VILNIAUS UNIVERSITETAS
ŠIAULIŲ AKADEMIJA

INFORMACINIŲ TECHNOLOGIJŲ VALDYMO MAGISTRO STUDIJŲ PROGRAMA

MANTAS MATUZEVIČIUS

Magistro studijų baigiamasis darbas

ISO 27001 IR ISO 27005 STANDARTŲ TAIKYMAS INFORMACINIŲ SISTEMŲ RIZIKŲ IR SAUGOS METODŲ VALDYMUI ĮMONĖJE

Darbo vadovas (-ė) Dr. L. Kaklauskas

Šiauliai, 2026

Studijuojančiojo, teikiančio baigiamąjį darbą, GARANTIJA

WARRANTY of Final Thesis

Vardas, pavardė *Name, Surname*	**Mantas Matuzevičius**
Padalinys *Faculty*	**Šiaulių akademija** ***Šiauliai Academy***
Studijų programa *Study Programme*	**Informacinių technologijų valdymas** ***Information technology management***
Darbo pavadinimas *Thesis topic*	**ISO 27001 ir ISO 27005 standartų taikymas informacinių sistemų rizikų ir saugos metodų valdymui įmonėje** **Application of ISO 27001 and ISO 27005 standards in managing information systems risks and security in an enterprise.**
Darbo tipas *Thesis type*	**Baigiamasis darbas** ***Final Thesis***

Garantuoju, kad mano baigiamasis darbas yra parengtas sąžiningai ir savarankiškai, kitų asmenų indėlio į parengtą darbą nėra. Jokių neteisėtų mokėjimų už šį darbą niekam nesu mokėjęs.

I guarantee that my thesis is prepared in good faith and independently, there is no contribution to this work from other individuals. I have not made any illegal payments related to this work.

Šiame darbe tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos yra pažymėtos literatūros nuorodose.

Quotes from other sources directly or indirectly used in this thesis, are indicated in literature references.

Aš, Mantas Matuzevičius, pateikdamas (-a) šį darbą, patvirtinu
(*pažymėti*) ☐

Embargo laikotarpis
Embargo Period

Prašau nustatyti šiam baigiamajam darbui toliau nurodytos trukmės embargo laikotarpį:
I am requesting an embargo of this thesis for the period indicated below:

_____ mėnesių / *months*
(embargo laikotarpis negali viršyti 60 mėn. / *an embargo period shall not exceed 60 months*).

Embargo laikotarpis nereikalingas / *no embargo requested.*

Embargo laikotarpio nustatymo priežastis / *Reason for embargo period*:

VILNIAUS UNIVERSITETO ŠIAULIŲ AKADEMIJOS DIRBTINIO INTELEKTO ĮRANKIŲ NAUDOJIMO RAŠTO DARBUOSE DEKLARACIJA

Vardas, pavardė: Mantas Matuzevičius
Studijų programa, kursas: Informacinių technologijų valdymas
Rašto darbo pavadinimas: ISO 27001 ir ISO 27005 standartų taikymas informacinių sistemų rizikų ir saugos metodų valdymui įmonėje
Rašto darbo tipas *(pvz., referatas, kursinis darbas, baigiamasis darbas):* Baigiamasis darbas
Modulio / dalyko pavadinimas *(išskyrus baigiamojo darbo atveju):*
Deklaracijos pateikimo data: 2025-12-1

Patvirtinu, kad vertinimui pateiktas savarankiškai atliktas rašto darbas yra parengtas laikantis Vilniaus universiteto Akademinės etikos kodekso[1], Vilniaus universiteto studijuojančiųjų rašto darbų rengimo, gynimo ir kaupimo nuostatai[2], Vilniaus universiteto Šiaulių akademijos rašto darbų rengimo ir gynimo tvarkos[3] ir Dirbtinio intelekto naudojimo Vilniaus universitete gairių[4].
Pažymiu, kad rašto darbo rengimui *buvo naudojami / nebuvo naudojami (pabraukti tinkamą variantą)* generatyvinio dirbtinio intelekto (toliau - DI) įrankiai.
Tuo atveju, jei darbo rengimui buvo pasitelkti DI įrankiai, pateikiu tikslią ir išsamią informaciją apie jų naudojimo tikslus ir apimtį:

1. DI įrankiai:

   - Naudoti įrankiai (pvz.: Connected Papers, Midjourney, GitHub Copilot ar kiti, *įrašyti*): ChatGPT (OpenAI).
   - Naudojimo tikslas (duomenų rinkimas, redagavimas, vertimas, priedų generavimas ar kitas, *įrašyti*): DI įrankis buvo naudojamas, kaip pagalbinė priemonė informacijos paieškai, sudėtingų teorinių sąvokų paaiškinimui, užsienio kalbos teksto formuluočių tikslinimui, bei supaprastinimui.

2. Esminiai DI panaudojimo atvejai:

Darbo dalis/vieta (puslapis, pastraipa)	Naudojimo tikslas	Užklausų pavyzdžiai
2 skyrius (teorinė dalis)	Terminų ir sąvokų paaiškinimas iš anglų kalbos, teksto supaprastinimas ir stiliaus	„Perfrazuok ISO 27001 reikalavimą paprasčiau“, „Paaiškink ISO 27005 rizikos

[1] Vilniaus universiteto akademinės etikos kodeksas, https://www.vu.lt/site_files/Akademines_etikos_kodeksas_suvestine_redakcija.pdf

[2] Vilniaus universiteto studijuojančiųjų rašto darbų rengimo, gynimo ir kaupimo nuostatai, 2024-05-21_Studijuojančiųjų_RD_rengimo_gynimo_ir_kaupimo_nuostatai.pdf

[3] Vilniaus universiteto Vilniaus universiteto Šiaulių akademijos rašto darbų rengimo ir gynimo tvarka, https://www.sa.vu.lt/external/sa/files/Studiju_skyrius/VUSA_Rasto_darb%C5%B3_rengimo_ir_gynimo_tvarka_2024.pdf

[4] Dirbtinio intelekto naudojimo Vilniaus universitete gairės, https://www.vu.lt/site_files/SPN-54_2024_priedas.pdf

Darbo dalis/vieta (puslapis, pastraipa)	Naudojimo tikslas	Užklausų pavyzdžiai
	korekcija verčiant iš anglų kalbos.	vertinimo esmę trumpai“, „Išversk ir pateik trumpą santrauką ISO 27001 standarto“
2.7 skyrius (praktinė dalis)	Incidentų valdymo proceso struktūros rengimas, vizualų logikos tikrinimas.	„Aš šis vizualas atitinka 27001 standartą“, „Kokie minimalus reikalavimai valdymo procesams mažai įmonei“
3 skyrius (ISVS modelis)	Modelio pritaikymas, formuluočių supaprastinimas ir struktūravimas.	„Ar PDCA schema atitinka pagrindinį modelį“, „Supaprastink PDCA modelio aprašymą“

3. Savarankiškumas ir autorystė:

- Patvirtinu, kad esu atsakingas(-a) už rašto darbo savarankiškumą ir autorystę: visos DI sugeneruotos rašto darbo dalys mano atidžiai patikrintos, patikslintos, pataisytos ir pažymėtos literatūros nuorodose. Darbas parengtas užtikrinant jame pateikiamų DI įrankiais sugeneruotų teksto dalių ir (ar) priedų tikslumą, patikimumą ir korektiškumą;
- Patvirtinu, kad DI įrankiai nenaudoti darbe pateikiamų duomenų, informacijos, autorių minčių klastojimui, iškraipymui ar kitokio pobūdžio klaidinančiam pateikimui.

4. Akademinė etika:

- Patvirtinu, kad pateikta informacija apie DI įrankių naudojimą yra tiksli ir išsami;
- Patvirtinu, kad DI įrankiai naudoti savarankiško duomenų rinkimo, tyrimo, analizės, teksto ar priedų (*pabraukti tinkamą; jei reikia, įrašyti papildomą informaciją*_____) (pa)pildymui, o ne kaip savarankiško darbo pakaitalas;
- Suprantu, kad nenurodytas DI įrankių naudojimas gali būti laikomas draudimo plagijuoti pažeidimu, kuris numatytas Vilniaus universiteto Akademinės etikos kodekse.

TURINYS

SANTRAUKA

ISO 27001 IR ISO 27005 STANDARTŲ TAIKYMAS INFORMACINIŲ SISTEMŲ RIZIKŲ IR SAUGOS METODŲ VALDYMUI ĮMONĖJE

Darbe nagrinėjama informacijos saugos valdymo problema mažoje žemės ūkio įmonėje, kurioje dėl ribotų žmogiškųjų ir finansinių išteklių saugos priemonės dažnai diegiamos tik iš dalies, o sauga neretai vertinama , kaip papildomos sąnaudos, nors įmonė kiekvieną dieną tvarko klientų, tiekėjų ir kitus finansinius duomenis.

Darbo tikslas – pritaikyti ISO 27001 ir ISO 27005 standartų principus įmonės informacinės sistemos rizikų ir saugos metodų valdymui.

Teorinėje dalyje apžvelgiami ISO 27000 serijos standartų pagrindai, rizikos samprata ir vertinimo logika, taip pat aptariamas teisinis ir rekomendacinis kontekstas (BDAR, NKSC, NIST).

Praktinėje dalyje atlikta įmonės informacinės aplinkos analizė, apibrėžtos vertinimo ribos, identifikuotos grėsmės ir pažeidžiamumai, sudaryta rizikos matrica ir rizikų registras, parengtas rizikų valdymo planas, taip pat išanalizuoti tipiniai incidentų scenarijai, kaip sukčiavimo laiškai, kasos kompiuterio sutrikimai ar NVR įrašų praradimas ir numatyti stebėsenos bei incidentų fiksavimo principai. Remiantis gautais rezultatais, pateiktas informacijos saugos tobulinimo modelis, kuris orientuotas į minimaliai pakankamą, bet tuo pačiu ir nuoseklų valdymą, pagal PDCA logiką, aiškių atsakomybių pasiskirstymą, prioritetinių kontrolės priemonių pasirinkimą pagal ISO 27001 standartą, minimalų dokumentų rinkinį ir įgyvendinimo planą, kuris leidžia vertinti prieš ir po būklės pokytį ir likutinę riziką.

Reikšmingi žodžiai: Informacijos sauga, ISVS, ISO 27001, ISO 27005, rizikų registras, rizikos matrica, incidentų valdymas, stebėsena.

SUMMARY

Application of ISO 27001 and ISO 27005 standards for information systems risk and security management in an enterprise

This thesis examines the problem of information security management in a small agricultural enterprise where due to limited human and financial resources, security measures are often implemented only partially, while information security is treated as an additional cost, even though customer, supplier, and other financial data are processed on a daily basis.

The aim of the thesis is to apply the principles of ISO 27001 and ISO 27005 standards to the management of information system risks and security methods in the company.

The theoretical part reviews the fundamentals of the ISO 27000 series standards, the concept of risk and the logic of risk assessment, and also discusses the legal and guidance context (GDPR, NKSC, NIST).

The practical part includes an analysis of the company's information environment, the definition of assessment boundaries, the identification of threats and vulnerabilities, the development of a risk matrix and a risk register, and the preparation of a risk management plan. It also analyzes typical incident scenarios such as phishing emails, point-of-sale computer disruptions, or the loss of NVR recordings, and defines monitoring and incident logging principles. Based on the obtained results, an information security improvement model is presented, which is focused on minimally sufficient but consistent management according to the PDCA cycle, a clear allocation of responsibilities, the selection of priority controls in line with ISO 27001, a minimal set of documents, and an implementation plan that enables the assessment of before-and-after changes and residual risk.

Keywords: Information security, ISMS, ISO 27001, ISO 27005, risk register, risk matrix, incident management, monitoring.

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Šiuolaikinėje skaitmeninėje eroje informacija tapo viena iš svarbiausiu kiekvienos organizacijos vertybių, taip pat ir jos saugumas, kuris yra vienas iš esminiu konkurencingumo bei patikimumo veiksniu. Sparčiai tobulėjant technologijoms, kaip debesų kompiuterijai, automatizavimui, dirbiniui intelektui ir daiktų interneto sprendimai iš esmės pakeitė verslų procesus, taip padidinant priklausomybę nuo informacinių sistemų. Dėl šios priežasties informacijos sauga tampo ne tik techniniu, bet ir strateginiu valdymo klausimu, turinčiu visiškai tiesioginį poveikį įmonės veiklos tęstinumui, reputacijai ir ekonominiam stabilumui.

Internetinių incidentų statistika rodo, kad pastaraisiais metais įmonės vis dažniau susiduria su įvairiais duomenų nutekėjimais, paslaugų trikdžiais, ar net finansiniais sukčiavimais bei kitomis saugumo grėsmėmis. Pagal pasaulio ekonomikos forumo „Global Cybersecurity Outlook 2025“ duomenis, daugiau nei 70 procentų viso pasaulio organizacijų patyrė vieną ar daugiau reikšmingų kibernetinių incidentų per pastaruosius dvejus metus, o itin mažos ar mažos įmonės tampa vis dažnesniu taikiniu, dėl turimų ribotu resursų, bei silpnų saugos planų [24]. Ši tendencija aktuali ir Lietuvoje, nacionalinio kibernetinio saugumo centro 2024 m. ataskaitose pažymima, kad itin didelė dalis incidentų kyla, dėl netinkamo rizikų vertinimo, prastos prieigos bei žmogiškųjų klaidų [21].

Norint sistemingai užtikrinti informacijos saugumą, organizacijos vis plačiau taiko ISO/IEC2700 standartus. Tarp šių standartų vienas iš pagrindinių yra ISO/IEC 27001, kuris nustato informacijos saugos valdymo sistemos reikalavimus. Šis standartas padeda struktūruotai, pagal atitinkamas gaires identifikuoti, vertinti ir mažinti informacijos saugumo rizikas, nustatant politiką, tikslus bei kontrolės priemones. ISO/IEC 27005 papildo ISO/IEC 27001 standartą, kuris apibrėžia rizikos valdymo procesus, kurie leidžia praktiškai taikyti rizikos analizės metodus ir formuoti prioritetus remiantis grėsmių tikimybe bei poveikiu. Abu šie standartai sudaro deranti, plačiu mastu taikomą ir pripažinta informacijos saugumo valdymo pagrindą, suderinamą su kitomis valdymo sistemomis, kaip ISO 9001 ar ISO 22301

Šio darbo aktualumą lemia tai, kad mažos, itin mažos ar vidutinės įmonės Lietuvoje nors ir suvokdamos informacijos saugos svarbą, dažnai į tai žiūri pro pirštus, dėl netinkamo kompetencijos lygio ar priemonių valdyti rizikas. Taip pat įmonės į šį saugumo klausimą neretai žiūri, kaip į papildomas išlaidas, o ne kaip investiciją į veiklos vientisumą ir tęstinumą. Tokia situacija būdinga ir nagrinėjamai mažai įmonei, veikiančiai žemės ūkio srityje. Įmonė kiekvieną dieną tvarko klientų, tiekėjų ir kitus finansinius duomenis, todėl jų saugumas yra svarbus tiek veiklos patikimumui, tiek atitikčiai teisiniams reikalavimams. Augantis kibernetinių grėsmių lygis lemia poreikį įmonei

taikyti veiksmingą informacijos saugumo valdymo sistemą, pagrįstą ISO standartais, kuri leistų valdyti, numatyti ir mažinti rizikas.

Magistro darbo problema.

Kaip efektyviai taikyti ISO 27001 ir ISO 27005 standartų principus mažoje žemės ūkio įmonėje, siekiant optimizuoti informacinių sistemų rizikų valdymą ir užtikrinti tinkamą duomenų apsaugos lygi.

Magistro darbo objektas

Informacinių sistemų rizikų ir saugos metodų valdymas taikant ISO 27001 ir ISO 27005 standartus.

Magistro darbo tikslas

Pritaikyti ISO 27001 ir ISO 27005 standartų principus mažos prekybinės įmonės informacinės sistemos rizikų ir saugos metodų valdymui.

Magistro darbo uždaviniai

1. Išnagrinėti informacijos saugumo ir rizikų valdymo teorinius modelius, remiantis ISO/IEC 27000 serijos minimais standartais.
2. Aptarti teisinį ir organizacinį informacijos saugumo valdymo modelį remiantis BDAR, NKSC gairėmis.
3. Įvertinti mažos žemės ūkio įmonės informacinės sistemos būklę ir identifikuoti pagrindines rizikas.
4. Sudaryti rizikų registrą ir įvertinti rizikų tikimybę bei poveikį pagal ISO 27005 taikomą metodiką.
5. Pasiūlyti rizikų valdymo priemones ir minimalų informacijos saugos valdymo modelį, pagrįsta ISO/IEC 27001 kontrolėmis ir PDCA logika.

Magistro darbo metodai

Mokslinės ir norminės literatūros analizė. Įmonės informacijos saugos būklės kokybinė atvejo analizė, remiantis faktine organizacijos infrastruktūra ir taikomomis saugos priemonėmis, kaip vietinės įrangos, programinės įrangos, paskyrų ir procesų aprašymu. Kokybinis rizikų vertinimas pagal ISO/IEC 27005 principus. Procesų modeliavimas BPMN diagrama. Lyginamoji analizė tarp teorinių saugos principų ir praktikoje taikomų sprendimų organizacijoje.

Magistro darbo šaltiniai

Pagrindinis informacijos šaltinis, tai tokie dokumentai, kaip ISO/IEC 27001 [4] ir ISO/IEC 27005 [6] standartų dokumentacija, NKSC rekomendacijos, BDAR nuostatos, NIST gairės. Praktinė dalis apima mažos žemės ūkio įmonės duomenis, tai rizikų registras, incidentų pranešimai, tyrimo ataskaitos bei veiklos procesų diagramos.

Magistro darbo struktūra

Darbas susideda ir įvado, trijų pagrindinių skyrių, išvadų, literatūros sąrašo ir priedų. Pirmajame skyriuje pateikiami informacijos sistemų saugos valdymo ir rizikos analizės teoriniai apibrėžimai. Nagrinėjami ISO standartų principai. Antrajame skyriuje atliekamas mažos žemės ūkio įmonės informacinės sistemos analizė, identifikuojamos rizikos, sudaromos rizikų registras ir vertinamos saugos priemonės. Trečiajame skyriuje pateikiamas ISO standarto taikymo modelis kuris apima rizikos valdymo ir saugos politikos tobulinimo rekomendacijas. Darbo pabaigoje pateikiamos praktinės rekomendacijos mažoms ar itin mažoms įmonėms, kurios siekia diegti saugos valdymo sistemas ir išvados.

