sukurti privataus sektoriaus įmonėms skirtą programą, kurioje mažo ir vidutinio dydžio įmonės galėtų dalintis informacija apie patiriamas atakas, pastebėtas saugumo spragas, gerąsias praktikas ir kt., atsižvelgiant į įmonės veiklos sektorių. Rekomenduojama skatinti įmones dalintis informacija neatskleidžiant įmonės pavadinimo ir išlaikant komercinių paslapčių bei konfidencialumo principus.
6. Valstybinei duomenų apsaugos inspekcijai bei Nacionaliniam kibernetinio saugumo centrui rekomenduojama organizuoti praktines mažų ir vidutinio dydžio įmonių darbuotojams skirtas pratybas, kuriuose aiškia ir suprantama kalba būtų paaiškinami pagrindiniai asmens duomenų nutekėjimo būdai, metodai bei pateikiami praktiniai pavydžiai.
7. Valstybiniu lygmeniu rekomenduojama stiprinti viešojo ir privataus sektoriaus bendradarbiavimą užtikrinant kibernetinį saugumą. Vykdyti bendrus renginius, skatinti dalintis geraja kibernetinio saugumo praktika.

8. Įmonėms rekomenduojama stiprinti kibernetinio saugumo brandos lygį pradedant nuo aukščiausių vadovų, suprantant, kad kibernetinis saugumas nėra tik informacinių technologijų specialisto darbo dalis, o visos įmonės rūpestis.
9. Įmonėms rekomenduojama atlikti rizikos vertinimą bei nustatyti atitinkamas kibernetinio saugumo priemones, užtikrinančias bent priimtiną saugumo riziką. Nustatytoms priemonėms skirti ekonomiškai pagrįstą subalansuotą finansavimą.
10. Įmonėms rekomenduojama plėtoti darbuotojų kibernetinio saugumo kultūros formavimą. Aukštas darbuotojų kibernetinio saugumo kultūros lygis įmonėje lemia darbuotojų pasitikėjimą darbdaviu, savo vykdomos veiklos teisėtumu, mažinamas nerimas dėl galimų asmens duomenų tvarkymo klaidų ir su tuo susijusių duomenų nutekėjimo atvejų. Skatinti darbuotojų asmeninį tobulėjimą kibernetinio saugumo srityje, vykdyti įvairius konkursus, skirti premijas, kitas motyvacines priemones už darbuotojų iniciatyvas asmens duomenų apsaugos bei kibernetinio saugumo srityje.
11. Įmonėms rekomenduojama reguliariai apmokyti darbuotojus pagal nuolat atnaujinamas asmens duomenų apsaugos bei kibernetinės higienos programas, patikrinti darbuotojų įgytas kompetencijas, vykdyti netikėtas įvairaus tipo kibernetinio saugumo atakas, patikrinti ir išsigryninti asmens duomenų saugumo pažeidimų valdymo tvarkos aprašų bei kitų saugos dokumentų poveikį bei atitiktį sumodeliuotose kibernetinių incidentų situacijose, išbandyti darbuotojų reakcijos laiką, gebėjimą atpažinti grėsmes.
12. Rekomenduojama įmonėms jungtis į kibernetinio saugumo srities asociacijas, skirti atsakingus darbuotojus ir aktyviai dalyvauti asociacijų veiklose, siekiant atsakingos kibernetinio saugumo politikos formavimo, patirties įgyvendinant kibernetinio saugumo reikalavimus dalinimosi, mokinimosi iš kitų įmonių klaidų bei gerosios patirties pavyzdžių.