1 INFORMACINIŲ SISTEMŲ SAUGOS VALDYMO TEORINIAI PAGRINDAI

Šiame skyriuje analizuojamos informacinės sistemos, jų saugos valdymo teoriniai aspektai kurie apima visą darbą. Aptariama informacijos saugos samprata, kokie pagrindiniai principai ir rizikų valdymo reikšmė šiuolaikinėje organizacijoje. Didelis dėmesys skiriamas ISO/IEC 27000 tipo standartams [7], kurie nustato informacijos saugos valdymo sistemos kūrimo, pritaikymo, vėliau priežiūros ir tobulinimo principus.

Analizuojamas ISO/IEC 27001 standartas [4], kuris aprašo informacijos saugos valdymo sistemos reikalavimus, ISO/IEC 27005 standartas [6], pateikia rizikos vertinimo ir valdymo metodus, principus. Visų šių standartų suderinimas leidžia įmonėms efektyviai pastebėti, vertinti bei kontroliuoti įvairias informacines saugos rizikas, užtikrinant nuoseklų ir tvarų kibernetinio saugumo valdymą.

Taip pat nagrinėjamas teisinis informacijos saugos valdymo kontekstas, kuris apima bendrąjį duomenų apsaugos reglamentą (BDAR) [13], ir nacionalinio kibernetinio saugumo centro (NKSC) rekomendacijas [12], [15], kurios padeda užtikrinti atitiktį Lietuvos, bei Europos Sąjungos teisės aktams.

Pateikiamos informacinių sistemų rizikos valdymo modelių analizė, aptariami mažoms ar itin mažoms įmonėms taikomi praktiniai metodai, bei priemonės leidžiančios valdyti kibernetines grėsmes turint itin ribotus resursus.

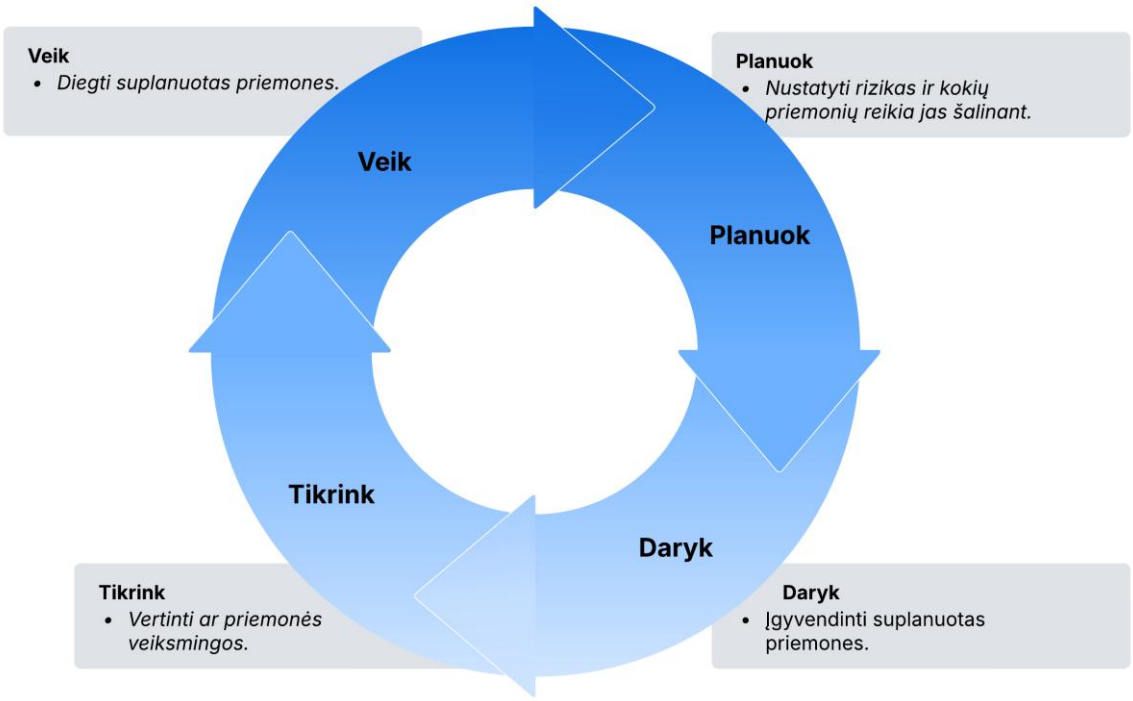
1.1 ISO/IEC 27001 standarto samprata

ISO/IEC 27001 standartas, tai tarptautiniu mastu primažintas informacijos saugumo valdymo standartas, kuris nustato reikalavimus informacijos saugos valdymo sistemai (ISVS). Standartas apibrėžia struktūruotą ir sistemingą metodą, leidžiantį organizacijoms identifikuoti informacines rizikas, jas vertinti ir įgyvendinti tinkamas kontrolės priemones, kurios užtikrina informacijos konfidencialumą, vientisumą ir pastovų pasiekiamumą [4].

Informacijos saugumas ir vientisumas dažniau tampa ne techniniu sprendimu, o strateginiu įmonės valdymo klausimu. Įvairios organizacijos savo veiklą grindžia turimais duomenimis, apie klientus, finansinius įrašus, partnerių ir tiekėjų ryšius, visų šių duomenų pažeidimas arba praradimas gali tiesiogiai paveikti įmonės veiklos tęstinumą. Kaip pažymi Venčkauskas ir Kazanavičius knygoje „Informacinių technologijų saugos metodai“, galime suprasti, kad informacijos saugumas šiuolaikinėje organizacijoje turi būti suprantamas ne tik, kaip technologinė apsauga, bet ir kaip nuoseklus, politikomis, atsakomybe ir kontrole grįstas procesas [1].

ISO/IEC standartas 27001 sako, kad visas valdymas turi būti procesiškai aiškus ir visada tobulėjantis [2]. Jis remiasi PDCA(Paln-Do-Check-Act) [2] modeliu, kuris apibrėžiamas įvairiuose tarptautiniuose dokumentuose, o ypač 27001 informacijos saugos standarto dokumentuose [2]. PDCA leidžia saugos valdymą vykdyti greitai, reaguojant į įvairius išorės ar vidaus pokyčius, naujas grėsmes ar technologinius pokyčius.

1 pav. PDCA ciklo etapai informacijos saugos valdymo sistemoje [2]
(Sudaryta autoriaus pagal Demingo cinklą [2])



1.2 ISO/IEC 27001 struktūra ir valdymo logika

ISO/IEC 27001 standartas turi aiškią, nuoseklią struktūrą, kuri padeda įmonėms ar organizacijoms tvarkingai valdyti informacijos saugumą. Standartas remiasi tuo, kad saugumas turi būti organizuojamas nuosekliai, planuojant, įgyvendinant, tikrinant bei tobulinant vykdomus procesus. ISO 27001 standartas sudarytas pagal bendrą ISO valdymo sistemų karkasą – Annex SL, kuris užtikrina vienodą logiką, struktūrą ir reikalavimų suderinamumą visiems standartams.

Moksliniuose straipsniuose pabrėžiama, kad Annex SL įvesta tam, kad visi ISO standartai turėtų tokią pačią aukšto lygio struktūrą, dar kitaip vadinama „High-Level Structure (HLS)“ [3]. Majernik ir kiti. (2017), nurodo, kad Annex SL struktūra suvienodina visus ISO standartus, jų valdymo struktūrą, kad jie taptų lengviau suprantami ir suderinami vienas su kitu [3], toks standartų

suderinimas palengvina integraciją tarp skirtingų sistemų, bei sumažina dokumentų kiekį aprašant standartus bei jų taikymą.

Atliekant mokslinę analizę, Majernik ir kiti (2017) išsamiai tyrė, kaip HLS struktūra praktiškai veikia organizacijų valdymo sistemas. Autoriai straipsnyje nurodo, kad ISO standartas parengtas pagal Annex SL ir jame numatytais 10 tokių pačių skyrių, nuo organizacijos iki tobulinimo, ir šie skyriai leidžia skirtingus standartus sujungti į vieną bendrą sistemą. Tyrėjai teigia, kad bendri reikalavimai, bei vienoda struktūra mažina procesų ir dokumentų kartojimasi ir visa tai supaprastina standartų diegimą, ypač jei jie diegiami keli iš karto [3]. Taip pat autoriai išskiria tai, kad HLS struktūra yra paremta PDCA ciklu, todėl ISO standartas paremtas Annex SL automatiškai skatina nuolatinį tobulėjimą, bei aiškius valdymo procesus. Straipsnyje taip pat pateikiami integruotų valdymo sistemų diegimo algoritmai, kurie parodo, kad dėl Annex SL organizacijos gali greičiau ir paprasčiau pereiti per analizės, planavimo, audito, tobulinimo etapus. Išvadose pabrėžiama, kad HLS ženkliai palengvina integruotų sistemų kūrimą, nes skirtingi standartai tampa tarpusavyje lengviau suderinami bei pritaikomi praktikoje [3].

Pagal Annex SL nustatytą struktūrą, visi ISO valdymo standartai turi vienodus skyrių numerius, nuo 4 iki 10, todėl ISO/IEC 27001 taip pat prasideda nuo 4 – skyriaus.

4. **Organizacijos kontekstas:**

   Organizacija turi žinoti ir suprasti, kokioje aplinkoje veikia, kokią informaciją saugo ir kokie veiksniai, išoriniai ar vidiniai daro ar gali padaryti įtaką jos saugumui.

5. **Vadovavimas:**

   Organizacijos vadovai turi rodyti iniciatyvą, kad saugumas jiems yra svarbu, patvirtinti naujas politikas ir atsakomybes.

6. **Planavimas:**

   Atliekamas organizacijos rizikos vertinimas, analizė bei planuojamos naujos priemonės kurios sumažins saugumo grėsmę.

7. **Parama (ištekliai):**

   Nustatoma kurie žmonės, priemonės, dokumentai ar kita informacija reikalinga tinkamam saugos sistemos veikimui.

8. **Veikla (įgyvendinimas):**

   Realūs veiksmai, diegiamos priemonės, procesai bei procedūros.

9. **Veiklos vertinimas**

   Atliekamas įgyvendintu priemonių vertinimas ar priemonės veikia – atliekami auditai, analizės, matuojami rodikliai ir lyginami su ankščiau atlikta analize.

10. Tobulinimas

Pagal vertinimo rezultatus priemonės koreguojamos, atnaujinamos ar kitaip stiprinamos.

Visa šis Annex SL struktūros priedas paremtas PDCA (Plan-Do-Check-Act) logika[3], tai reiškia:

- Plan (Planavimas): Nustatomos rizikos ir tikslai.
- Do (Įgyvendinimas): Diegiamos suplanuotos priemonės.
- Check (Tikrinimas): Tikrinama, bei vertinama, kas veikia, o kas ne.
- Act (Tobulinimas): Šalinami trūkumai, tobulinami procesai.

Taip pat ISO/IEC 27001 turi svarbų A priedą, kuriame pateikiamas kontrolės priemonių sąrašas, kaip prieigos kontrolė, incidentų valdymas ir tt, viso jų 93 [4], bet organizacija neprivalo jų visų taikyti, ji pati pasirenka tik tas priemones, kurios reikalingos pagal atlikta rizikos vertinimą. Visa tai yra ypač labai svarbu mažoms įmonėms, kurioms reikia efektyvių, bet ne per sudėtingų ar brangių saugos sprendimų.

Dėl tokios puikios ISO/IEC 27001 struktūros, jis yra lengvai pritaikomos įvairių dydžių organizacijose. Jis padeda dirbti nuosekliai, pagal aiškų ir nuoseklu procesą. Toks principas bus taikomas ir naudojamas vertinant ir tobulinant nagrinėjamos mažos įmonės informacijos saugumo valdymą

ISO/IEC 27001 A priedas apima viso 93 kontroles priemones [4], kurios suskirstytos į keturias pagrindines grupes, kiekviena grupė orientuota į skirtingą informacijos saugos sritį ir jos visos kartu sudaro vieną didelį saugos valdymo rinkinį. Visų šių priemonių paskirtis, padėti organizacijoms, kaip tinkamai įgyvendinti apsaugos priemones pagal priskirtas rizikas.

1 lentelė. ISO/IEC 27001:2022 A priedo kontrolės grupės

(Sudaryta autoriaus pagal ISO/IEC 27001:2022 A priedą [4])

Priemonių grupė	Ką apima priemonės	Priemonių pavyzdžiai
Organizacijos sauga	37 – priemonės apima politikas, procedūras, atsakomybes, valdymo taisykles kurios reikalingos kurti ISVS sukūrimui.	• Atsakomybių apibrėžimas • Grėsmių stebėsena • Turto valdymas • Praeigos kontrolė
Darbuotojų sauga	8 – priemonės kurios susijusios su darbuotojų mokymais, atsakomybėmis, saugiu elgesiu tvarkant ir dirbant su informacijos tvarkymo veiklomis.	• Darbuotojų patikros • Darbuotojų mokymai • Konfidencialumo sutartis

Priemonių grupė	Ką apima priemonės	Priemonių pavyzdžiai
		• Incidentų pranešimai
Fizinė sauga	14 – priemonių užtikrina fizinę patalpų, įrangos, bei infrastruktūros apsaugą nuo neteisėtos prieigos ar kitų fizinių grėsmių.	• Patalpų apsauga • Įrangos priežiūra • Darbo aplinkos politika
Technologinė sauga	15 – priemonių skirtos informacinių sistemų, tinklų ir duomenų apsaugai nuo galimų kibernetinių ir kitų technologinių grėsmių.	• Atsarginių kopijų kūrimas • Apsaugos nuo kenkėjiškų programų • Tinklo segmentavimas

Pateiktoje pirmoje lentelėje, matomos kontrolės priemonių grupės, kurios parodo, kad ISO/IEC 27001 A priedas apima - organizacinius, žmoniškuosius, fizinius bei technologinius informacijos saugos aspektus. Tokia struktūra leidžia įmonėms pasirinkti, tik jai reikalingiausias ir būtiniausias priemones, pagal atliktą rizikos vertinimą, todėl standartas yra ypač lankstus ir tuo pačiu tinkamas įvairioms organizacijoms, tuo tarpu ir mažoms. Visas šias priemones gali pritaikyti ir maža įmonė atsirenkant, kas jai yra svarbiausia, taip sutelkiant visą dėmesį į didžiausias rizikas, tokias kaip prieigos kontrolė, darbuotojų mokymai, tinklo apsauga, bei fizine vidaus sauga. Tokiu būdu užtikrinamas efektyvus informacijos saugumo valdymas, neapkraunant mažos įmonės dideliais, pertekliniais ar brangiais sprendimais. Taip pat, šis standartas aiškiai apibrėžia reikalavimus ir suteikia struktūrizuotą veiklos modelį, todėl jis yra lengvai diegiamas, net ir mažose įmonėse, kurios neturi sudėtingų valdymo procesų. Dėl šios priežasties ISO 27001 standartas tampa tinkamu pagrindu kurti ir palaikyti informacijos saugumo valdymą mažose įmonėse, įskaitant ir nagrinėjama įmonę.

1.3 ISO/IEC 27005 standarto samprata ir rizikų valdymo principai

ISO/IEC 27005 standartas buvo sukurtas siekiant suteikti organizacijoms praktines gaires, kaip įgyvendinti informacijos saugumo rizikų valdymo procesą. Šio standarto ištakos siekia BS 7799-3:2006 „Information security management systems – Guidelines for information security risk management“ [5], kuris tapo vienu pagrindinių dokumentų kuriant tarptautiniu mastu pripažintas ir plačiai naudojamas rizikų valdymo metodikas

Kitaip nei ISO/IEC 27001, kuris nustato bendrinius informacijos saugos valdymo sistemos reikalavimus, ISO/IEC 27005 atsako į vieną iš pagrindinių praktinių klausimų: „Kaip tinkamai valdyti informacijos saugumo rizikas?“[6]. ISO/IEC 27005 ir NIST SP 800-30 dokumentuose aiškiai pateikiama metodinė struktūra [6], kuri detalizuoja visą rizikos valdymo logiką, nuo konteksto nustatymo, rizikų indentifikavimo iki rizikos tvarkymo ir procedūrų priėmimo. Dėl šios

priežasties standartas laikomas metodiniu įrankiu, kuris leidžia įmonėms aiškiai struktūrizuoti rizikų valdymo procesą, parinkti tinkamas saugos priemones ir priimti pagrįstus sprendimus.

ISO/IEC 27005 standartas yra vienas iš svarbiausių ISO/IEC 27000 serijos standartų, skirtų informacinių rizikų valdymui organizacijose. Jis papildo ISO/IEC 27001 standartą ir pateikia metodinį pagrindą, kaip tinkamai identifikuoti, vertinti, analizuoti bei valdyti pasitaikančias ar galimas rizikas, atsižvelgiant į įmonės veiklą, turimus išteklius ir technologinę aplinką. Šis standartas orientuotas į praktinį rizikų valdymo proceso taikymą ir suteikia įmonėms struktūrą, kuri leidžia efektyviai spręsti kylančias saugos problemas, nusistatyti prioritetus bei pasirinkti geriausiai įmonės poreikius atitinkančias kontrolės priemone.

ISO/IEC 27005 standartas nėra susijęs su konkrečiomis technologijomis ar tam tikrais techniniais sprendimais, todėl jis yra universalus ir pritaikomas įvairaus dydžio bei skirtingos veiklos įmonėse. Jį taikant galima formuoti rizikomis grįstą informacijos saugos valdymo sistemą, kuri remiasi turto, grėsmių ir pažeidžiamumų analize, rizikos tikimybės ir poveikio vertinimu bei racionaliu kontrolės priemonių parinkimu.

Šis principas grindžiamas tuo, kad rizika atsiranda tuomet, kai egzistuoja vertingas turtas, jam grėsmę keliantis veiksnys ir pažeidžiamumas, leidžiantis tai grėsmei pasireikšti. Todėl ISO/IEC 27005 itin daug dėmesio skiria tam, kad organizacija gebėtų nustatyti savo kritinį turtą, jam kylančias grėsmes ir vidaus ar išorės pažeidžiamumus, kurie galėtų sukelti incidentą.

Be to, standartas pabrėžia, kad rizikų valdymas yra nuolatinis procesas, o ne vienkartinis veiksmas. Rizikos turi būti identifikuojamos, analizuojamos ir vertinamos reguliariai, atliekant stebėseną bei peržiūras, nes tiek technologijos, tiek grėsmės, tiek organizacijos veikla nuolat kinta. Dėl to ISO/IEC 27005 rizikų valdymo modelis glaudžiai siejasi su ISO/IEC 27001 taikomu PDCA principu, kuris užtikrina procesų tęstinumą ir nuolatinį tobulinimą

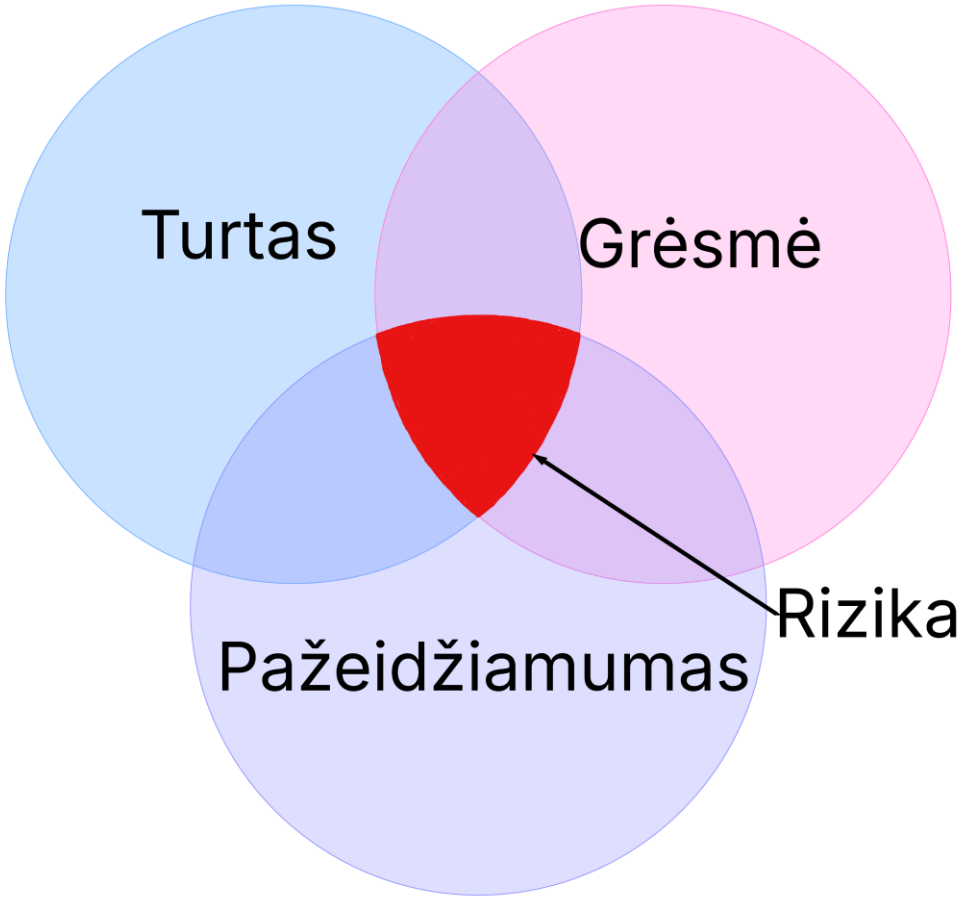
Apibendrinant galima teigti, kad ISO/IEC 27005 – „Informacijos saugos rizikų valdymas“ [7], kuris suteikia įmonėms aiškų, nuoseklų ir rizika grįstą metodinį pagrindą, kuris padeda priimti objektyvius saugos sprendimus, efektyviai planuoti investicijas į kontrolės priemones ir valdyti saugumo rizikas taip, kad jos minimaliai paveiktų įmonės veiklą ir svarbiausius procesus.

1.4 Rizikos samprata ir turto-grėsmės-pažeidžiamumo sąveika

Rizikos samprata informacijos saugos srityje siejama su galimais įvykiais, kurie gali įvykti ir sukelti poveikį organizacijos veiklai, jo turtui ar duomenų konfidencialumui, vientisumui, bei prieinamumui. ISO 27005 standartas apibrėžia rizikas, kaip jos gali turėti tam tikrą neigiamą poveikį informacijai ar veiklos procesams. Kitaip tariant rizika atsiranda ne iškarto ir ne savaime, bet tada kai egzistuoja trys pagrindiniai elementai: Turtas (asset), grėsmė (threat), pažeidžiamumas (vulnerability) [6].

2 pav. Rizikos atsiradimo venn diagrama pagal NIST SP 800 [8].

(Sudaryta autoriaus remiantis NIST SP 800[8])



Kaip matyti iš pateikto antro paveikslėlio, rizika susidaro tik tada, kai visi trys elementai – turtas, grėsmė ir pažeidžiamumas veikia kartu. Jeigu egzistuoja turtas, tačiau nėra realios grėsmės, rizika neatsiranda, taip pat jei yra grėsmė, bet nėra pažeidžiamumo, grėsmei nėra kaip pasireikšti, nes nėra pažeidžiamumo ir incidentas neįvyksta. Rizikos valdymo procese pirmiausias būtina nustatyti kritinius įmonės turtus, kokios grėsmės gali jiems kilti, bei vidinius ir išorinius pažeidžiamumus, kurie sudaro sąlygas incidentui įvykti. Modelis leidžia labai paprastai ir tiksliai

suprasti, kaip formuojasi ir atsiranda rizika, taip pat modelis įmonei padeda paprasčiau pasirinkti tinkamas kontroles priemones pagal jų silpniausias vietas.

1.5 Rizikos analizės tipai

ISO/IEC 27005 nurodo, kad rizikos analizė gali būti atliekama keliais skirtingais metodais: kokybiniu, kiekybiniu ir mišriuoju būdu. Konkretaus metodo pasirinkimas priklauso nuo organizacijos turimų duomenų, laiko, patirties bei resursų. Šis požiūris visiškai sutampa su tuo, kas aprašoma ir kitose metodikose, kaip nepaprastųjų situacijų valdymo vadovuose, kuriuose akcentuojama, kad analizės išsamumas „Priklauso nuo išteklių ir skito laiko, rizikos apimties ir kompleksiškumo“[9].

1.5.1 Kokybinė rizikos analizė

Kokybinė analizė yra pats paprasčiausias ir dažniausias praktikoje naudojamas metodas, kai rizikų tikimybė ir poveikis vertinami žodinėmis kategorijomis – „žema“, „vidutinė“ ir didelė, o ne konkrečiais skaičiais. Šis metodas yra lankstus, greitas ir nereikalauja didelių duomenų apimčių, todėl yra ypač tinkamas mažoms įmonėms.

A. Survila pabrėžia, kad kokybiniai metodai yra patrauklūs tuo, kad jie reikalauja mažiau laiko, pinigų ir (labai svarbu) patirties juos taikyti. Taip pat pažymi, kad kokybinė analizė suteikia vertintojams plačias galimybes ir leidžia efektyviai nustatyti prioritetus, net tada, kai statistinių duomenų nėra [9]. Tačiau kokybinė analizė turi ir trūkumų – vertinimas yra subjektyvus, priklauso nuo vertintojo patirties ir gali skirtis tarp kitų specialistų, todėl ISO/IEC 27005 standartas rekomenduoja kokybinę analizę taikyti tik tada, kai analizuojamos tipinės situacijos, puikiai žinomos rizikos ir duomenų nėra poreikio išversti į finansinę vertę [6].

1.5.2 Kiekybinė rizikos analizė

Kiekybinė analizė leidžia tiksliai apskaičiuoti riziką matematiniais modeliais, naudojant tikimybinius skaičiavimus, istorinius duomenis ir poveikio dydžius pinigine išraiška. Pagal A.Survilą, „tikimybiniai modeliai yra pagrindinė priemonė kiekybiniam rizikos vertinimui atlikti“ [9], o tikimybė „gali būti įvertinta skaičiumi nuo 0 iki 1 arba procentais nuo 0 iki 100 proc“[9]. Šis metodas suteikia didžiausią tikslumą, tačiau jam atlikti reikalingi ganėtinai sudėtingi duomenys, įrankiai, ištekliai, kaip:

- Istoriniai incidentų duomenys
- Žalos statistika
- Matematiniai įvertinimo įrankiai

- Kompetentingi specialistai

A.Survila taip pat aiškiai nurodo, kad kiekybinės analizės rezultatai turi būti atlikti vieni iš pirmųjų, nes – „Kokybinis grėsmių rangavimas turi būti grindžiamas kiekybinės analizės rezultatais“ [9]. Tai reiškia, kad kiekviena kokybinė išvada turėtų turėti duomenimis grįstą logiką.

1.5.3 Mišri rizikos analizė

Mišrioji analizė sujungia abu metodus, jų privalumus, dažniausiai naudojama tada, kai:

- Organizacija turi dalį kiekybinių duomenų,
- Organizacijai nepakanka turimos informacijos atlikti pilną kiekybinį skaičiavimą,
- Norima didesnio tikslumo, nei leidžia kokybinė analizė.

ISO/IEC 27005 praktikoje mirši analizė yra dažniausias pasirinkimas, o ypač mažose ar vidutinėse organizacijose, kuriuose rizikų poveikis gali būti įvertintas finansine išraiška, kaip BDAR bauda už netinkamą klientų duomenų tvarkymą, tačiau tikimybės įvertinimas išlieka kokybinis. A.Survila patvirtina šį požiūrį nurodydamas, kad realiame rizikos vertinime galima taikyti ir kokybinius, ir kiekybinius metodus kartu ir kad jie turi papildyti vienas kitą pagal duomenų kiekį bei tikslumą[9].

2 lentelė. Rizikos analizės tipų palyginimas pagal A.Survila[9]

(Sudaryta autoriaus remiantis A.Survila [9])

Analizės tipas	**Aprašymas**	**Citata iš šaltinio**	**Tinka kam?**
Kokybinis	Rizika vertinama žodinėmis kategorijomis	„Kokybiniai metodai lengviau apibrėžiami ir reikalauja mažiau laiko, pinigų ir patirties“ [9]	Mažoms įmonėms, kurios turi ribotus resursus.
Kiekybinis	Rizika apskaičiuojama matematiškai, remiantis tikimybėmis ir padariniais	„Tikimybiniai modeliai yra pagrindinė priemonė kiekybiniam rizikos vertinimui atlikti„ [9]	Didelėms įmonėms ir organizacijoms, turinčioms įvairių duomenų, kaip incidentų statistika ir tt.
Mišri	Derinami žodiniai ir	Kiekviena grėsmė	Mažoms ar vidutinėms

Analizės tipas	Aprašymas	Citata iš šaltinio	Tinka kam?
	skaitiniai vertinimai	analizuojama pagal jos pasireiškimo tikimybę (realų dažnį) ir padarinių apimtį. „ [9]	įmonėms, turinčioms mišrią IT infrastruktūrą.

Apibendrinant rizikos analizės metodų teorines įžvalgas, galima matyti, kad ISO/IEC 27005 nereglamentuoja vieno privalomo metodo, o akcentuoja nuoseklų, bei pagrįsta pasirinkimą pagal turimus įmonės duomenis, brandą ir tikslus. A.Survila pažymi, kad kokybinė analizė yra patraukli, nes „ Kokybiniai metodai lengviau apibrėžiami ir reikalauja mažiau laiko, pinigų ir patirties“ [9]. Tokio metodo ribotumas atsiskleidžia ten, kur būtinas tikslesnis padarinių įvertinimas. Kiekybinė analizė suteikia didesnį tikslumą, nes „Tikimybiniai modeliai yra pagrindinė priemonė kiekybiniam rizikos vertinimui atlikti“ [9], bet norint jį atlikti reikalingi duomenys, kurių mažos įmonės dažnai neturi. Taip pat nurodoma, kad taikymo metodai neturi būti supriešinami, „Kokybinės grėsmių rangavimas turi būti grindžiamas kiekybinės analizės rezultatais“ [9], kitaip tariant, metodai papildo vienas kitą ir leidžia sumažinti subjektyvumą vertinime.

Mišrus metodas tampa labiau tinkamu pasirinkimu, nes, kaip rašo Survila, mišrioje analizėje „Kiekviena grėsmė analizuojama pagal jos pasireiškimo tikimybė (realų dažnį) ir padarinių apimtį“ [9], todėl įmonė gali tiksliau vertintis tuos rizikos aspektus, kurie turi skaitinių duomenų ir kartu įtraukti kokybinį vertinimą ten, kur tiksliai apskaičiuoti to neįmanoma.

Analizuojant rizikų vertinimo metodų tinkamumą mažai žemės ūkio įmonei matoma, kad įmonė neturi pakankamai istorinių incidentų duomenų, todėl pilnai kiekybinio rizikos vertinimo atlikti nėra galimybės. Kita vertus, dalies rizikų poveikis gali būti apibūdinamas ir finansiniais terminais, kaip kasos neveikimo nuostoliai, duomenų praradimo ir vėliau jų atkūrimo kaštai, taip pat galimos baudos dėl BDAR pažeidimų. Tačiau, šie dydžiai dažnai yra apytiksliai ir priklauso nuo konkrečių aplinkybių. Dėl to šiame darbe tinkamiausias laikomas kokybinis rizikų vertinimas, o kur įmanoma pateikiami galimų finansinių pasekmių pavyzdžiai. Toks sprendimas leidžia atlikti rizikos vertinimą esant ribotiems duomenimis ir kartu išlaikyti ryši su realiais įmonės patiriamais nuostoliais.

1.5.4 Rizikų vertinimo kriterijai

Rizikų vertinimo kriterijai apibrėžia tam tikras ribas, pagal kurias įmonė ar organizacija gali nuspręsti, kokios rizikos yra priimtinos, o kurias būtina mažinti. ISO/IEC 27005 pateikia aiškia rizikos valdymo struktūrą, kuri leidžia apibrėžti šituos kriterijus dar prieš atliekant rizikos analizę.

Mokslinėje literatūroje pabrėžiama, kad ISS 27005 standartas yra vienas tiksliausias rizikos procesus apibrėžiančių standartų: „ ISO 27005 provides more accurate deifinitions fore ach stage of the ISRA process“ [10]. Tai reiškia, kad standartas suteikia aiškų pagrindą kriterijams nustatyti ir taip užtikrinti vertinimo nuoseklumą.

Taip pat rizikos vertinimas ISO 27005 suprantamas, kaip analizės palyginimas su iš anksto nustatytais kriterijais, siekiant nuspręsti dėl rizikos reikšmingumo, moksliniame straipsnyje, L.Pan ir A.Tomlinson tai patvirtina: „Risk evaluation is the process of comparing the results of risk analysis with risk criteria do determine whether the risk and/ori ts magnitude is acceptable or tolerable“ [10]. Todėl kriterijų nebuvimas lemią netinkamą vertinimą, o jų nusistatymas užtikrina, kad vertinimas bus atliekamas objektyviai, vienodais sprendimais organizacijos mastu.

ISO/IEC 27005 metodika dažnai siejama ir su ISO 31000, kuris detaliai paaiškina rizikos valdymo principus. Catherine Everett savo moksliniame leidinyje nurodo, kad ISO 27005 pateikia konkretesnes gaires standartų taikymui informacijos saugos srityje: „ISO 27005 provides detailed guidance for applying risk management within information security“ [11]. Tai, taipogi patvirtina, kad kriterijų sistema yra standartų pagrindas, kuris leidžia įmonės ar organizacijoms nusistatyti ribas tarp priimtinų ir nepriimtinų rizikų.

Praktikoje rizikų vertinimo kriterijai dažniausiai apima rizikos apetitą, rizikos toleranciją, priimtiną rizikos lygį ir nepriimtiną rizikos lygį. Rizikos apetitas parodo, kiek rizikos organizacija yra pasirengusi priimti. Šis aspektas laikomas būtinu pradiniam rizikos vertinimo etapui, nes, kaip teigiama mokslinėje literatūroje: „risk managers play a crucial role in helping organisations understand both their own risk tolerance and risk appetite – a necessary precursor before any other work in this area can begin“ [11]. Rizikos tolerancija apibrėžia ribas, nuo kurių rizika tampa nebepriimtina. Priimtinas rizikos lygis reiškia, kad rizika yra sumažinta iki tokio lygio, kuriam valdyti pakanka minimalių priemonių, tuo tarpu nepriimtinas lygis reikalauja nedelsiant imtis veiksmų.

NKSC vertinimai rodo, kad mažos ir vidutinės įmonės dažnai susiduria su ribotais ištekliais, pasenusia programine įranga ir silpnais vidaus procesais, o tai lemia didesnį pažeidžiamumą. Kaip pažymi NKSC, „Didelė dalis MVĮ labai mažai investuoja į kibernetinį saugumą, todėl jų sistemose yra daug pažeidžiamumų“[12]. Dėl šios priežasties rizikų vertinimo kriterijų nustatymas tampa esminis, nes leidžia MVĮ susidėlioti prioritetines rizikas ir nukreipti ribotus išteklius ten, kur poveikis būtų pats didžiausias.

Norint tinkamai suprasti, kaip rizikų vertinimo kriterijai taikomi praktikoje, būtina juos susisteminti ir pateikti struktūruotai. Toliau pateikta lentelė apibendrina pagrindinius rizikos

kriterijus, rizikos apetitą, rizikos toleranciją, priimtiną ir nepriimtiną rizikos lygius, paaiškina kokia jų praktinė reikšmė mažoms ar vidutinėms įmonėms.

3 lentelė. Rizikų vertinimo kriterijai ir jų praktinės reikšmė mažoms ir vidutinėms įmonėms (Sudaryta autoriaus remiantis NKSC pateikiamomis rekomendacijomis)

Kriterijus	Apibūdinimas	Aprašyta praktinė reikšmė
Rizikos apetitas	Lygis, kurį įmonė nori toleruoti.	Mažos ir vidutinės įmonės dėl ribotų išteklių dažniausiai pasirenka žemą rizikos apetitą, nes net ir menki incidentai gali sukelti itin didelius finansinius nuostolius.
Rizikos tolerancija	Riba, prieš pradedant taikyti priemones	Pagal NKSC, neapsaugotos darbo stotys ar pasenusi įranga gali viršyti tolerancijos ribas ir būti laikoma aukšta rizika.
Priimtinas rizikos lygis	Lygis sumažinamas tiek, kad tampa nebereikšmingas	Priimtinas rizikos lygis siejamas su rizika, kuriai pakanka taikyti minimalų stebėjimą ar priežiūrą, kaip antivirusinė ar atsarginės kopijos
Nepriimtinas rizikos lygis	Viršijamos tolerancijos ribos ir pradedami veiksmai	NKSC incidentų klasifikacija nurodo, kad didelio poveikio rizika laikoma tik tada, kai sutrikimas yra tęsiasi daugiau nei 2h ir yra pažeidžiamas konfidencialumas.