LITERATŪRA

1. Neigel A. R., Claypoole V.L., Waldfogle G. E., Acharya S., Hancock G. M. *Holistic cyber hygiene education: Accounting for the human factors*. (2020). Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S0167404820300183;
2. Uddin M. R.. *Developing a data breach protection capability framework in retailing*. (2024). Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S0925527324000598;
3. Swani K., Labrecque L., Markos E.. *Are B2B data breaches concerning? Consequences of buyer's or firm's data loss on buyer and supplier related outcomes*. (2024). P. 43-61. Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S0019850124000452;
4. Zhou F., Huang J.. *Cybersecurity data breaches and internal control*. (2024). Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S1057521924001066;
5. Barati M., Yankson B., *Predicting the Occurrence of a Data Breach*. (2022). Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S2667096822000714;
6. Poelhman N., Caramancion K. M. *The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review.* (2021). Prieiga per internetą: https://link.springer.com/chapter/10.1007/978-3-030-71017-0_27;
7. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.
8. Lietuvos Respublikos Kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428.
9. Lietuvos bankas. *Apklausa: rusijos karo prieš Ukrainą metu padaugėjo kibernetinių atakų ir prieš Lietuvos finansų įstaigas*. Prieiga per internetą: https://www.lb.lt/lt/naujienos/apklausa-rusijos-karo-pries-ukraina-metu-padaugejo-kibernetiniu-ataku-ir-pries-lietuvos-finansu-istaigas;
10. Nacionalinis kibernetinio saugumo centras. *Svarbiausia Lietuvos kibernetinio saugumo būklės statistika ir tendencijos 2021 m. – 2022 m. I ketv*. Prieiga per internetą: https://kam.lt/wp-content/uploads/2022/05/Kibernetinio-saugumo-santrauka-1.pdf.;
11. Darius Štitilis. *Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos.* (2013). Prieiga per internetą:

https://repository.mruni.eu/bitstream/handle/007/10657/489-843-2-PB.pdf?sequence=1&isAllowed=y>.

12. Valstybinė duomenų apsaugos inspekcija. *2021 m. pranešimų apie asmens duomenų saugumo pažeidimus apžvalga.* (2021). Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/2021-m-pranesimu-apie-asmens-duomenu-saugumo-pazeidimus-apzvalga;
13. Valstybinė duomenų apsaugos inspekcija. *2022 m. I pusmečio pranešimų apie asmens duomenų saugumo pažeidimus apžvalga*. (2022). Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/2022-m-i-pusmecio-pranesimu-apie-asmens-duomenu-saugumo-pazeidimus-apzvalga;
14. Valstybinė duomenų apsaugos inspekcija. *Veiklos ataskaita.* (2023). Prieiga per internetą: https://vdai.lrv.lt/media/viesa/saugykla/2024/3/nLYMpcYmDDQ.pdf.
15. Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*. 2020-06-18 3 versija. Prieiga per internetą: VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf;
16. Kardelis K. (2016) *Mokslinių tyrimų metodologija ir metodai.* Mokslo ir enciklopedijų leidybos centras;
17. Falch, M., Olesen, H., Skouby, K. E., Tadayoni, R., & Williams, I. (2022). *Cybersecurity in SMEs in the Baltic Sea Region. In ITS 31th European Conference 2022 International Telecommunications Society*. Prieiga per internetą: https://www.econstor.eu/bitstream/10419/265624/1/Falch-et-al.pdf;
18. Tam, T., Rao, A., & Hall, J. (2021, 109, 102385.). *The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security*. Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S0167404821002091;
19. ENISA *Threat landscape*. (2020). Prieiga per internetą: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape-2020-top-15-threats;
20. ENISA *Thread landscape*. (2021). Prieiga per internetą: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021;