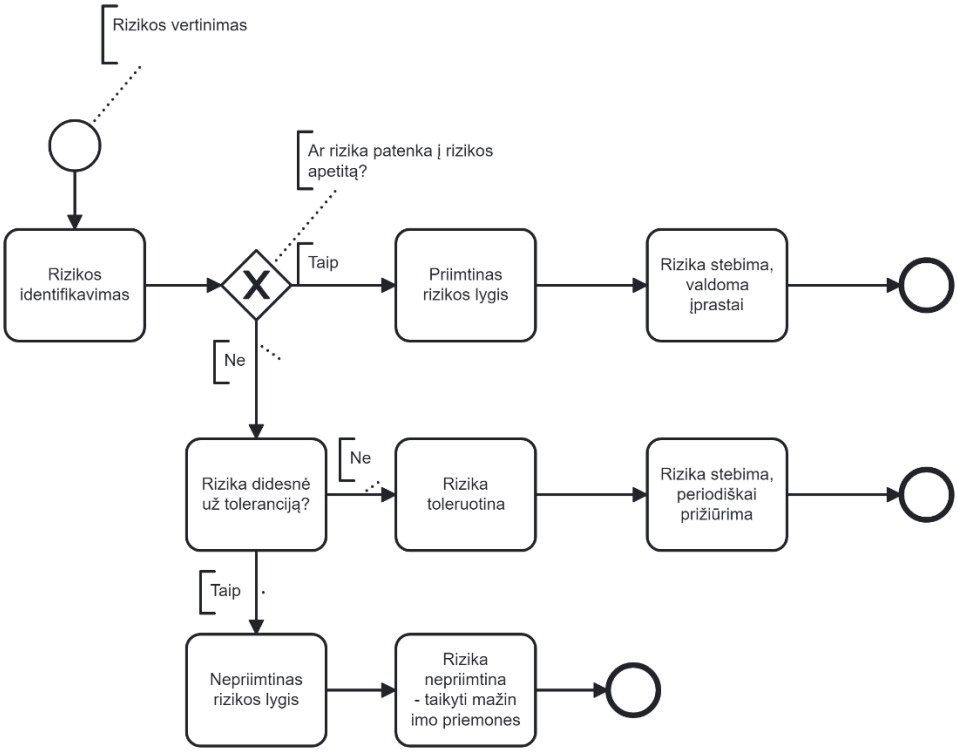
Galima teigti, kad visi rizikų vertinimo kriterijai leidžia paprasčiau suprasti, kokias ir kiek rizikų gali toleruoti mažos ar vidutinės įmonės, kada rizika jau tampa tokia didelė, kad būtina ją pradėti valdyti aktyviai. Pateiktoje lentelėje matoma, kad rizikos apetitas vienaip ar kitaip nusako įmonės dydį ir finansinį pajėgumą rizikos atžvilgiu, rizikos tolerancija padeda nusistatyti ribas. Priimtinos ir nepriimtinos rizikos lygiai leidžia atskirti, kada rizikos gali būti stebimos, o kada reikalinga imtis veiksmų. Visi šie kriterijai yra aktualūs mažoms įmonėms, nes joms labai svarbu tinkamai nusistatyti prioritetus, kurie efektyviai leistų naudoti turimus resursus.

Kadangi rizikų vertinimo kriterijai sudaro pagrindą sprendimų priėmimui, natūralu juos perkelti į procesinį modelį. Todėl toliau pateikiama BPMN schema iliustruoja, kaip organizacija praktiškai taiko rizikos apetitą, tolerancijos ribas ir priimtino ar nepriimtino lygio nustatymą rizikos

vertinimo procese. Schema parodo, kokiais etapais vadovaujantis priimami sprendimai dėl rizikos lygio ir kokie veiksmai atliekami, kai nustatytos ribos yra viršijamos.

3 pav. Rizikos kriterijų taikymo ir vertinimo BPMN schema sudaryta remiantis NKSC ataskaita[12].

(Sudaryta autoriaus remiantis NKSC rekomendacijomis)



Galima teigti, kad rizikų vertinimo kriterijų taikymas ypač svarbus mažoms ir vidutinėms įmonėms, nes jie padeda aiškiai atskirti toleruotinas rizikas nuo tų, kurios gali sukelti reikšmingų padarinių. Aiškiai nustatyti kriterijai leidžia nuosekliai vertinti rizikas ir priimti pagrįstus sprendimus dėl jų valdymo. Dėl ribotų išteklių MVĮ privalo tinkamai dėlioti prioritetus, todėl rizikos apetito, tolerancijos ir priimtino rizikos lygio nustatymas tampa praktiniu įrankiu, padedančiu efektyviai paskirstyti resursus. Remiantis nustatytais kriterijais galima atlikti rizikos lygio nustatymą ir sudaryti rizikos matricą, kuri leidžia įvertinti tikimybę ir poveikį bei priimti sprendimus dėl rizikos valdymo priemonių taikymo.

1.5.5 Rizikos lygio nustatymas ir rizikos matrica

Rizikos lygio nusistatymas yra vienas svarbiausiu rizikos vertinimo etapų. Rizikos vertinimas leidžia tinkamai įvertinti, kokią įtaką turi konkretus incidentas organizacijai, kokia tikimybė, kad incidentas pasireikš. ISO 27005 standartas sako, kad rizikos lygis nustatomas

vertinant tikimybės ir pasekmių arba poveikio kombinaciją [6]. Toks procesas yra labai svarbus mažoms ar vidutinėms įmonėms, joms turint ribotus išteklius, aiškiai yra identifikuojamos prioritetinės rizikos, bei jų valdymo kryptis. A. Survila rizikos vertinimą apibrėžia, kaip: „sisteminis (žingsnis po žingsnio) procesas, skirtas nustatyti grėsmės pasireiškimo tikimybę ir jos sukeltus padarinius“[9]. Ši mintis sutampa ir su ISO/IEC 27005 logika [6], kuri taip pat teikia, kad rizika atsiranda tik tada, kai vertinami du objektai, tai tikimybė ir poveikis.

Rizikos apskaičiavimo principas

Nors ISO/IEC 27005 rekomenduoja vertinti riziką pagal tikimybę ir poveikį, pats standartas nepateikia vienos konkrečios formulės. Todėl praktikoje dažniausiai taikomas dviejų komponentų modelis, kai rizika suprantama kaip tikimybės ir padarinių sąveika. Tokį principą puikiai atitinka A. Survilos pateikiamas rizikos apibrėžimas bei formulė.

Survila riziką nusako taip:

„Rizika yra tikimybė įvykti įvykiui, padauginta iš jau įvykusio įvykio padarinių“[9]

Tai yra aiški dviejų komponentų formulė, naudojama tiek ekstremalių situacijų valdyme, tiek lengvai pritaikoma informacinių sistemų saugos kontekste:

R = Tikimybė × Padariniai

Survila taip pat pateikia išplėstinę rizikos lygtį, naudojamą išsamiai rizikos analizei:

R = Hz × Vu × Cq

kur:

- **Hz** – grėsmės tikimybė,
- **Vu** – pažeidžiamumo lygis,
- **Cq** – pasekmių dydis (padariniai)[9].

Kadangi informacinių sistemų saugos analizėje dažniausiai vertinami du komponentai – tikimybė ir poveikis – Survilos formulė yra visiškai tinkama mažoms ir vidutinėms įmonėms, kur detalūs kiekybiniai duomenys dažniausiai nėra prieinami.

Tikimybės nustatymas

A.Survila aprašo aiškiai tikimybės vertinimo pavyzdį, kuriame tikimybės vertinimas, kaip „tikėtina“ susiejamas su tikimybe procentaliai [9] ir visa tai galima pritaikyti informacinių sistemų ar kitų objektų rizikų vertinimui.

4 lentelė. Tikimybės kokybinio vertinimo pavyzdys pagal A.Survila [9]

(Sudaryta autoriaus pagal A.Survilos vertinimo pavyzdžius)

Tikimybės kokybinis vertinimas	Kiekybinis apibūdinimas
Neabejotina	Daugiau, nei 99 % tikimybė, kad įvyks
Tikėtina	50-99 %
Galima	5-49 %
Netikėtina	2-5 %
Reta	1-2 %
Labai reta	Mažiau, nei 1 %

Pagal šį modelį įmonė gali aiškiai suprasti ir susiskirstyti rizikas, pagal tikimybės lygį bei pasirinkti tinkamiausią priemonę rizikai mažinti.

Rizikos poveikio/pasekmės nusistatymas

Pagal ISO/IEC 27005 rekomendacijas, rizikos poveikis paprastai vertinamas pagal finansinę žalą, veiklos sutrikimus, reputacijos žalą, bei galimas teisines pasekmes. Šią logiką patvirtina ir NIST SP 800-30 metodika [8].

Tinkamai įvertinus tikimybę ir poveikį atskirai, galime juos sujungti į vieną bendrą vertinimą. Pagal ISO/IEC 27005, matome, kad rizika realiai suprantama tada, kai tikimybė vertinama kartu ir su pasekmių mastu. A.Survila taip pat pažymi, kad rizikos vertinimas yra grindžiamas tikimybe ir poveikiu, kad viską dar geriau ir lengviau suprasti yra taikoma rizikos matrica, kuria galime palyginti du rizikos komponentus [9].

Rizikos matrica

A. Survila plačiai aprašo rizikos matricos sudarymo principus ir parodo, kad tokia matrica leidžia struktūruotai palyginti pagrindinius rizikos komponentus, tai tikimybę ir poveikį. Autorius pabrėžia, kad rizikos matrica padeda nustatyti rizikų prioritetus, greitai išskirti labiausiai pavojingas rizikas ir pasirinkti tinkamiausias jų mažinimo priemones [9].

5 lentelė. Pavyzdinė rizikos matrica, pagal A.Survila [9].

(Sudaryta autoriaus pagal A.Survilos pateiktą pavyzdinę rizikos matricą)

Tikimybė ↓ Padariniai →	Labai maži	Maži	Vidutiniai	Dideli	Labai dideli
Labai didelė	C	B	B	A	A
Didelė	D	C	B	B	A
Vidutinė	D	D	C	B	A
Maža	D	D	C	C	B
Labai maža	D	D	D	C	C

Tipai: A, B, C, D atitinka rizikos tipus.

- A – Labai didelė rizika, vykdomi neatidėliotini veiksmai,
- B – Didelė rizika, priimami skubūs sprendimai ir veiksmai,
- C – Vidutinė rizika, planuojami būsimi veiksmai,
- D – Maža rizika, vykdoma stebėsena.

Rizikos matricos taikymas įmonei palengvina aiškiai nusistatyti kokios rizikos yra kritinės, o kurios reikalaus daugiau greitų veiksmų, o kurias tiesiog galime stebėti ar ruoštis joms. Matrica suteikia pagrindą priimti sprendimus dėl saugos ir resursų priemonių paskirstymo. Tačiau vien tik rizikos nustatyto nepakanka, įmonė turi taip pat įsivertinti ir teisinius, ir nacionalinius reikalavimus kuriuose yra reglamentuojama, kaip tinkamai turi būti valdomos rizikos, kokias priemones privalu taikyti. Įmonei pagrindą sudaro BDAR ir NKSC gairės [13], [15,] taip pat ir tarptautiniai saugos standartai, kurie apibrėžia, koks yra minimalus saugos lygis, kurio privalu laikytis mažai ar vidutiniai įmonei.

1.6 Teisinis pagrindas – BDAR, NKSC, NIST

Informacijos saugos valdymas įmonėje dažnai priklauso ne vien tik nuo vidinių procesų ar taikomų techninių priemonių, bet ir nuo išorės teisės reguliavimo. Atliekant rizikos vertinama, taip pat turi būti atitinkamai atsižvelgta ir į nacionalinius bei tarptautinius teisės aktus, kurie aprašo, kokie minimalūs reikalavimai yra išskirti įmonės saugai bei kokios rekomendacijos gerajai praktikai. Mažoms ir vidutinės įmonės šie teisiniai dokumentai yra labai svarbūs, nes būtent tai padeda suprasti, kokio tipo priemones reikalinga pritaikyti esant ribotiems ištekliams.

1.6.1 Bendrasis duomenų apsaugos reglamentas – BDAR

BDAR nustato teisinius reikalavimus, kurie tiesiogiai formuoja informacijos saugos valdymą organizacijose. Reglamente įtvirtinti principai yra pagrindas visoms techninėms ir organizacinėms saugumo priemonėms, todėl jų analizė leidžia suprasti, kokius minimalius saugos lūkesčius turi atitikti mažos ar vidutinės įmonės.

Vienas svarbiausių BDAR principų, tai teisėtumas, sąžiningumas ir skaidrumas. Reglamente nurodoma, kad duomenys turi būti tvarkomi „duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas)“ [13]. Šis principas reikalauja, kad organizacija ne tik turėtų aiškius duomenų tvarkymo procesus, bet ir gebėtų juos pagrįsti. Analitiškai vertinant, tai reiškia, kad net ir techninės informacijos saugos priemonės, kaip prieigos kontrolė ir šifravimas yra tiesiogiai susietos su skaidrumo įgyvendinimu, nes BDAR numato atsakomybės įrodymą.

Kitas svarbus aspektas, tai duomenų kiekio mažinimas. BDAR pabrėžia, kad turi būti tvarkomi tik tie duomenys, kurie būtini tikslo pasiekimui: „adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų kiekio mažinimo principas)“ [13]. Šis principas yra vienas iš pagrindinių rizikos mažinimo elementų, nes kuo daugiau duomenų organizacija sukaupia, tuo didesnio masto incidentas gali įvykti. Praktikoje mažos įmonės dažnai pažeidžia šį principą, nes kaupia perteklinius klientų ir darbuotojų duomenis, o tai didina kibernetinių incidentų poveikį.

Svarbus BDAR principas – tikslumo reikalavimas. Reglamento 5 – straipsnyje, 1 – dalyje nurodoma, kad duomenys turi būti „tikslūs ir prireikus atnaujinami“ [13]. Iš informacijos saugos perspektyvos, netikslūs duomenys gali lemti klaidingą identifikavimą, teisėtų naudotojų blokavimą ar net neteisėtą prieigą, jei, kaip pavyzdys prieigos teisės yra suteiktos nebedirbantiems asmenims. Analizuojant mažų įmonių praktiką, pastebima, kad mažos įmonės dažnai neturi procesų, skirtų reguliariam duomenų tikslinimui, dėl to rizika tik išauga.

Vienas iš kritinių BDAR elementų informacinei saugai – vientisumo ir konfidencialumo principas. Jame nustatyta, kad duomenys: „tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo“ [13]. Tai yra tiesioginis teisinis pagrindas taikyti tokias saugos priemones kaip šifravimas, atsarginės kopijos, prieigos kontrolė ir incidentų valdymo procesai. Analitiniu požiūriu, šis punktas sujungia teisinį reguliavimą su techniniais ISO/IEC 27001 reikalavimais.

Atskaitomybės principas yra vienas sudėtingiausių praktiniame taikyme, nes BDAR 5 str. 2d nurodo, kad: „Duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi 1 dalies, ir turi sugebėti įrodyti, kad jos laikomasi“ [13]. Tai reiškia, kad neužtenka įdiegti saugos priemonių, reikalinga turėti ir dokumentuotus procesus, įrodymus, politikos veikimo patvirtinimus. Mažos ar vidutinės įmonės dažniausiai patiria sunkumų būtent šioje srityje dėl ribotų savo resursų.

BDAR 32 straipsnis papildo principus ir įpareigoja organizacijas parinkti tinkamas technines ir organizacines priemones, atsižvelgiant į jų riziką, technologijų lygį ir įgyvendinimo kaštus [13]. Tai leidžia teigti, kad BDAR iš esmės naudoja rizikos pagrindu grįstą požiūrį, kuris suderinamas su ISO/IEC 27005 rizikų valdymo metodika. Taip pat, tame pačiame straipsnyje pateikiami konkretūs techniniai pavyzdžiai, kaip „pseudonimų suteikimą asmens duomenims ir jų šifravimą“ [13], bei reikalavimą užtikrinti sistemų „duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą“ [13].

Incidentų valdymo būtinybę pabrėžia BDAR 33–34 straipsniai. Reglamento 33 straipsnyje, 1 dalyje, pabrėžiama, kad priežiūros institucijai apie pažeidimą būtina pranešti „ne vėliau kaip per 72 valandas“ [13]. Tai reiškia, kad incidentų valdymas įmonei nėra tik pasirinktinė priemonė, tai teisiškai privalomas procesas, kurį ji turi užtikrinti. 34 straipsnyje 1 dalyje nurodoma, kad jei incidentas gali sukelti didelę žalą privačiam asmeniu, tad: „duomenų valdytojas nepagrįstai nedelsdamas praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui“ [13]. Analitiškai vertinant, tai įpareigoja organizacijas turėti ne tik techninį incidentų valdymą, bet ir komunikacijos planus bei atsakomybės paskirstymą, kas kam turim kokią informaciją pranešti.

Praktiškai BDAR principai mažos ūkio bendrovės atveju aiškiai atsispindi vaizdo stebėjimo srityje. Vaizdo įrašai laikomi asmens duomenimis, todėl įmonė turi nusistatyti aiškų įrašų saugojimo terminą, pagrįsta kokiu tikslu tai laikoma ir užtikrinti, kad įrašai būtų perrašomi pasibaigus nustatytam laikotarpiui. Taip pat turi būti apibrėžta, kas konkrečiai turi teisės peržiūrėti ir eksportuoti įrašus, bei užtikrinti, kad prieiga prie jų būtų suteikiama pagal būtinybės principą. Siekiant atskaitomybės, reikalinga fiksuoti įrašuose, kas peržiūrėjo ar juos eksportavo, tokiu būdu prireikus galima nustatyti, kas naudojosi įrašais ir pagrįsti tam veiksmus ar incidentą.

Apibendrinant, BDAR principai sudaro sisteminį pagrindą informacijos saugos valdymui ir glaudžiai siejasi su ISO/IEC 27001 bei ISO/IEC 27005 standartų struktūra. Mažoms ir vidutinėms įmonėms šie principai yra ypač reikšmingi, nes jie įpareigoja diegti procesus, kurie padeda valdyti rizikas, apsaugoti duomenis ir užtikrinti atitiktį teisės aktams. Analizė rodo, kad BDAR akcentuoja rizikos pagrindu grindžiamą saugos valdymą bei suteikia aiškią kryptį, kokios priemonės privalo būti diegiamos praktikoje.