21. Mykolo Romerio universitetas. Publikacija. Prieiga per internetą: https://www.mruni.eu/news/ivyko-tarptautinio-projekto-tebelsi-pirmas-partneriu-susitikimas;
22. Eurostat. *22 % ES įmonių patyrė IRT saugumo incidentų.* (2023). Prieiga per internetą: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1;
23. Jastiuginas. S (2012). *Integralus informacijos saugumo valdymo modelis*. P. 8 DOI: 10.15388/Im.2012.0.1063. Prieiga per internetą https://talpykla.elaba.lt/elabafedora/objects/elaba:4683733/datastreams/MAIN/content
24. 1996 m. birželio 11 d. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas Nr. Nr. I-1374 (Suvestinė redakcija nuo 2024-01-01);
25. 2018 m. rugpjūčio 29 d. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas „*Dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo*“ Nr. Nr. 1T-82(1.12.E) (2018);
26. Valstybinė duomenų apsaugos inspekcija. „*Asmens duomenų saugumo pažeidimai Lietuvoje 2023 m. I pusmetį.“* (2023). Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2023-m-i-pusmeti/.;
27. Lietuvos Respublikos smulkiojo ir vidutinio verslo plėtros įstatymo Nr. VIII-935 pakeitimo įstatymas. 2017 m. sausio 12 d. Nr. XIII-192;
28. Didžiosios Britanijos duomenų ir informacijos apsaugos institucija (ICO). Prieiga per internetą: https://ico.org.uk/for-organisations/advice-for-small-organisations/frequently-asked-questions/getting-started-with-data-protection/;
29. Europos komisija. *Kas yra asmens duomenys?* Prieiga per internetą: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_lt;
30. 29 straipsnio duomenų apsaugos darbo grupė. *Nuomonė 4/2007 dėl asmens duomenų sąvokos* [interaktyvus]. (2007). Prieiga per internetą: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_lt.pdf;
31. Nacionalinis kibernetinio saugumo centras. *Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas.* (2020). Prieiga per internetą: https://www.nksc.lt/doc/Kibernetinio_saugumo_vadovas_verslui_2020.pdf;
32. 29 straipsnio darbo grupė. *Duomenų apsaugos pareigūnų gairės*. (2016). Prieiga per internetą: https://old.gamta.lt/files/GAires%20wp243rev01_lt.pdf;

33. Valstybinė duomenų apsaugos inspekcija. *Valstybinės duomenų apsaugos inspekcijos duomenų apsaugos pareigūnų tikrinimo apibendrinimas.* (2023). Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/apibendrinti-duomenu-apsaugos-pareigunu-veiklos-patikrinimu-rezultatai/;
34. CNIL. *Prancūzijos praktinis duomenų apsaugos pareigūnų gidas (angl. CNIL Practical Guide GDPR for Data protection officers).* Prieiga per internetą: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf;
35. Romansky R.P., Noninska I. S. *Challenges of the digital age for privacy and personal data protection*. Prieiga per internetą: https://www.aimspress.com/article/doi/10.3934/mbe.2020286;
36. International Conference of Data Protection & Privacy Commissioners (ICDPPC). *Resolution to address the role of human error in personal data breaches. 41st International Conference of Data Protection and Privacy Commissioners*. (2019). Prieiga per internetą: https://edps.europa.eu/sites/edp/files/publication/aoic-resolution-final adopted_en.pdf;
37. Stasitytė S. Aleksienė L. *Įmonės veiklos rizikos vertinimas ir valdymas mažose ir vidutinėse įmonėse*. (2015). Prieiga per internetą: https://etalpykla.lituanistika.lt/object/LT-LDB-0001:J.04~2015~1463321727750/J.04~2015~1463321727750.pdf;
38. Civilka M., Šlapimaitė L. *Asmens duomenų samprata elektroninėje erdvėje*. (2015). Prieiga per internetą: https://www.zurnalai.vu.lt/teise/article/view/8761/7647;
39. Julius Zaleskis. B*endrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Monografija (2019);
40. Štitilis, D. (2011). *Elektroniniai nusikaltimai*. Metodinė priemonė. Vilnius: Mykolo Romerio universitetas;
41. Gaižauskienė I., Mikėnė S. (2014). *Socialinių tyrimų metodai: apklausa*. Vadovėlis;
42. Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. (2006). *Teisės informatika ir informatikos teisė*. Vadovėlis. Vilnius: Mykolo Romerio universitetas;
43. Valstybinė duomenų apsaugos inspekcija. *2020 metų asmens duomenų apsaugos priežiūros Lietuvoje apžvalga*. (2020). Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/2020%20m_%20asmens%20duomenu%20apsaugos%20Lietuvoje%20apzvalga.pdf. (p.40);

44. CMS. *Law, tax, future*. Prieiga per internetą: https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/industry-and-commerce;
45. Valstybinė duomenų apsaugos inspekcija. *Valstybinė duomenų apsaugos inspekcija, atlikusi tyrimą, priėmė sprendimą dėl neužtikrinto tinkamo asmens duomenų konfidencialumo, vientisumo, prieinamumo ir atsparumo bei pažeisto duomenų saugojimo trukmės principo*. (2023). Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Apibendrinimas%20d%C4%97l%20saugumo%20priemoniu%20neuztikrinimo%20ir%20terminu%202023-04-20.pdf;
46. Valstybinė duomenų apsaugos inspekcija. A*pklausa. Ką galvoja Lietuvos gyventojai?* (2024). Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-apsauga-ka-galvoja-lietuvos-gyventojai/;
47. Valstybinė duomenų apsaugos inspekcija. *Asmens duomenų apsaugos pažeidimai Lietuvoje 2023 m. I pusmetį*. Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2023-m-i-pusmeti/;
48. Bilevičienė, T., Jonušauskas, S. (2011). *Statistinių metodų taikymas rinkos tyrimuose*. Vilnius: Mykolo Riomerio universitetas;
49. Valstybės duomenų agentūra. *Statistikos departamento statistinių rodiklių analizė*. Prieiga per internetą: https://osp.stat.gov.lt/statistiniu-rodikliu-analize?hash=acd06c32-c602-4cbf-b4ec-386e5e5a1d47#/;
50. Valstybės duomenų agentūra. *Statistikos departamento statistinių rodiklių analizė*. Prieiga per internetą:https://osp.stat.gov.lt/statistiniu-rodikliu-analize?hash=c98b9b00-4b05-48d6-aeb4-d1ede120a8a2#/;
51. Nacionalinis kibernetinio saugumo centras. *KSIT*. Prieiga per internetą: https://www.nksc.lt/ksit;
52. Nacionalinis kibernetinio saugumo centras. *Nauja NKSC nemokama kibernetinių mokymų platforma padės organizacijoms sustiprinti savo kibernetinį atsparumą*. Prieiga per internetą: https://www.nksc.lt/naujienos/nauja_nksc_nemokama_kibernetiniu_mokymu_platforma_.html;.
53. Cheng L., Liu F., Yao D. (2017). *Enterprise data breach: causes, challenges, prevention, and future directions*. Prieiga per internetą: https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1211;