1.6.2 Nacionalinio kibernetinio saugumo centro rekomendacijos

Nacionalinis kibernetinio saugumo centras yra pagrindinė institucija Lietuvoje, atsakinga už kibernetinio saugumo politikų įgyvendinimą ir praktinių gairių rengimą įvairaus tipo organizacijoms. Nacionalinio kibernetinio saugumo centro 2024–2025 m. rekomendacijose pateikiama metodika [15], leidžianti organizacijoms savarankiškai įsivertinti savo brandą, nusistatyti reikiamą saugumo lygį, bei pasirinkti atitinkamas technines ir organizacines priemones. Dokumente akcentuojama, kad kibernetinio saugumo užtikrinimas turi būti pritaikytas pagal rizikas ir organizacijos pajėgumus.

Svarbu tai, kad NKSC metodika yra pritaikyta būtent mažoms ir vidutinėms įmonėms. 2024 m. ataskaitoje rašoma, kad dauguma mažų ir vidutinių įmonių Lietuvoje susiduria su itin ribotais ištekliais ir dažnai nėra tinkamai pajėgios įdiegti brangių, bei sudėtingų saugumo sprendimų. Kaip teigiama NKSC grėsmių vertinime, „Didelė dalis MVĮ labai mažai investuoja į kibernetinį saugumą, todėl jų sistemose yra daug pažeidžiamumų.“ [12].
Tokia įžvalga aiškiai parodo, kodėl MVĮ yra vienas labiausiai pažeidžiamų sektorių ir kodėl joms reikalinga turėti aiškias, paprastas bei įgyvendinamas priemones.

Kodėl MVĮ labiausiai pažeidžiamos (NKSC analizė)

Remiantis NKSC grėsmių vertinimu [12], MVĮ pažeidžiamumą lemia šie veiksniai:

- Riboti finansiniai ir žmogiškieji resursai,
- IT saugos specialistų trūkumas,
- Didelė priklausomybė nuo trečiųjų šalių paslaugų ir įrangos,
- Pasenusi arba neprižiūrima IT infrastruktūra,

Būtent šie veiksniai ir sudaro tinkamas sąlygas kibernetinėms atakoms, mažose ir vidutinėse įmonėse.

Dėl visų, šių veiksnių, MVĮ saugumo stiprinimas turi būti paremtas efektyviausiomis ir lengviausiai įgyvendinamomis kontrolėmis.

Taip pat, Nacionalinis Kibernetinis Saugumo Centras, savo rekomendacijas tiesiogiai grindžia tarptautiniu CIS Controls modeliu, tai plačiai pripažintas informacijos saugos kontrolės rinkinys. Kaip nurodo Dr. Vilius CIS Controls V7 dokumente, „CIS Controls metodas, kartu su CIS Saugumo Konfigūracijų šablonais (angl. CIS Benchmarks), yra itin vertingi įrankiai visiems, kurie siekia užtikrinti savo informacinių instrumentų ir sistemų apsaugą nuo kibernetinių grėsmių“ [14].

NKSC aktyviai rekomenduoja CIS Controls rinkinį, Lietuvos organizacijoms kaip standartizuotas, aiškias ir tinkamas praktines saugos gaires, bei metodikas MVĮ aplinkai.

CIS Controls suskirstytos į tris grupes, tai bazines, kertinės ir organizacinės ir šis suskirstymas tapo NKSC metodikos pagrindu [14]:

- Bazinės kontrolės (1–6) – techninės įrangos inventorizacija, pažeidžiamumų valdymas, saugios konfigūracijos, antivirusinė apsauga.
- Kertinės kontrolės (7–16) – el. pašto sauga, tinklo sauga, duomenų apsauga, audito žurnalai.
- Organizacinės kontrolės (17–20) – mokymai, incidentų valdymas, programų sauga, įsilaužimo testai.

CIS Controls dokumentas aiškiai aprašo šių priemonių vertę. Kaip, pažeidžiamumų valdymas aprašomas kaip būtinybė „Nuolat rinkti ir vertinti informaciją, susijusią su programinės įrangos pažeidžiamumu ir saugumo spragų ištaisymu“ [14].

Tai pažymi mažų ir vidutinių įmonių realybę, kur neatnaujintos sistemos tampa pagrindiniu įsilaužimų taikiniu.

NKSC metodikos reikšmė MVĮ

Lyginant NKSC rekomendacijas su CIS Controls struktūra, galima matyti, kad svarbiausias prioritetas, tai saugumo funkcijų įgyvendinimas, o ne visų įmanomų priemonių diegimas. NKSC dokumente[15], mažos ir vidutinės įmonės raginamos pasirinkti vieną iš trijų saugumo lygių (žalias, oranžinis, raudonas), kurie nustatomi pagal:

- Tvarkomų duomenų jautrumą,
- Kritinių funkcijų kiekį,
- Organizacijos brandą.

Toks modelio tipas leidžia MVĮ tinkamai planuoti saugos priemones, neprarandant kontrolės ir neviršijant finansinių galimybių ir įsipareigojimu.

- **Žalias lygis** reikalauja tik pagrindinių priemonių, tokių kaip turto inventorizacija, antivirusinė apsauga, bei reguliarūs atnaujinimai,
- **Oranžinis lygis** apima monitoringą, tinklo segmentavimą, incidentų valdymą,
- **Raudonas lygis** skirtas didesnėms organizacijoms, tvarkančioms kritinius duomenis ar teikiančioms viešąsias paslaugas.

Analizuojant pateiktus dokumentus matoma, kad NKSC metodikos mažoms įmonėms yra naudingos ir priimtinos dėl šių priežasčių:

- Aiškiai prioretizuojamos svarbiausios priemones, todėl MVĮ nereikia investuoti į visas 20 CIS kontrolės sričių.

- Pašalinama perteklinė biurokratija, pateikiant tik praktiškai įgyvendinamus žingsnius.
- Orientuojamasi į didžiausias rizikas mažinančias priemones, tokias kaip pažeidžiamumų valdymas bei atsarginės kopijos.
- Numatomos realios grėsmės MVĮ sektoriui, pavyzdžiui, ransomware, socialinė inžinerija ar pasenusi įranga.

NKSC grėsmių analizė aiškiai įvardija, kad dažniausia MVĮ pažeidimų priežastis yra ne technologijų trūkumas, bet tada, kai organizacija ar įmonė nesilaiko tinkamų saugos politikų, reguliariai nenaujina programinės įrangos, ar neturi tinkamo pažeidimų valdymo [12].

Atsižvengiant į NKSC dokumentus ir juose išdėstytus principus, galime matyti, kad kai kurios priemonės yra itin svarbios būtent mažoms ar vidutinėms įmonėms. Pateiktoje lentelėje apibendrintos NKSC siūlomos saugos priemonės, jų tikslai, praktinė nauda mažoms įmonėms.

6 lentelė. Rekomenduojamos saugos priemonės ir jų taikymo nauda MVĮ, pagal NKSC [12] (Sudaryta autoriaus remiantis NKSC pateiktomis rekomendacijomis)

Rekomendacija	NKSC tikslas	Pritaikymas MVĮ
IT turto inventorizacija	Visų įrenginių, programų ir paskyrų registravimas, nuolatinė stebėsena.	Leidžia matyti neautorizuotus įrenginius, sumažina atakų paviršių.
Pažeidžiamumo valdymas	Reguliarūs skenavimai, Programinės įrangos atnaujinimai.	Labiausiai kritinė kontrolė MVĮ, nes laiku neatnaujintos sistemos tampa pagrindiniu įsilaužimų taikiniu.
Apsauga nuo kenkėjiškų programų	Antivirusinės, elgsenos analizės sprendimai, el. pašto filtravimas.	Apsaugo nuo ransomware ir phishing atakų, kurios dominuoja MVĮ sektoriuje.
Prieigos kontrolė	Paskyrų inventorizacija, 2FA, administratoriaus paskyrų atskyrimas.	Mažina žmogiškųjų klaidų riziką, apsaugo kritines sistemas.
Duomenų sauga ir	Duomenų	Užtikrina BDAR atitiktį ir

Rekomendacija	NKSC tikslas	Pritaikymas MVĮ
šifravimas	klasifikavimas, šifravimas, VPN naudojimas, saugyklų apsauga.	apsaugo jautrią informaciją.
Atsarginės kopijos	Izoliuotos kopijos, testavimas kas ketvirtį, kelių kopijų palaikymas.	Kritiška priemonė apsisaugoti nuo ransomware ir įrenginių gedimų.
Tinklo sauga	Ugniasienės, tinklo segmentavimas, žurnalų rinkimas ir analizė.	Sumažinama įsilaužimo tikimybė.
Darbuotojų mokymai	Phishing, slaptažodžių higiena, incidentų pranešimai, socialinė inžinerija.	Didina organizacijos atsparumą, nes 80 % incidentų prasideda nuo žmogaus klaidos.

1.6.3 Nacionalinio standartų ir technologijų instituto – NIST gairės

Nacionalinio standartų ir technologijų instituto parengtos informacijos saugos gairės yra vienas svarbiausių tarptautinių šaltinių, naudojamų organizacijų rizikos valdymui. Nors NIST standartai Europos Sąjungoje nėra privalomi, jie plačiai taikomi kaip metodikos, padedančios užtikrinti brandų ir struktūruotą saugos valdymą. NIST SP 800-12 Rev.1 dokumente informacijos sauga apibrėžiama kaip informacijos ir informacinių sistemų apsauga nuo neautorizuotos prieigos, panaudojimo, atskleidimo, trikdymo, modifikavimo ar sunaikinimo, o pagrindinis saugos tikslas yra: „unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability“ [8].

Analizuojant dokumentą matyti, kad NIST saugą traktuoja ne kaip techninį priedą, o kaip bendrą valdymo procesą. Kaip ir teigiama metodikoje, saugos priemonės turi būti integruotos į visą organizacijos veiklos ciklą, o saugumo funkcijos privalo išlikti nuolatinė sistemos gyvavimo ciklo dalimi: „Providing effective information security requires a comprehensive approach that considers a variety of areas both within and outside of the information security field. This approach applies throughout the entire system life cycle“ [8].

Toks požiūris taip pat artimas ISO/IEC 27005 logikai, nes NIST irgi išskiria pagrindinius rizikos valdymo komponentus:

- Informacinių išteklių identifikavimą,
- Grėsmių ir pažeidžiamumų nustatymą,
- Rizikos įvertinimą,
- Rizikos mažinimo priemonių parinkimą,
- Likutinės rizikos stebėseną [8].

NIST dokumentas pateikia ne tik principus, bet ir konkrečius techninių ir organizacinių kontrolės priemonių pavyzdžius, kaip prieigos kontrolę, tinklo saugą, atsarginių kopijų politiką, incidentų valdymo procesus, vartotojų mokymus. Dėl tokios struktūros NIST gairės itin vertingos mažoms organizacijoms, kurios neturi išteklių sudėtingoms sistemoms diegti, tačiau nori turėti aiškų saugos valdymo pagrindą.

Taip pat svarbu tai, kad NIST susieja saugos priemones su konfidencialumo, vientisumo ir prieinamumo CIA modeliu. CIA modelis padeda suprasti, kuri kontrolė kokį saugos aspektą stiprina, pavyzdžiui: šifravimas saugo konfidencialumą, registrų analizė didina vientisumą, o atsarginės kopijos didina prieinamumą.

Dėl tokių priežasčių NIST gairės dažnu atveju naudojamos, kaip papildoma metodika šalia ISO/IEC ir NKSC rekomendacijų, ypač MVĮ kontekste. Jos padeda įmonėms suprasti, kaip derinti techninius sprendimus su organizacinėmis politikomis, bei, kad sauga nėra vien tik technologijų rinkinys, bet nuolatinis procesas reikalaujantis valdymo, priežiūros ir nuolatinio tobulinimo[8].

Apibendrinant, MVĮ segmentui NIST gairės yra naudingos dėl trijų priežasčių:

- Jos pateikia paprastą, bet struktūruotą saugos valdymo modelį,
- Aiškiai parodo, kaip derinti technines ir organizacines priemones,
- Suteikia praktiškus kontrolės pavyzdžius, kurie padeda MVĮ pasirinkti sprendimus pagal jų galimybes ir brandą.

1.7 Teorinio skyriaus santrauka

Teorinėje dalyje buvo išnagrinėti pagrindiniai informacijos saugos valdymo modeliai ir rizikos analizės principai, kurie bus pagrindas mažos žemės ūkio įmonės būklės vertinimui. ISO/IEC 27001 ir ISO/IEC 27005 standartų analizė parodė, kad informacijos sauga turi būti suprantama, kaip nuoseklus ir tęstinis procesas, apimantis, ne tik techninius sprendimus, bet ir organizacinius aspektus, tokius, kaip politikų kūrimas, atsakomybių suskirstymas, bei rizikų vertinimas. ISO/IEC 27001 standartas pateikia struktūruotą valdymo sistemą, o ISO 27005 nustato metodikas, kaip tinkamai ir praktiškai identifikuoti, analizuoti, bei valdyti rizikas.

Pati rizikos samprata paremta turto, grėsme ir pažeidžiamumo sąveika ir tai leidžia įmonei lengviau suprasti, dėl kokių priežasčių formuojasi realios rizikos. Analizuoti rizikos vertinimo

metodai, kaip kokybinis, kiekybinis ir mišrus, suteikia galimybę pasirinkti tinkamiausią vertinimo būdą, pagal turimus duomenis, bei organizacijos brandą. Remiantis literatūra, mažoms įmonėms labiausiai tinkamas yra kokybinis vertinimas, dėl to, kad jis nereikalauja didelio istorinių duomenų kiekio ir leidžia praktiškai įvertinti galimą poveikį, įskaitant finansines pasekmes.

Teisės aktų analizė, kaip BDAR parodė, kad informacijos saugumas mažoms ir vidutinėms įmonėms nėra pasirenkamas procesas, reglamentas įpareigoja įmones taikyti tinkamas technines ir organizacines priemones, kad užtikrinti vientisumą, konfidencialumą, bei prieinamumą, tuo pačiu gebėti pranešti apie įvykius per 72 valandas. Tai parodo, kad incidentų valdymo procesas įmonei nėra tik papildoma priemonė, tai yra teisinė pareiga.

NKSC rekomendacijų analizė taip pat parodė, kad mažos ir vidutinės įmonės segmentas pasižymi itin ribotais ištekliais, todėl saugos priemonės turi būti paprastos, lengvai diegiamos ir orientuotos į didžiausią rizikos mažinimo efektą. NKSC siūlomos metodikos remiasi CIS Controls modeliu, kas suteikia struktūruotą priemonių rinkinį pritaikyta MVĮ.

NIST SP 800-12 gairės papildė analizę tuo, kad jose aiškiai apibrėžiama saugumo priemonių integracija į visą sistemos gyvavimo ciklą, NIST pateikia ne vien tik principus, bet ir praktines gaires, kaip tinkamai suderinti technines ir organizacines priemones. Taip pat NIST kalba apie CIA modelį, kuris padeda paprasčiau suprasti, kuri priemonė stiprina konfidencialumą, vientisumą ir prieinamumą. Toks modelis itin naudingas MVĮ, nes padeda tinkamai suprasti kontrolės priemonių paskirtį.

Apibendrinant, teorinėje dalyje suformuotas teorinis pagrindas mažos žemės ūkio įmonės informacijos saugai vertinti. Standartų, teisinių reikalavimų ir nacionalinių gairių taikymas leidžia nuosekliai vertinti esamą infrastruktūrą, bei pagrindines rizikas. Toks teorinis pagrindas padeda nustatyti, kurios saugos priemonės yra tinkamai įdiegtos, kurios veikia nepakankamai ir kuriose srityse egzistuoja kontrolės spragos.

2 INFORMACINIŲ SISTEMŲ SAUGOS ANALIZĖ MAŽOJE ĮMONĖJE

Šiame skyriuje analizuojama įmonės informacinė aplinka, vertinant jau esamą informacijos saugos būklę, bei jos atitiktį gerosioms praktikoms ir tarptautinių standartų reikalavimams. Analizė atliekama remiantis aptartais standartais, kaip ISO/IEC 27001 ir ISO/IEC 27005, taip pat analizėje atsižvelgiama ir į įmonės anksčiau patirtus incidentus.

Pradžioje pateikiama įmonės veiklos, bei informacinių technologijų infrastruktūros apžvalga, vėliau analizuojama jau esama saugos situacija įmonėje, išskiriant jau taikomas technines, organizacines ir fizines saugos priemones, atsižvelgus tai nustatomi pagrindiniai saugos trūkumai. Remiantis analize, identifikuojamos pagrindinės informacinių sistemų grėsmės, trūkumai, pažeidžiamumai, kurie gali turėti įtakos įmonės veiklos tęstinumui.

Vėlesniuose skyreliuose atliekamas rizikų vertinimas, taikant pasirinktus metodus, bei sudaroma rizikos matrica kartu su rizikų registru. Pateikiamas rizikų valdymo priemonių planas, planas sudaromas atsižvelgiant į ISO/IEC 27001 kontrolės priemones. Skyriaus pabaigoje aptariami informacijos saugos stebėsenos aspektai.

2.1 Įmonės veiklos ir informacinės aplinkos aprašymas

Vadovaujantis smulkiojo ir vidutinio verslo praktikoje taikomais kriterijais, ši organizacija darbe priskiriama mažos įmonės kategorijai (iki 50 darbuotojų) [23], todėl šis pasirinkimas svarbus, kad saugos priemonės turi būti realistiškos mažos įmonės biudžetui ir kompetencijoms.

Nagrinėjama maža žemės ūkio įmonė, vykdanti veiklą fizinėje prekybos vietoje su sandėliavimo patalpomis. Įmonės veikla orientuota į prekybą, klientų aptarnavimą, prekių apskaitą ir tiekimo procesus, todėl kasdieną naudojamos informacinės sistemos, kaip kasos, darbo kompiuteriai, tinklo ir ryšio įranga, vaizdo stebėjimas, apsaugos sistemos.

Organizacinėje struktūroje išskiriami pagrindiniai funkciniai padaliniai, kaip administracija, finansai, apskaita, vadyba ir prekyba. Darbo vietos paskirstytos pagal funkcijas, prekybos patalpoje ir sandėlyje naudojamos darbo vietos prekių apskaitai, klientų aptarnavimui, administracijos ir finansų skyriuose – dokumentų valdymui, apskaitai, vidinei komunikacijai. Praktinėje dalyje daroma prielaida, kad organizacijoje naudojama 10-20 darbo vietų/paskyrų, įskaitant ir sezoninį poreikį, kad būtų realistiškai atspindėtas mažos įmonės veiklos mastas [23].

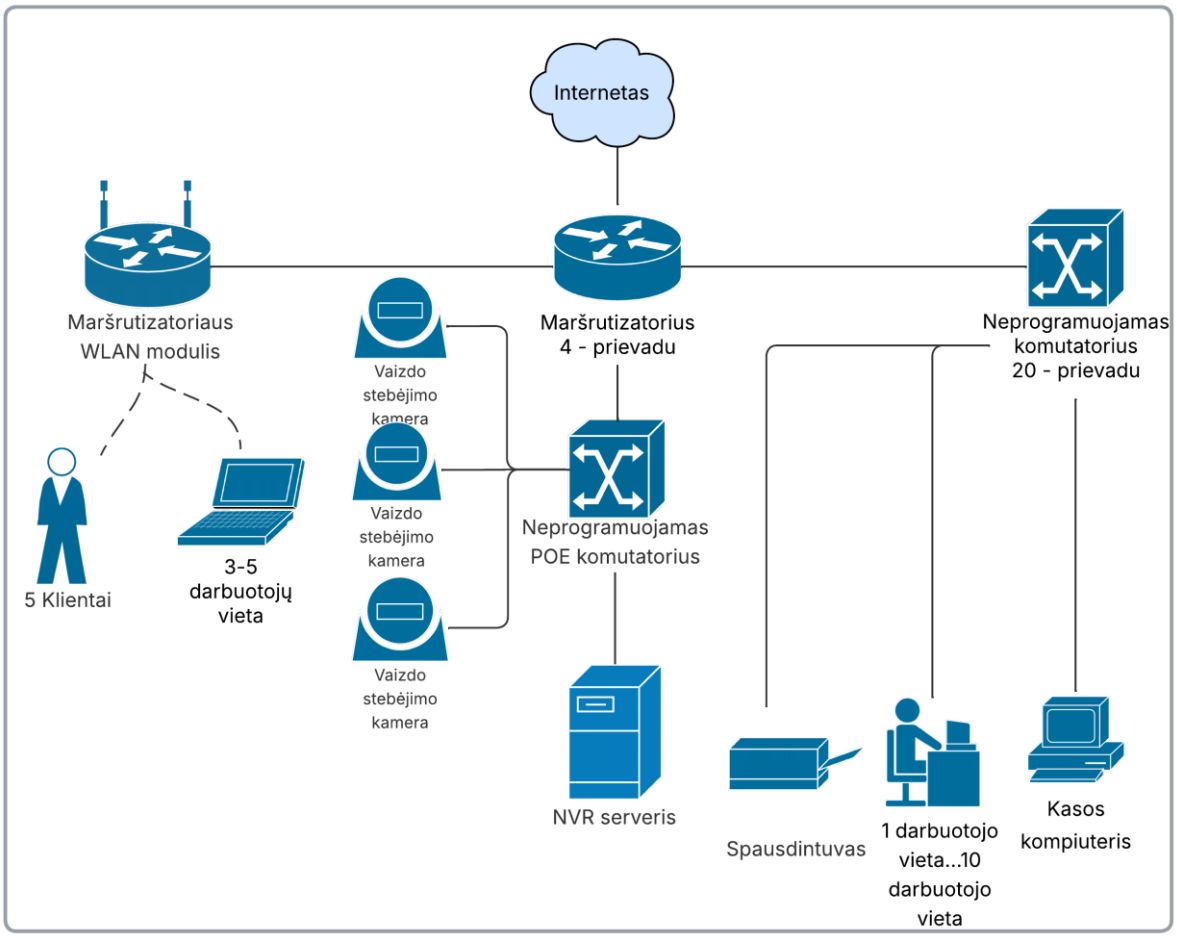
Pati įmonės veikla pasižymi sezoniškumu, piko metu klientų srautai stipriai išauga, todėl informacinių sistemų sutrikimai turi tiesioginį poveikį aptarnavimo greičiui, prekių apskaitai, bei veiklos tęstinumui. Dėl galimo didelio klientų srauto ir nuolatinio prekių judėjimo informacinių sistemų veikimo sutrikimai gali turėti itin stiprų tiesioginį poveikį įmonės veiklos tęstinumui, bei finansiniams rezultatams.

Įmonėje už administracinius sprendimus ir veiklos koordinavimą atsakingas vadovas – administracija. IT infrastruktūros priežiūra vykdoma mišriu būdu, kasdieniniai procesai atliekami įmonės viduje, pagal nustatytas taisykles, o sudėtingesni darbai, kaip tinklo, vaizdo stebėjimo ar saugos sistemų konfigūravimas periodiškai atliekamas išorinio IT specialisto.

Įmonė kiekvieną dieną naudoja kompiuterius su „Windows 11“ operacines sistema, kurie skirti kasos, administracinėms, bei pagalbinėms funkcijoms atlikti. Visi darbo kompiuteriai apsaugoti antivirusine programine įranga, prisijungimo slaptažodžiais, kurie užtikrina bazines saugos priemones. Įmonėje naudojamas miršus tinklas, tai laidinis LAN ir belaidis WLAN. Laidinis tinklas naudojamas pagrindinėms darbo vietoms ir infrastruktūros įrenginiams, kaip NVR serveris, spausdintuvas, kasos aparatas, o belaidis tinklas – mobilumui užtikrinti ir atskiroms naudotojų grupėms, kaip darbuotojų, svečių ar klientų prisijungimams. Tinklo atskyrimas yra minimalus, darbo ir svečių belaidžiai prisijungimai nėra segmentuoti, nenaudojamos jokios loginio atskyrimo priemonės, todėl padidėja neautorizuotos prieigos ir incidentų rizika. Toks supaprastintas sprendimas yra būdingas mažoms įmonėms ir tai riboja prieigų valdymą, srauto kontrolę, bei stebėseną.

4 pav. Mažos žemės ūkio įmonės IT infrastruktūros schema

(Sudaryta autoriaus)



Įmonės kompiuteriuose saugomi prekybos ir apskaitos duomenys, taip pat klientų asmens duomenys, įskaitant vardus, pavardes, telefonų numerius, asmens kodus ir kitą sąskaitų informaciją. Įmonė neturi bendros atsarginių kopijų darymo sistemos, todėl yra galimas duomenų praradimas, kuris galėtų reikšti tik itin stiprų veiklos sutrikdymą, ar net visišką prekybos sustabdymą. Kadangi įmonė tvarko klientų ir tiekėjų asmens duomenis, veikloje taikomas BDAR, dėl to informacijos saugos priemonės turi būti parenkamos taip, kad užtikrintų asmens duomenų konfidencialumą, vientisumą ir prieinamumą bei sumažintų asmens duomenų saugumo pažeidimų riziką.

Vaizdo apsaugą sudaro trys vaizdo stebėjimo kameros, iš kurių dvi įrengtos parduotuvės patalpose, o trečia sandėlyje. Viena kamera specifiškai nukreipta į pardavėjo darbo vietą siekiant užtikrinti veiklos kontrolę ir incidentų atsekamumą. Vaizdo įrašai saugomi lokaliame NVR serveryje, kurio atmintis išplėsta kas užtikrina galimybę peržiūrėti vaizdo įrašus, ilgesniu laikotarpiu, ypač atliekant inventorizaciją, ar tiriant galimus prekių trūkumus. Taip pat svarbu pažymėti, kad vaizdo įrašų saugojimo trukmė turi būti apibrėžta ir pagrįsta tikslu, todėl praktikoje reikalinga nusistatyti konkrečių įrašų saugojimo terminą ir taikyti automatinį perrašymą. Taip didesnė NVR talpa nei įprastai vertinama, kaip priemonė užtikrinti, kad per nustatytą laiką įrašai nebūtų perrašyti per anksti, dėl didesnio srauto ir didesnio judėjimo sezono metu.

Fizinė apsauga užtikrinama naudojant signalizacijos sistema, kurioje yra judesio, dūmų, langų, bei gaisro jutikliai, taip pat parduotuvė ir sandėlis turi įrengtas fizines apsaugos priemones – grotas ant langų. Prieiga prie patalpų raktų ir signalizacijos kodų suteikiama pagal pareigas, vadovui, pamainos atsakingiems darbuotojams, kai yra reikalinga atsakingam asmeniui iš finansų, apskaitos skyrių. Prieiga prie tinklo įrangos ir vaizdo stebėjimo administravimo suteikiama tik ribotam skaičiui žmonių, vadovui, išoriniam IT specialistui.

Bendros organizacinės informacijos saugos taisyklės ar gairės nėra įmonėje formaliai dokumentuotos, taip pat darbuotojai nėra praėję informacijos saugos mokymų ar klausę paskaitų ta tematika, vidinis saugos užtikrinimas grindžiamas daugiausiai žmogiškuoju pasitikėjimu ir praktine patirtimi. Būtent tokia situacija ir būdinga mažoms įmonėms, ir visa tai stipriai didina žmogiškųjų klaidų sukeltų rizikų tikimybę.

Bendrai teigiant, galima matyti, kad mažos žemės ūkio įmonės informacinė aplinka pasižymi bazinėmis techninėmis ir fizinėmis apsaugos priemonėmis, įmonei trūksta sisteminio požiūrio į informacijos saugos valdymą. Dalis saugos sprendimų buvo įgyvendinti jau ankščiau reaguojant į realius incidentus lėmusius įmonei finansinius nuostolius, todėl egzistuoja poreikis nuosekliai įvertinti rizikas ir taikyti struktūruotas informacijos saugos valdymo priemones grįstas ISO 27001 ir ISO 27005 standartais.

2.2 Informacinės sistemos ribų ir vertinimo objekto apibrėžimas

Norint atlikti saugos rizikų vertinimą pagal ISO 27001 ir ISO 27005 standartus, pirmasis žingsnis yra aiškus informacinės sistemos ribų apsibrėžimas. Standartas ISO/IEC 27001 pabrėžia, kad organizacija turi aiškiai apibrėžti, kokiai veiklos daliai taikoma informacijos saugos valdymo sistema, atsižvelgdama į savo veiklą, turimus išteklius ir kitų suinteresuotų šalių poreikius [4]. Taip pat standartas numato, kad organizacija turi taip pat aiškiai apsibrėžti, kur ir kam bus taikoma informacijos saugos valdymo sistema, įsivertinus veiklos aplinką [4]. Darbe nagrinėjama įmonė – maža įmonė, vykdanti žemės ūkio veiklą. Vertinama nagrinėjamos įmonės informacinė aplinka, kuri tiesiogiai susijusi su kasdieniniais prekybos, administravimo ir valdymo procesais, bei veiklos tęstinumu. Vertinimo ribos apima informacines sistemas, procesus ir informacinius išteklius, kurių sutrikimas ar pažeidimas galėtų turėti reikšmingą poveikį nagrinėjamos įmonės veiklos tęstinumui, finansiniams rezultatams, ar teisinių reikalavimų laikymuisi. Į informacijos sistemos ribas įtraukiami šie pagrindiniai elementai:

- Darbo vietų kompiuteriai su „Windows 11“ operacine sistema (~12 aktyvių kompiuterių), naudojami administracijos, finansų, vadybos ir prekybos skyriuose.
- Kasos sistema ir su ja susiję prekybos bei apskaitos duomenys,
- Duomenys, saugomi darbo vietų kompiuteriuose, kaip klientų ir tiekėjų kontaktiniai duomenys – vardai, pavardės, telefono numeriai. Sąskaitų ir užsakymų informacija ir kiti apskaitai reikalingi įrašai.
- Vaizdo stebėjimo sprendimai, kaip kameros, NVR serveris su išplėsta vidine atmintimi,
- Tinklo infrastruktūra, apimanti laidinį vidinį tinklą, darbuotojų ir klientų belaidį tinklą, tinklo šakotuvus, maršrutizatorių,
- Fizinės saugos priemonės, kurios tiesiogiai susijusios su informacinių išteklių apsauga, kaip signalizacija ir fizine patekimo į patalpas kontrole.

Taip pat nustatoma, kad vertinimo ribos apima ne visas informacines sistemas, paslaugos kurios tiekiamos išorinių tiekėjų, tokios kaip buhalterinė apskaita ar kasos sistema, tokie komponentai vertinami tik tiek, kiek jie daro poveikį įmonės veiklai per paslaugų naudojimą, tačiau jų techninis saugumas nedetalizuojamas, nes šių paslaugų saugumas nėra tiesiogiai kontroliuojamas nagrinėjamos įmonės. Toks ribų nusistatymas yra priimtinas ir atitinka ISO/IEC 27001 praktiką, kai vertinami tik tie elementai, už kuriuos įmonė gali prisiimti atsakomybę.

ISO 27005 standartas nurodo, kad rizikos vertinimas turi būti atliekamas aiškiai apibrėžtoje aplinkoje, siekiant užtikrinti, kad identifikuojamos rizikos būtų realios, susijusios su organizacijos procesais ar ištekliais, taip pat standarte pabrėžiama, kad rizikos vertinimas apima vertinimo objektą, ribas, bei prielaidas, todėl rizikos vertinimas orientuojamas į praktinius, realiai naudojamus informacinius išteklius, o ne į teorines sistemas [6].

Atsižvelgiant į tai, kad įmonėje saugos sprendimai buvo sudiegti reaguojant į jau įvykusius incidentus, nustatytos vertinimo ribos leidžia teorinius informacijos saugos principus taikyti atsižvelgiant į realią nagrinėjamos įmonės veiklos patirtį, bei turimus išteklius. Toks požiūris sudaro pagrindą tolimesniam grėsmių identifikavimui, bei rizikų vertinimui, pagal ISO/IEC 27005 gaires.

Apibendrinus, galima matyti, kad jei informacinės sistemos ribos yra aiškiai apibrėžtos, tai leidžia nuosekliai, bei pagrįstai atlikti rizikos analizę, kuri užtikrina vertinimo tikslumą ir sudaro tinkamas prielaidas rizikos valdymo priemonių pasirinkimui, pagal nurodomus ISO 27001 reikalavimus.

2.3 Grėsmių identifikavimas mažoje žemės ūkio įmonės informacinėje aplinkoje

Pagal ISO 27005, rizikos vertinimo procesas pradedamas nuo grėsmių identifikavimo, pagal tai galime nustatyti kokie galimi įvykiai ar aplinkybės galinčios neigiamai paveikti įmonę, įmonės informacinius turtus. Grėsmės gali būti įvairaus pobūdžio, kaip techninio, organizacinio ar fizinio ir visos jos turi būti vertinamos atsižlegiant į įmonės veiklą, bei realią informacinę aplinką. Atsižvelgiant į nagrinėjamos įmonės veiklos pobūdį ir naudojamas informacines sistemas, bei ankstesnių incidentų patirtį, grėsmių identifikavimas atliekamas orientuojantis tik į tuos informacinius išteklius, kurių pažeidimai sukeltų didžiausią poveikį įmonės veiklos tęstinumui ar finansiniams rezultatams. Grėsmių analizė apima tiek informacinių sistemų sutrikimus, tiek žmogiškojo faktoriaus klaidas ar fizines saugos elementus. Toks požiūris leidžia koncentruotis į realias, o ne tik vien teorines grėsmes, su kuriomis įmonė gali susidurti savo kasdieninėje veikloje.

Techninės grėsmės – siejamos su informacinėmis sistemomis, tinklo infrastruktūra, bei duomenų saugumu. Žemės ūkio įmonėje naudojami darbo kompiuteriai ir kitos vietinės duomenų saugyklos, nėra įdiegta centralizuota duomenų atsarginių kopijų sistema, kas didina rizika, kuri yra susijusi su duomenų praradimu, dėl galimų techninių gedimų, programinės įrangos sutrikimų, ar kenkėjiškų programų kurios gali užrakinti turimus duomenis, duomenų praradimas šiuo atveju galėtų būti tiesiogiai sutrikdyti prekybos procesus ir laikinai sustabdyti įmonės veiklą. Papildomą riziką kelia ir tai, kad įmonė neturi tinklo segmentacijos, ko pasėkoje gali susidaryti sąlygos neautorizuotai prieigai prie vidaus tinklo. Bendro tinklo naudojimas darbo, tiek kitoms reikmėms didina galimą kibernetinės atakos vietą, bei tuo pačiu tokio tipo tinklas apsunkina prieigos kontrolę.

Organizacinės grėsmės – organizacinės grėsmės labiausiai siejamos su žmogiškuoju faktoriumi. Įmonėje nėra tinkamai formaliai aprašytų informacijos saugos dokumentų, taisyklių ar gairių, kaip reikia elgtis kibernetinės krizės metu, taip pat darbuotojai nėra praėję informacijos saugos mokymu ar supažindinti su pagrindiniais saugaus darbo principais. Saugos užtikrinimas daugiausiai grindžiamas pasitikėjimu, bei turima patirtimi ir tokia situacija ypač didina rizika, kad dėl žinių trūkumo ar neatsargių veiksmų gali būti pažeisti informacijos saugos reikalavimai, ypač tvarkantis su klientų duomenimis. Taip pat nėra aiškiai apibrėžtų prieigos teisių prie informacinių sistemų, todėl yra rizika, kad darbuotojai gali turėti daugiau prieigos teisių, nei yra būtina jų pagrindinėms funkcijoms atlikti.

Fizinės grėsmės – yra susijusios su patalpų ir materialinių išteklių apsauga. Kadangi įmonė jau yra patyrusi vagysčių, fizinis neteisėtas patekimas į patalpas gali turėti tiesioginį poveikį tiek materialiam, tiek informaciniam turtui ir tokio tipo incidentai gali lemti, ne vien įrangos praradimą, bet ir informacijos sunaikinimą ar neteisėtą atskleidimą.

Vaizdo stebėjimo kameros įmonėje yra labai svarbi saugos priemonė, kuri atlieka reikšmingą vaidmenį incidentų fiksavime, veiklos kontrolei, bei galimų pažeidimu užkardymui, ar tyrimui. Tačiau, vaizdo įrašai saugomo vienoje vietoje, nekuriant jų atsarginių kopijų, dėl ko įrašų praradimas galėtų reikšmingai apsunkinti incidentų tyrimą, bei vidaus kontrolės procesus.