54. Verslo žinios. *Kibernetinių atakų skaičius auga sparčiai: lemia ir geopolitika, ir nesutvarkytas IT ūkis*. (2023). Prieiga per internetą: https://www.vz.lt/inovacijos/technologijos/2024/01/16/kibernetiniu-ataku-skaicius-auga-sparciai-lemia-ir-geopolitika-ir-nesutvarkytas-it-ukis;
55. Visuotinė lietuvių enciklopedija. Straipsnis. *Privatus sektorius*. Prieiga per internetą: https://www.vle.lt/straipsnis/privatus-sektorius/;
56. Visuotinė lietuvių enciklopedija. Straipsnis. *Prevencija*. Prieiga per internetą: https://www.vle.lt/straipsnis/prevencija/;
57. Toldinas J, Venčkauskas A., Damaševičius R., Grigaliūnas Š., Morkevičius N., Baranauskas E. *A novel approach for network intrusion detection using multistage deep learning image recognition* // Electronics. Basel : MDPI. ISSN 2079-9292. (2021), vol. 10, iss. 15, art. no. 1854, p. 1-21. DOI: 10.3390/electronics10151854. Prieiga per internetą: https://www.mdpi.com/2079-9292/10/15/1854;
58. Damaševičius R., Venčkauskas A., Toldinas J. Grigaliūnas Š.. *Ensemble-based classification using neural networks and machine learning models for windows pe malware detection.*// Electronics. Basel : MDPI. ISSN 2079-9292. 2021, vol. 10, iss.4, art. no. 485, p. 1-23. DOI: 10.3390/electronics10040485. Prieiga per internetą: https://www.mdpi.com/2079-9292/10/4/485.
59. Kuklytė J., Ūsas A.. *Informacinės visuomenės iššūkiai: kokios yra kibernetinių nusikaltimų formos?* Mokslinių straipsnių rinkinys. Visuomenės saugumas ir viešoji tvarka. 2021. ISSN 2029-1701, p. 184-194. Prieiga per interentą: file:///C:/Users/saugo/Downloads/%23%23common.file.namingPattern%23%23%20(7).pdf.
60. Cartwright A., Cartwright E., Edunc E. S. *Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies*. (2024). Computers & Security. Volume 131, August 2023, 103288. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S0167404823001980?via%3Dihub.
61. Alahmaris A., Duncanas B. *Kibernetinio saugumo rizikos valdymas mažose ir vidutinėse įmonėse: sisteminga naujausių įrodymų apžvalga*. (2020). Prieiga per internetą: https://ieeexplore.ieee.org/document/9139638;
62. Maximiano A., Pinto G. *Informacijos saugumas ir kibernetinio saugumo valdymas: atvejo tyrimas su MVĮ Portugalijoje*. (2021). Prieiga per internetą: https://www.mdpi.com/2624-800X/1/2/12;

63. Chang L., Coppel N. *Kibernetinio saugumo supratimo ugdymas besivystančioje šalyje: pamokos iš Mianmaro*. (2020). Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S0167404820302352;
64. Arranz A., Arroyabe D.. *Kibernetinio saugumo pajėgumai ir kibernetinės atakos kaip investicijų į kibernetinio saugumo sistemas varikliai: JK 2018 ir 2019 m*. (2023). Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S0167404822003467;
65. Cartwright A. Cartwright E., Edun E. S. *Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies*. Computers and Security 131 (2023) 103288. P.2. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S0167404823001980?via%3Dihub;
66. Pawar Sh., Palivela H, Ph.D. *LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)*. (2023). P. 3. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S2667096822000234?via%3Dihub;
67. ICDPPC (International Conference of Data Protection ant Privacy Commissioners. Resolution to address the role of human error ir personal data breaches. (2019);
68. Šidlauskas A. *Valstybinės duomenų apsaugos inspekcijos administracinių baudų skyrimo praktika ES šalių kontekste*. Mykolo Romerio universitetas. 2021, vol. 44(2), pp. 153–169. EISSN 2351-6712. DOI: https://doi.org/10.15388/Soctyr.44.2.10 P.154. Prieiga per internetą: https://www.zurnalai.vu.lt/social-research/article/view/25059;
69. Osborn M., Simpson A. *Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study*. (2017). P. 472-495. Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S0167404817300925‘
70. Kern M., Landauer M., Weippl E. (2024). *A logging maturity and decision model for the selection of intrusion detection cyber security solutions*. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S0167404824001457;
71. Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. *Cyber hygiene: The concept, its measure, and its initial tests*. (2020). Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S0167923619301897.
72. Lietuvos Respublikos Vidaus reikalų ministerija. *Rizikos analizės vadovas*. (2005). Prieiga per internetą: https://www.nksc.lt/doc/rizikos_analize.pdf.

Dilienė I. (2024). *Asmens duomenų nutekėjimo privačiame sektoriuje prevencija* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe išanalizuota privataus sektoriaus įmonių kibernetinio saugumo brandos lygio užtikrinimo problematika. Pirmajame skyriuje nagrinėjama asmens duomenų nutekėjimo prevencijos samprata bei priežastys. Antrame skyriuje yra nagrinėjamas tvarkomų asmens duomenų rizikos vertinimo bei nutekėjimo prevencijos teorinis konceptas, apžvelgiami rizikų vertinimo aspektai, nagrinėjamos organizacinės bei techninės asmens duomenų apsaugos priemonės bei jų taikymo poveikis įmonių saugumo kultūros bei darbuotojų sąmoningumo lygio didinimui. Trečiajame skyriuje pateikiami kokybinis ir kiekybinis tyrimai. Kokybiniu tyrimu atskleidžiami Pasvalio bei Pakruojo privataus sektoriaus mažo ir vidutinio dydžio įmonių poreikiai asmens duomenų apsaugos prevencijai bei identifikuojamos privataus sektoriaus mažų ir vidutinių įmonių galimybės užtikrinti kibernetinį saugumą. Kiekybiniu tyrimu atskleidžiami Pasvalio bei Pakruojo privataus sektoriaus mažo ir vidutinio dydžio įmonių darbuotojų dalyvavimo įmonių saugumo politikos kūrime ypatumai bei požiūris į įmonės asmens duomenų apsaugos bei kibernetinio saugumo prevencijos priemonių taikymą. Skyriuje pateikiamos tyrimų išvados bei detalizuojamos problemos, darančios įtaką įmonių asmens duomenų nutekėjimo prevencijai.

Pagrindiniai žodžiai: asmens duomenų nutekėjimas, kibernetinio saugumo priemonės, rizikos valdymas, kibernetinio saugumo mokymai, informacijos saugumo brandos lygis.

Diliene I. (2024). *Prevention of leakage of personal data in the private sector* (master's thesis). Vilnius: Mykolas Romeris University

ANNOTATION

The master's thesis deals with the issue of ensuring the maturity level of cyber security of private sector companies. The first chapter examines the concept and causes of personal data leakage prevention. The second chapter examines the theoretical concept of risk assessment of processed personal data and leakage prevention, reviews the aspects of risk assessment, examines organizational and technical personal data protection measures and the effect of their application on increasing the level of corporate security culture and employee awareness. The third chapter presents qualitative and quantitative research. The qualitative research reveals the needs of small and medium-sized enterprises of the private sector of Pasvalys and Pakruojis for the prevention of personal data protection and identifies the possibilities of small and medium enterprises of the private sector to ensure cyber security. The quantitative research reveals the peculiarities of the participation of employees of small and medium-sized enterprises in the private sector of Pasvalys and Pakruojis in the development of corporate security policies, as well as the approach to the application of company personal data protection and cyber security prevention measures. The chapter presents the research findings and details the problems affecting the prevention of corporate personal data leakage.

Key words: personal data leakage, cyber security measures, risk management, cyber security training, information security maturity level.

Dilienė I. (2024). Asmens duomenų nutekėjimo privačiame sektoriuje prevencija (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Asmens duomenų nutekėjimo privačiame sektoriuje prevencijos magistro baigiamojo darbo tema yra aktuali priežiūros institucijoms, privataus sektoriaus įmonėms bei darbuotojams siekiant įgyvendinti aukštą kibernetinio saugumo brandos lygį ne tik viešajame sektoriuje. Mokslininkai kibernetinės brandos lygį apibrėžia per gebėjimą identifikuoti rizikas, pažeidžiamus bei kontrapriemones, kurias panaudojus užkertamas kelias pavojui. Privataus sektoriaus kibernetinio saugumo politikos formavimas yra pakankamai naujas objektas, todėl buvo iškelta pagrindinė darbo problema - kaip turėtų būti užtikrinama asmens duomenų apsaugos nutekėjimo prevencija Lietuvos mažose ir vidutinėse įmonėse? Darbo objektas: Lietuvos privataus sektoriaus mažo ir vidutinio dydžio įmonės. Dalykas: asmens duomenų nutekėjimo prevencijos aktualumas Pasvalio ir Pakruojo privataus sektoriaus mažo ir vidutinio dydžio įmonėse. Darbo tikslas: identifikuoti kibernetinės brandos lygį Pasvalio ir Pakruojo miestų mažose ir vidutinėse įmonėse. Darbo uždaviniai: aptarti asmens duomenų nutekėjimo prevencijos teorinius aspektus, išryškinti privataus sektoriaus mažų ir vidutinių įmonių pasirengimo asmens duomenų nutekėjimo prevencijos tendencijas, ištirti Pasvalio ir Pakruojo miestų mažo ir vidutinio dydžio įmonių asmens duomenų nutekėjimo prevencijos pajėgumus, pateikti rekomendacijas privataus sektoriaus mažoms ir vidutinėms įmonėms bei priežiūros institucijoms dėl geriausių praktikų asmens duomenų nutekėjimo prevencijai užtikrinti. Darbo metodai: mokslinės literatūros analizė, lyginamoji literatūros analizė, duomenų vizualizacija, kokybinė turinio analizė, kiekybinė turinio analizė.