7 lentelė. Pagrindinės grėsmės žemės ūkio įmonės informaciniams ištekliams
(Sudaryta autoriaus, remiantis ISO/IEC 27005)

Grėsmės tipas	**Grėsmės aprašymas**	**Trūkumas**	**Pasekmės**	**Kokie informaciniai ištekliai paveikiami**
Techninė	Duomenų praradimas dėl atsarginių kopijų nebuvimo	Nėra centralizuotos atsarginių kopijų sistemos	Veiklos sutrikdymas, prekybos laikinas stabdymas, finansiniai nuostoliai dėl neveiksnumo	Kasos ir apskaitos duomenis
Techninė	Kompiuterių ar programinės įrangos sutrikimas	Naudojama vienetinė įranga, be rezervo sprendimų	Laikinas ar visiškas darbo vietų neveiksnumas	Darbo kompiuteriai
Techninė	Neautorizuota prieiga prie tinklo per bendrą belaidį tinklą	Nesegmentuotas belaidis tinklas	Neautorizuota prieiga, duomenų praradimas	Vidaus tinklas ir privatūs duomenys

Grėsmės tipas	Grėsmės aprašymas	Trūkumas	Pasekmės	Kokie informaciniai ištekliai paveikiami
Organizacinė	Žmogiškosios klaidos dėl mokymų trūkumo	Darbuotojai neapmokami informacijos saugos	Asmens duomenų pažeidimai, veiklos neveiksnumas, BDAR pažeidimas	Klientų duomenys
Organizacinė	Neapibrėžtos prieigos teisės	Įmonė neturi prieigos taisyklių	Netinkamas ar nereikalingas priėjimas prie sistemų	Informacinės sistemos
Fizinė	Vagystė ar neteisėtas patekimas į įmonės patalpas	Ribota fizinė prieigos kontrolė darbo valandų metu	Įrangos praradimas ar veiklos laikinas sutrikdymas	Įranga, duomenys
Fizinė	Vaizdo įrašų praradimas ar sugadinimas	Vaizdo įrašai saugomi vienoje vietoje, nekuriant jų atsarginių kopijų	Incidentų informacijos ir kontrolės praradimas	NVR serveris, vaizdo, garso duomenys

Identifikuotas grėsmes apima pagrindinės informacijos saugos sritis ir sudaro tinkamas prielaidas tolimesniam rizikų vertinimui, kuriuo analizuojamos grėsmių pasireiškimo tikimybė, bei galimas poveikis nagrinėjamos įmonės veiklai.

2.4 Rizikų vertinimas tiriamos įmonės informacinėje aplinkoje

Rizikų vertinimas atliekamas remiantis ISO/IEC 27005 standarto metodinėmis gairėmis, taikant kokybinį rizikų vertinimo metodą. Toks metodas pasirenkamas atsižvelgiant į įmonės dydį, jos turima ribotą duomenį kiekį, bei praktinį vertinimo tikslą. Rizika vertinama, kaip grėsmės pasireiškimo tikimybės ir galimo poveikio įmonės veiklai derinys [9]. Vertinimo metu, analizuojamos identifikuotos grėsmės, nustatant jų pasireiškimo tikimybę ir galimą poveikį veiklos tęstinumui, finansiniams sunkumams ir teisiniams reikalavimams. Rizikos lygis nustatomas naudojant rizikos matrica, kuri leidžia palyginti skirtingų rizikų reikšmingumą ir pagal tai nusistatyti tinkamus prioritetus jų valdymui.

2.4.1 Rizikos tikimybės vertinimo kriterijai

Rizikos tikimybė apibrėžiama tuo, kad dažnai tikra grėsmė gali pasireikšti realioje organizacijos veikloje, vertinant mažos žemės ūkio įmonės informacinę aplinką, tikimybė nustatoma remiantis faktine veiklos patirtimi, ankstesniais incidentais, bei esama informacijos saugos būkle.

8 lentelė. Rizikos pasireiškimo tikimybės vertinimo kriterijai

(Sudaryta autoriaus, remiantis ISO/IEC 27005 ir A.Survila [9])

Tikimybės lygis	**Aprašymas**
Labai maža	Grėsmės pasireiškimas itin mažai tikėtinas, anksčiau niekada nebuvo įvykęs
Maža	Grėsmė gali pasireikšti retai, anksčiau nefiksuotas incidentas, arba tokie incidentai buvo ypač reti ir pavieniai
Vidutinė	Grėsmė gali pasireikšti kartais, nutikę pavieniai atvejai
Didelė	Grėsmė pasireiškė anksčiau, arba tikėtina artimu metu
Labai didelė	Grėsmė pasireiškia dažnai arba yra visada tikėtina

9 lentelė. Rizikos poveikio vertinimo kriterijai

(Sudaryta autoriaus, remiantis ISO/IEC 27005 ir A.Survila [9])

Poveikis	**Aprašymas**
Labai mažas	Poveikio nėra, arba jis nepastebimas, veikla nenutrūkta, nuostolių nėra arba jie nereikšmingi
Mažas	Nedidelis veiklos sutrikdymas, neturintis esminio poveikio
Vidutinis	Laikinas veiklos sutrikdymas, kuris gali turėti minimalius finansinius nuostolius
Didelis	Veiklos sutrikdymas, dideli finansiniai ar teisiniai padariniai
Labai didelis	Visikas veiklos sustabdymas, labai dideli finansiniai nuostoliai arba rimti teisiniai padariniai

2.4.2 Rizikos lygio nustatymas

Rizikos lygis nustatomas derinant grėsmės pasireiškimo tikimybę su galimu poveikiu. Tokio tipo vertinimas leidžia atsižvelgti į tikėtiną grėsmę, tiek į galimas pasekmes įmonei. Rizikos vertinimui taikoma 5x5 rizikos matrica, kuri grįsta penkių lygių tikimybės ir poveikio skalėmis.

Rizikos lygis nustatomas taikant rizikos priimtinumo klasifikaciją, pagal A.Survilos metodiką [9], kur rizika skirstoma į keturias kategorijas (A-D), atsižvelgiant į tikimybės ir padarinių derinį. Tokio tipo metodika plačiai taikoma praktikoje ir priimtina mažoms įmonėms, kai rizikos vertinimas atliekamas kokybiniu principu, remiantis ISO/IEC 27005 rekomendacijomis.

10 lentelė. Rizikos priimtinumo matrica

(Sudaryta autoriaus remiantis A.Survilos pavyzdine rizikos matrica [9])

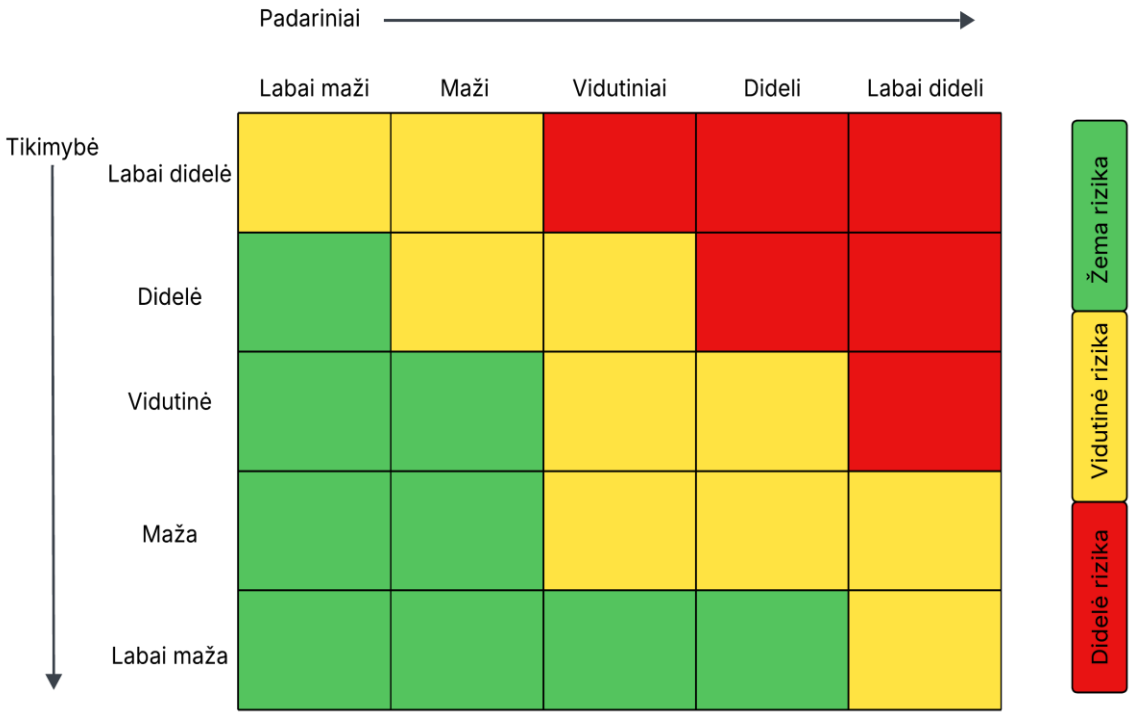
Tikimybė ↓ Padariniai →	Labai maži	Maži	Vidutiniai	Dideli	Labai dideli
Labai didelė	C	B	B	A	A
Didelė	D	C	B	B	A
Vidutinė	D	D	C	B	A
Maža	D	D	C	C	B
Labai maža	D	D	D	C	C

Rizikos lygis nustatomas kai kiekvienai grėsmei įvertinama tikimybė ir poveikis, tada šie du įvertinimai sujungiami rizikos matricoje. Rizikos matricoje kiekviena kombinacija patenka į vieną iš klasių A-D, todėl iškarto yra matoma, ar rizika didelė, vidutinė ar maža. „A klasė – labai didelė rizika, B klasė – vidutinės ir didelės rizikos, C klasė – Vidutinės, D klasė – mažos rizikos“ [9].

Siekiant aiškiau pavaizduoti 10 lentelėje pateiktą rizikos priimtinumo klasifikacija (A-D), šios matricos reikšmės papildomai perteiktos į „heatmapp“ formą.

5 pav. Rizikų žemėlapis

(Sudaryta autoriaus remiantis A.Survila [9])



2.4.3 Rizikos registras

Atlikus grėsmių identifikavimą ir nusistačius kokie yra pagrindiniai pažeidimai, sudaromas rizikų registras, kuris leidžia sistemiškai pažiūrėti ir įvertinti galimas rizikas, jų poveikį įmonės veiklai. Registras sudaromas remiantis ISO/IEC 27005 rekomendacijomis [6], ir apima svarbiausias rizikas, susijusias su turimais informaciniais turtais, technine infrastruktūra, žmogiškuoju faktoriumi, bei fizine sauga. Kiekviena rizika vertinama pagal jos pasireiškimo tikimybę, bei galima poveikį, o rizikos lygis nustatomas panaudojus rizikos matricą, kuri leidžia paprastai ir aiškiai nustatyti rizikas pagal jų svarbą. Toks vertinimo būdas yra tinkamas mažai įmonei, nes nereikalauja sudėtingų skaičiavimų ar didelio kiekio įmonės statistinių duomenų, bet vis tiek suteikia pakankamai gerą pagrindą sprendimų priėmimui.

Rizikų registras sudaro tolimesnį pagrindą sprendimams, dėl rizikų valdymo, priemonių pasirinkimo bei jų suskirstymo pagal prioritetus. Praktinėje darbo dalyje pateikiama supaprastinta rizikų registro forma, pilnas rizikų vertinimas pateiktas darbo prieduose.

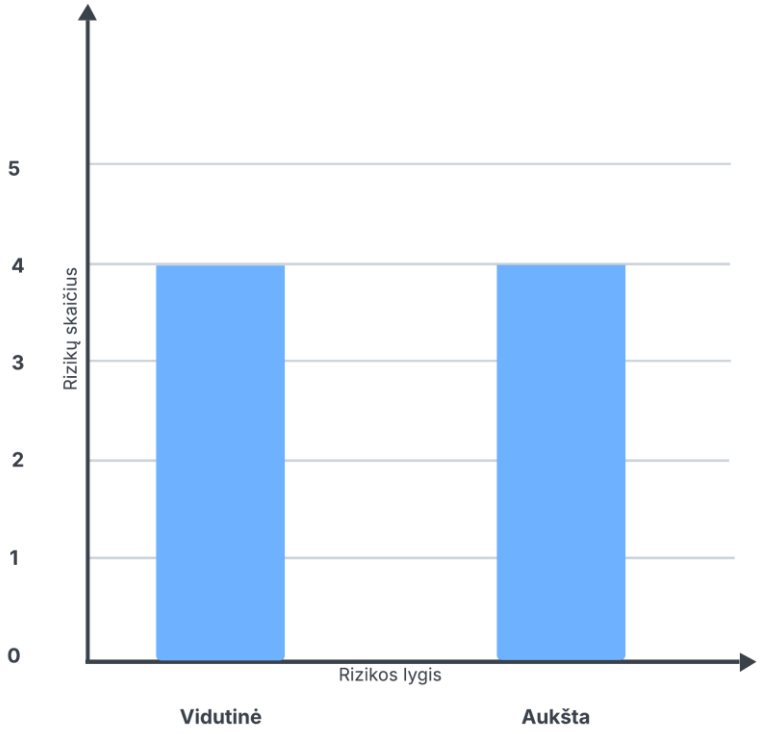
Toliau pateikiama lentelė kuri apibendrina pagrindines identifikuotas rizikas, kurios yra aktualios mažai žemės ūkio informaciniai aplinkai.

11 lentelė. Supaprastina rizikų registro analizė
(Sudaryta autoriaus remiantis ISO 27001, 27005 standartais)

Nr.	**Rizika**	**Rizikos lygis**
1	Duomenų praradimas	Aukšta
2	Neteisėta prieiga prie tinklo	Aukšta
3	Klientų duomenų nutekinimas	Aukšta
4	Kompiuterinės įrangos gedimas	Vidutinė
5	Vaizdo įrašų praradimas	Vidutinė
6	Slaptažodžių vagystė	Vidutinė
7	Socialinės inžinerijos atakos	Aukšta
8	Vagystė	Vidutinė

6 pav. Aukšto ir vidutinio lygio rizikų pasiskirstymas

(Sudaryta autoriaus)



6 paveiksle pateikta diagrama, parodo, kad sudarytame rizikų registre identifikuotos svarbiausios 8 rizikos, iš kurių 4 priskirtos aukštam lygiui ir 4 vidutiniam. Toks pasiskirstymas rodo, kad dalis grėsmių turi būti tvarkoma prioritetine tvarka, nes aukšto lygio rizikos laikomos nepriimtinomis ir reikalauja aktyvių kontrolės priemonių. Vidutinio lygio rizikos gali būti valdomos etapais atsižvelgiant į priemonių įgyvendinimo prioritetus, bei turimus išteklius.

Rizikų registro analizė

Analizuojant sudaryta rizikų registrą matyti, kad didžiausią grėsmę įmonės veiklai kelia rizikos kurios yra susijusios su duomenų saugumu, bei žmogiškuoju faktoriumi. Aukšto lygio rizikos daugiausiai siejamos su duomenų praradimu, klientų duomenų apsauga, bei socialinės inžinerijos atakomis, visos šios rizikos galit turėti itin neigiama poveikį įmonės veiklai, bei tęstinumui, finansiniams nuostoliams ir reputacijai. Atsižvelgiant į tai, kad įmonėje nėra formalių informacijos saugos politikų ir personalo mokymu, žmogiškasis faktorius tampa vienu iš svarbiausiu rizikos šaltinių.

Vidutinio lygio rizikos daugiausiai susijusios su techninės įrangos patikimumu ir fizine sauga. Kompiuterinės įrangos gedimai ar vaizdo įrašų praradimas gali sukelti trumpalaikius veiklos sutrikimus ir papildomas išlaidas, tačiau paprastai neturi kritinio poveikio visai įmonės veiklai. Fizinė saugos rizikos, kaip vagystė, taip pat vertinama kaip vidutinės, tačiau jų reikšmė didėja, jei

jos kartu įvyksta su kitais pažeidimais, kaip nepakankama prieigos kontrole ar stebėjimo priemonių trūkumu.

Sudarytas rizikų registras leidžia aiškiai nustatyti, kurios rizikos turi būti tvarkomos pirmiausiai, o kurios gali būti valdomos vėlesniais etapais, arba laikomos priimtinos atsižvelgiant į įmonės galimybes, tai sudaro pagrindą tolimesnių rizikų valdymo etapui, kur parenkami tinkamiausios rizikų valdymo priemonės ir nustatomi jų įgyvendinimo prioritetai atsižvelgiant į ISO 27001 standarto reikalavimus [4].

Vertinant nustatytas rizikas praktinėje dalyje, laikomasi teorinėje darbo dalyje aprašyto rizikos priimtinumo požiūrio, pagal kurį aukšto lygio rizikos laikomos nepriimtinomis ir reikalauja aktyvaus valdymo, o dalis vidutinių lygio rizikų, atsižvelgiant į įmonės mastą ir jos pobūdį, gali būti laikomos laikinai priimtinomis.

2.5 Rizikų valdymo planas

Rizikų valdymas yra neatsiejama dalis rizikų vertinimo proceso, kai remiantis sudarytu rizikų registru yra pasirenkami konkretūs veiksmai nustatytoms rizikoms sumažinti, kontroliuoti arba jas priimti. ISO 27005 standartas pabrėžia, kad rizikų valdymo sprendimai turi būti grindžiami įvertintu rizikos lygiu, organizacijos kontekstu ir turimais jos ištekliais [6], todėl praktikoje svarbu pasirinkti tokias priemones, kurios būtų realiai įgyvendinamos ir tinkamos įmonės mastui.

Remiantis aprašytais rizikų vertinimo kriterijais ir rizikos matrica, galime laikytis požiūrio, kad mažos žemės ūkio įmonės rizikos apetitas, arba kitaip tariant rizikos tolerancija yra žema ir tai reiškia, kad aušto lygio rizikos laikomos nepriimtinos ir turi būti valdomos pirmiausiai, dalis vidutinio lygio rizikų gali būti laikomos laikinai priimtinos ir tuo atveju, jei jos nekelia kritinės grėsmės veiklos tęstinumui. Toks rizikos priimtinumo apibrėžimas leidžia suderinti teorijoje aptartą rizikos priimtinumo principą su praktiniu mažos įmonės sprendimų priėmimu.

Rizikų valdymui taikomi pagrindiniai rizikų valdymo būdai:

- Rizikos mažinimas, taikant organizacines ir technines priemones, kurios mažina rizikos tikimybę ir jos poveikį.
- Rizikos perkėlimas, pasitelkiant trečiąsias šalis, kaip paslaugų sutartis ir draudimai.
- Rizikos priėmimas, kai rizika laikoma toleruotina įmonei, bet pats sprendimas pagrindžiamas tuo, kad bus numatoma stebėsena.