Empirinio tyrimo metu buvo, kad įmonių privatumo vadovai bei specialistai mano, kad įmonės neturi žmogiškųjų bei finansinių išteklių užtikrinti kibernetinio saugumo prevenciją. Nėra vykdomi asmens duomenų apsaugos bei kibernetinio saugumo auditai, nėra atliekamas rizikų vertinimas, darbuotojams nevedami asmens duomenų apsaugos bei kibernetinės higienos mokymai. Įmonių darbuotojai įmonių kibernetinio saugumo politiką vertina vidutiniškai, taikomos priemonės neužtikrina kibernetinio saugumo kultūros vystymo.

Magistro baigiamojo darbo pabaigoje pateikiamos išvados bei siūlymai dėl kibernetinio saugumo prevencijos užtikrinimo bei kibernetinės brandos lygio didinimo privataus sektoriaus įmonėse.

Diliene I. (2024). Prevention of leakage of personal data in the private sector (master's thesis). Vilnius: Mykolas Romeris University

SUMMARY

The topic of the master's thesis on prevention of personal data leakage in the private sector is relevant for supervisory authorities, private sector companies and employees in order to implement a high level of cyber security maturity not only in the public sector. Researchers define the level of cyber security maturity through the ability to identify risks, vulnerabilities and countermeasures that prevent the threat. The formation of the cyber security policy of the private sector is a fairly new object, therefore the main work problem was raised: how should the prevention of leakage of personal data protection be ensured in Lithuanian small and medium enterprises? Object of work: small and medium-sized enterprises of the Lithuanian private sector. Subject: the relevance of personal data leakage prevention in small and medium-sized enterprises of the private sector of Pasvalys and Pakruojis. The purpose of the work: to identify the level of cyber security maturity in the small and medium-sized enterprises of the cities of Pasvalys and Pakruojis. Tasks: to discuss the theoretical aspects of personal data leakage prevention, to highlight the trends in the preparation of private sector small and medium-sized enterprises for the prevention of personal data leakage, to study the personal data leakage prevention capacities of small and medium-sized enterprises in the cities of Pasvalys and Pakruojis, to provide recommendations for private sector small and medium-sized enterprises and supervisory authorities on best practices to ensure the prevention of personal data leakage. Work methods: scientific literature analysis, comparative literature analysis, data visualization, qualitative content analysis, quantitative content analysis.

During the empirical research, it was found that company privacy managers and specialists believe that companies do not have the human and financial resources to ensure cyber security prevention. Personal data protection and cyber security audits are not carried out, risk assessment is not carried out, personal data protection and cyber hygiene training is not conducted for employees. The employees of the companies evaluate the cyber security policy of the companies as average, the applied measures do not ensure the development of the cyber security culture.

At the end of the master's thesis, conclusions and suggestions are presented regarding the assurance of cyber security prevention and increasing the level of cyber maturity in private sector companies.

PRIEDAI

1 PRIEDAS

KIEKYBINIO TYRIMO KLAUSIMYNAS

Laba diena,

Esu Mykolo Romerio universiteto, viešojo valdymo ir verslo fakulteto, Kibernetinio saugumo valdymo studijų studentė – Inga Dilienė. Magistro baigiamajame darbe atlieku tyrimą ir kviečiu Jus dalyvauti apklausoje, skirtoje išsiaiškinti Jūsų patirtis taikant asmens duomenų nutekėjimo prevencijos priemones įmonėje. Tik Jūsų atsakymų dėka pavyks gauti objektyvius tyrimo rezultatus, kurie padės identifikuoti problemas ir prisidėti prie kokybiškesnio saugumo kultūros vystymo privataus sektoriaus įmonėse.

Apklausa anoniminė, todėl užtikrinu Jūsų atsakymų anonimiškumą (bus panaudoti tik apibendrinti rezultatai).

1. Jūsų lytis:

□ vyr.

□ mot.

2. Miestas, kuriame dirbate:

□ Pasvalys

□ Pakruojis

3. Kiek laiko dirbate įmonėje?

□ iki metų

□ daugiau nei 1 metus, bet mažiau nei 3 metus

□ daugiau nei 3 metus, bet mažiau nei 5 metus

□ daugiau nei 5 metus

4. Įvertinkite savo žinias apie asmens duomenų saugumą skalėje nuo 1 iki 10:

1	2	3	4	5	6	7	8	9	10

5. Ar esate susipažinę su pagrindiniais asmens duomenų apsaugos principais?

□ taip

□ ne

6. Ar žinote kaip identifikuoti potencialius duomenų nutekėjimo pavojus?

 taip

 ne

7. Ar Jūsų įmonėje yra aiškiai apibrėžtos duomenų saugumo procedūros?

 taip

 ne

8. Kaip vertinate Jūsų įmonėje esamų saugumo priemonių efektyvumą 1 – 10 balų skalėje?

1	2	3	4	5	6	7	8	9	10

9. Ar manote, kad Jūsų įmonė investuoja pakankamai išteklių į duomenų saugumą?

 taip

 ne

 nežinau

10. Kaip manote ar Jūsų įmonėje yra reguliariai atnaujinamos saugumo sistemos ir priemonės?

 taip

 ne

 nežinau

11. Ar per paskutinius 12 mėnesių dalyvavote duomenų apsaugos mokymuose?

 taip

 ne

12. Kaip vertinate galimų mokymų poveikį Jūsų sąmoningumui apie duomenų saugumą? (1-10 skalėje)

1	2	3	4	5	6	7	8	9	10

13. Ar Jūsų įmonė skatina nuolatinį mokymąsi ir tobulėjimą saugumo klausimais?

 taip

 ne

14. Ar esate pakankamai informuota (-as) apie asmens duomenų tvarkymo rizikas?

 taip

 ne

15. Ar Jūsų įmonėje per pastaruosius du metus įvyko asmens duomenų nutekėjimo atvejų?

 taip

 ne

 nežinau

16. Jei 15 klausime atsakėte „taip“, ar manote, kad buvo imtasi pakankamai priemonių, kad asmens duomenų nutekėjimo incidentai nepasikartotų?

 taip

 ne

 nežinau

17. Ar Jūsų įmonėje yra greitas ir veiksmingas planas reaguoti į asmens duomenų nutekėjimo incidentus?

 taip

 ne

 nežinau

18. Ar Jūsų įmonė reguliariai atlieka duomenų saugumo auditus?

 taip

 ne

 nežinau

19. Ar Jūsų įmonė laikosi Bendrojo duomenų apsaugos reglamento ir kitų asmens duomenų apsaugą reglamentuojančių teisės aktų?

 taip

 ne

 nežinau

20. Kaip vertinate Jūsų įmonės saugumo politikos aiškumą ir prieinamumą? (1-10 balų skalėje)

1	2	3	4	5	6	7	8	9	10

Dėkoju už Jūsų atsakymus!