Rizikos vengimas praktikoje taikomas ribotai, nes įmonė negali atsisakyti pagrindinių informacinių sistemų ir procesų kurie yra reikalingi kasdieninei veiklai, kaip darbas kompiuteriu, vidaus tinklas, kasos darbas ir vaizdo stebėjimas.

Rizikų valdymo plano įgyvendinimui įmonėje taip pat turi būti paskirtas atsakingas asmuo, savininkas ar kitas sutartas IT specialistas/prižiūrėtojas, kuris koordinuoja priemonių diegimą ir stebi jų vykdymą. Priemonės įgyvendinamos palaipsniui, pagal nustatytą prioritetą: 1 – prioriteto rizikos mažinamos pirmos ir nedelsiant, 2 – prioriteto rizikos mažinamos artimiausiu laiku, o 3 – prioriteto rizikos planuojamos mažinti vėlesniu etapu atsižvelgiant į įmonės resursus.

Vadovaujantis ISO 27001 6.1.3 punktu [4], kuriame numatyta parengti rizikų tvarkymo planą, žemiau pateikiama suvestinė lentelė, kuri apibendrina, kaip aukšto ir vidutinio lygio rizikos yra tvarkomos pagal jų svarbą.

12 lentelė. Supaprastinta rizikų valdymo sprendimų suvestinė

(Sudaryta autoriaus)

Nr.	**Rizika**	**Rizikos lygis**	**Valdymo būdas**	**Prioritetas**
1	Duomenų praradimas	Aukštas	Mažinimas	1
2	Neteisėta prieiga prie tinklo	Aukštas	Mažinimas	1
3	Klientų duomenų nutekinimas	Aukštas	Mažinimas	1
7	Socialinės inžinerijos atakos	Aukštas	Mažinimas	1
4	Kompiuterinės įrangos gedimas	Vidutinis	Mažinimas/Perkėlimas	2
5	Vaizdo įrašų praradimas	Vidutinis	Mažinimas	2
6	Slaptažodžių vagystė	Vidutinis	Mažinimas	2
8	Vagystė	Vidutinė	Mažinimas/Perkėlimas/Priėmimas	3

Didžiausias dėmesys skiriamas aukšto lygio rizikoms, nes jos tiesiogiai yra susijusios su duomenų saugumu, veiklos tęstinumu ir įmonės reputacija. Pirmojo prioriteto rizikoms priskiriamas duomenų praradimas, nes net ir trumpalaikis duomenų praradimas mažoje įmonėje gali sutrikdyti kasdienines operacijas ir sukelti papildomas išlaidas. Dėl šios priežasties pagrindinis sprendimas tokiai rizikai valdyti yra aiškus atsarginių kopijų darymo procesas, kuris įtraukia ne vien tik kopijų atlikimą, bet ir periodinį duomenų atkūrimo patikrinimą.

Neteisėtos prieigos prie tinklo ir kitų klientų duomenų nutekinimo rizikos taip pat laikomas prioritetiniu, nes jos gali sukelti finansines, reparacinės ir net teisines pasekmes. Tokių rizikų mažinimas aptariamoje įmonėje dažniausiai pradedamas nuo bazinių priemonių, tokių kaip prieigos ribojimo, slaptažodžių naudojimo taisyklių, bei periodinės priežiūros. Socialinės inžinerijos atakos

rizika daugiausiai siejama su žmogiškuoju faktoriumi, todėl čia taikomos praktinės priemonės, kaip trumpi darbuotojų saugos mokymai, aiški taisyklė tikrinti įtartinus laiškus bei nuorodas ir incidentų pranešimo tvarka, kam reikia pranešti pastebėjus įtartiną veiklą.

Vidutinio lygio rizikos, kaip įrangos gedimai, vaizdo įrašų praradimas ar paprasta vagystė yra valdomos etapais, taikant gerinimo metodus palaipsniui, tai reiškia, kad jos gali būti toleruojamos trumpuoju laiku, tačiau joms numatomos priemonės ir stebėsena, kad rizikos tikimybė ir poveikis mažėtų. Kai kuriais atvejais gali būti taikomas ir rizikos perkėlimas pasitelkiant išorines paslaugas, kaip draudimas.

Svarbu, kad rizikų valdymas nėra vienkartinis veiksmas, sudiegus priemones turi būti atliktas vertinimas, ar rizikos lygis sumažėjo ir jeigu reikalinga pakoreguoti priimtus sprendimus.

2.6 Incidentų analizė

Incidentų analizės tikslas, tai parodyti, kokios situacijos realiai gali įvykti mažoje žemės ūkio įmonėje ir kaip jos susijusios su rizikų registru bei numatytomis priemonėmis. Pasirinkti incidentai yra ypač dažni mažoms ar vidutinėms įmonėms, nes jose paprastai trūksta personalo, laiko ir finansų, o IT sauga dažnai tvarkoma tik tada, kai „reikia“. Kiekvienas atvejis aprašomas pagal logiką, kas įvyko, kokios pasekmės, kodėl įvyko ir kokios priemonės turtėtų būti taikomos, kad sumažinti riziką. Taip pat kiekvienu atveju nurodomas ryšys su rizikų registre identifikuota rizika, bei minimalūs incidento valdymo žingsniai, kaip identifikavimas, suvaldymas, atkūrimas, kurie mažoje įmonėje yra praktiškai įgyvendinami.

2.6.1 Sukčiavimo laiškas ir prisijungimo duomenų nutekėjimas

Ryšys su rizikų registru: Incidentas atitinka riziką susijusią su socialine inžinerija – „phishing“ ataka ir paskyrų kompromitavimu, kai per apgaulingus laiškus yra išgaunami prisijungimo duomenys.

Kas įvyko: Darbuotojas gauna el.laišką, kuris iš pirmo žvilgsnio atrodo patikimas, nes gaunama iš tiekėjo, banko ar kitos valstybinės institucijos. Laiške nurodyta nuoroda „Peržiūrėti dokumentą“, „Peržiūrėti banko pranešimą“, „Patvirtinti dokumentą“. Paspaudus nuorodą atidaromas netikras puslapis kuriame prašoma įvesti įmonės ar darbuotojo prisijungimo duomenis, suvedus duomenis langas užsidaro.

Pasekmės įmonei: Dėl suvestų duomenų, gali būti perrimtas el.pašto prieinamumas ar visa paskyra, visi siųsti ir gauti, bei siunčiami ir gaunami laiškai nutekinami, kartu su jais ir kontaktai ar

kiti svarbus dokumentai. Taip pat galimi ir finansiniai nuostoliai, dėl neteisingo pervedimo, ar reputacijos žala, dėl atskleistų klientų duomenų.

Kodėl įvyko: Tokio tipo atakos dažniausiai įvyksta dėl skubėjimo, pasitikėjimo, nepakankamo informuotumo, neaiškių taisyklių. Rizika padidėja, jei naudojami silpni ir besikartojantis slaptažodžiai, taip pat, jei įmonė nenaudoja kelių faktorių autentifikacijos.

Kontrolės priemonės kurios sumažintų riziką ir būtų tinkamiausios mažai įmonei:

- Pagrindinės darbuotojų paskyros autentifikuojamos kelių faktorių autentifikacija.
- Taisyklė, kuri neleidžia suvedinėti slaptažodžių nes neaiškias nuorodas iš laiškų.
- Trumpi periodiniai priminimai, kaip kartą per ketvirtį, apie galimas grėsmes, dėl tokio tipo įvykių.
- Slaptažodžių taisyklės.
- Incidento pranešimo taisyklė, kam pranešti ir ką daryti pirmiausia pastebėjus tokį įvykį: atsijungimas, slaptažodžio keitimas, prisijungimų tikrinimas kitose platformose.

Incidento valdymo veiksmai(minimalus praktinis scenarijus): 1 – identifikavimas, užfiksuojama, kas įvyko(kas laiško siuntėjas, nuoroda, laikas, paveikti prisijungimai); 2 – suvaldymas – keičiami slaptažodžiai, atjungiamos paskyros, įjungiama kelių faktorių autentifikacija; 3 – atkūrimas – atstatoma paskyra ir jos kontrolė, bei patikrinama ar nebuvo atliktų neteisėtų veiksmų; 4 – Pamoka, atnaujinamos taisyklės, darbuotojams pateikiamas konkretus pavyzdys, kad incidentas nebepasikartotu.

2.6.2 Kasos kompiuterio sutrikimas arba užsikrėtimas kenkėjiška programa

Ryšys su rizikų registru: Incidentas atitinka rizika su kritinės darbo vietos nepasiekiamumu(kasa), kenkėjiškų programų patekimu ir galimu duomenų praradimu ar šifravimu.

Kas įvyko: Sugenda pagrindinis kompiuteris, kasos darbo vietoje arba užsikrečia kenkėjiška programa, per atsiųstą failą el.paštu, iš USB laikmenos ar paspaustą nesaugią nuorodą.

Pasekmės įmonei: Dėl nebeveikiančio, ar netinkamai pradėjusio veikti kompiuterio sustoja darbas, tampa sudėtinga aptarnauti klientus, atsiranda prastovos ir papildomos išlaidos, kaip remontas, kenkėjiškos programos šalinimas ar net duomenų atstatymas. Jei kenkėjiška programa yra orientuota į šifravimo ataką, gali būti užrakinti duomenys ir veikla sustabdoma ilgesniam laikui.

Kodėl įvyko: Dažniausiai tokio tipo atakos įvyksta, kai nėra aiškios tvarkos dėl aparatinės įrangos atnaujinimų, dirbama administratoriaus teisėmis, nėra taisyklių dėl programų diegimo, o antivirusinė neįdiegta, arba įdiegta, bet netvarkinga, nedaromos atsarginės kopijos.

Praktinės kontrolės priemonės kurios padėtų sumažinti riziką:

- Aiški atnaujinimų tvarka, kas atsakingas už juos ir kaip dažnai tikrinama ar jie atlikti.
- Antivirusinė programa.
- Vartotojų teisių ribojimas, kaip programas diegia tik administratorius.
- Atsarginių kopijų darymas, reguliarios jų patikros.
- Veiksmų planas įvykus incidentui, kaip: atjungti nuo tinklo, nepriimti skuboti veiksmų, informuoti atsakingą IT asmenį, fiksuoti požymius ir įrangos veiksmus, jei tokie yra.

Incidento valdymo veiksmai (minimalus praktinis scenarijus): 1 – identifikavimas, tai gedimas ar programinis užkratas; 2 – suvaldymas, kompiuterio atjungimas nuo tinklo, sustabdomas galimas plitimas į kitas darbo vietas ar įrenginius; 3 – atkūrimas, atkuriama veikla iš patikimų turimų kopijų arba paruošiama atsarginė darbo vieta; 4 – pamoka, peržiūrima techninė įranga, patikrinami USB laikmenos, peržiūrimos ir jei reikalinga papildomos/pataisomos taisyklės.

2.6.3 Vaizdo kamerų įrašų praradimas (NVR arba kita disko problema)

Ryšys su rizikų registru: incidentas atitinka riziką, susijusią su fizinio saugumo kontrolės priemonių nepasiekiamumu ir įrodymų praradimu dėl techninių ar programinių priežasčių.

Kas įvyko: Tinklo įrašymo įrenginys nustoja įrašinėti, arba įrašai tampa nebeprieinami, dėl disko gedimo, vietos trūkumo, nustatymų klaidos, elektros sutrikimo.

Pasekmės įmonei: Prarasti įrašai išryškėja ne iš karto, jų prireikia tada, kai nutinka vagystė, kilus ginčui ar tiriant incidentą. Jei įrašų nėra, įmonė praranda įrodymus ir sumažėja tikimybė atkurti įvykius. Kai kuriais atvejais sukeliami tiesioginiai finansiniai nuostoliai.

Kodėl įvyko: Dėl IT specialisto nebūvimo ir rutinos neturėjimo, nėra pastebima, blogos diskų būklės, kad įrašai nebevyksta, dėl netinkamų nustatymų diskas prisirašė pilnas ir nėra rašoma „ant viršaus“, netikrinamos serverio klaidos ar kitos išklotinės ir jos nėra siunčiamos į kitą sistemą, todėl gedimas pastebimas tik po kurio laiko.

Kontrolės priemonės sumažinančios riziką:

- Periodinis NVR patikrinimas, kokia įrašymo būsena, diskų būklė, tikrinamos klaidos ir išklotinės.
- NVR pranešimai apie kritines klaidas peradresuojami į kitus dažniau naudojamus įrenginius(telefonas, kompiuteris).
- UPS naudojimas.
- Ribojama prieiga prie NVR sistemos.

Incidento valdymo veiksmai (minimalus praktinis scenarijus): 1 – identifikavimas, nustatoma, nuo kada NVR nebeveikia ir kokia to priežastis(disko problema, maitinimas, nustatymai); 2 – suvaldymas, stabdomas tolimesnis įrašų praradimas, atstatomas įrašymas, keičiamas diskas ar koreguojami nustatymai; 3 – atkūrimas, patikrinama ar įrašai pasiekiami, ar reikalinga keisti/atstatyti serverio konfigūraciją, įvertinami likę įrašai; 4 – pamoka, įvedamas aiškus periodinis patikrinimas ir automatiniai pranešimai įrangos gedimo atveju, kad sutrikimas būtų fiksuojamas iškarto.

Apibendrinant incidentų pirminę analizę matyti, kad mažoje įmonėje didžiausią riziką sukuria, ne vien techniniai sutrikimai, bet ir žmogiškasis faktorius, bei priežiūros trūkumas. Praktikoje incidentai dažnai pastebimi ne iš karto, kaip vaizdo įrašų praradimas išryškėja tik tada, kai jų realiai prireikia, todėl įmonei būtina turėti ne vien tik pavienes kontroles priemones, bet ir nuoseklų stebėsenos procesą, kuris leistų laiku identifikuoti nuokrypius, įsivertinti priemonių veiksmingumą, bei sumažinti likutinę riziką. Atsižvelgiant į tai, toliau pateikiami stebėsenos procesai kurie mažos žemės ūkio įmonės atveju yra realiai įgyvendinami ir tiesiogiai siejasi su rizikų registre numatytomis prioritetinėmis rizikomis. Praktiniu lygmeniu rekomenduojama fiksuoti incidentus, bent minimaliame incidentų žurnale, nes ateityje tai leidžia matyti pasikartojančius incidentus ir pagal tai pagrįsti, kodėl tam tikros kontrolės priemonės yra prioritetinės.

2.7 Stebėsenos procesai

Stebėsena suprantama kaip suplanuotas ir periodiškai vykdomas procesas kuris leidžia įmonei laiku pastebėti sutrikimus, reikiamus atnaujinimus, atsarginių kopijų problemas, įvertinti taikomų priemonių veiksmingumą ir priimti sprendimus dėl jų tobulinimo. ISO 27001 reikalauja, kad organizacija nustatytų, ką ir kaip stebės, bei matuos, kada bus analizuojami rezultatai, kas už tai atsakingas ir kad informacija apie įrodymus būtų išsaugoma [4].

Mažų ir vidutinių įmonių kontekste, stebėsena turi būti orientuota į didžiausią rizikos mažinimo efektą ir paprastai įgyvendinama, nes dažniausiai grėsmės mažose įmonėse yra sukčiavimas, kenkėjiškos programos, netinkama ar nepakankama prieigos kontrolė ir pasenusios sistemos. Dėl to minimoje žemės ūkio įmonėje stebėsenos procesai formuojami remiantis prioritetinėmis rizikomis, kaip „phishing“ atakos, kasos darbo vietos sutrikimai ar užkrėtimai kenkėjiška programine įranga, vaizdo įrašų praradimas, kurios buvo išskirtos incidentų analizėje.

Taip pat procesai šioje dalyje suprantami, kaip ciklo „PDCA“ „Check“ dalis, tai periodiškas tikrinimas ar taikomos priemonės realiai veikia ir ar rizikos lygis mažėja, tokia logika mažoje

įmonėje yra patogi tuo, kad leidžia remtis ne abstrakčiais vertinimais, o konkrečiais įrodymais, kaip įrašų žurnalo įrašas.

2.7.1 Stebėsenos objektai ir atsakomybės

Kad stebėsena būtų vykdoma realiai ir paprastai, reikalinga apibrėžti minimalų sąrašą, „ ką tikriname?“, tikrinimo periodiškumą, atsakingą asmenį ir fiksavimo būdą. ISO 27001 taip pat akcentuoja, kad tokie rezultatai turi būti dokumentuojami, kaip įrodymai [4].

13 lentelė. Mažos žemės ūkio įmonės minimalus stebėsenos praktinis planas

(Sudaryta autoriaus)

Stebėjimo objektas	Ką tikrinti	Periodiškumas	Atsakingas asmuo	Įrodymai(fiksavimas)
Paskyros ir prieigos	Ar įjungtas MFA, ar nėra neįprastų prisijungimų, ar teisės atitinka pareigas	Kiekvieną mėn. Po įtarimo Po įvykio	Vadovas Paskirtas asmuo	Įrašas stebėsenos žurnale
Programinės įrangos atnaujinimai	Ar atlikti siūlomi/kritiniai atnaujinimai, ar nėra pasenusių versijų	Kiekvieną mėn.	Paskirtas asmuo IT specialistas	Atnaujinimų žurnalas
Antivirusinė kita apsaugos priemonė nuo kenkėjiškų programų	Ar apsauga aktyvi, ar nėra įspėjimų, Ar atliktas skenavimas	Kiekvieną sav.	Paskirtas asmuo IT specialistas	Įrašas stebėsenos žurnale
Atsarginės kopijos	Ar kopija sukurta, Ar nėra klaidų	Kiekvieną sav.	Paskirtas asmuo IT specialistas	Kopijų būklės įrašas
Atsarginių kopijų atkūrimo testas	Ar įmanoma atkurti 1 failą, katalogą	Kiekvieną ketvirtį	Paskirtas asmuo IT specialistas	Kopijų būklės įrašas
NVR serveris	Įrašymo būsena, disko būklė, užpildymas, klaidos, kas turi prieigą peržiūrai/eksportui	Kiekvieną mėn.	Paskirtas asmuo IT specialistas	NVR patikros įrašas

Tokio tipo planas atitinka NKSC rekomendacijas mažoms ir vidutinėms įmonėms, kur nurodoma, reiktų prioritetą kelių faktorių autentifikacijai, atnaujinimams, darbuotojų sąmoningumui

ir techninių spragų mažinimui, nes tai yra ekonomiškiausias, bet tuo pačiu ir efektyviausias būdas ribotų išteklių aplinkoje[12].

2.7.2 Incidentų fiksavimas ir incidentų žurnalas

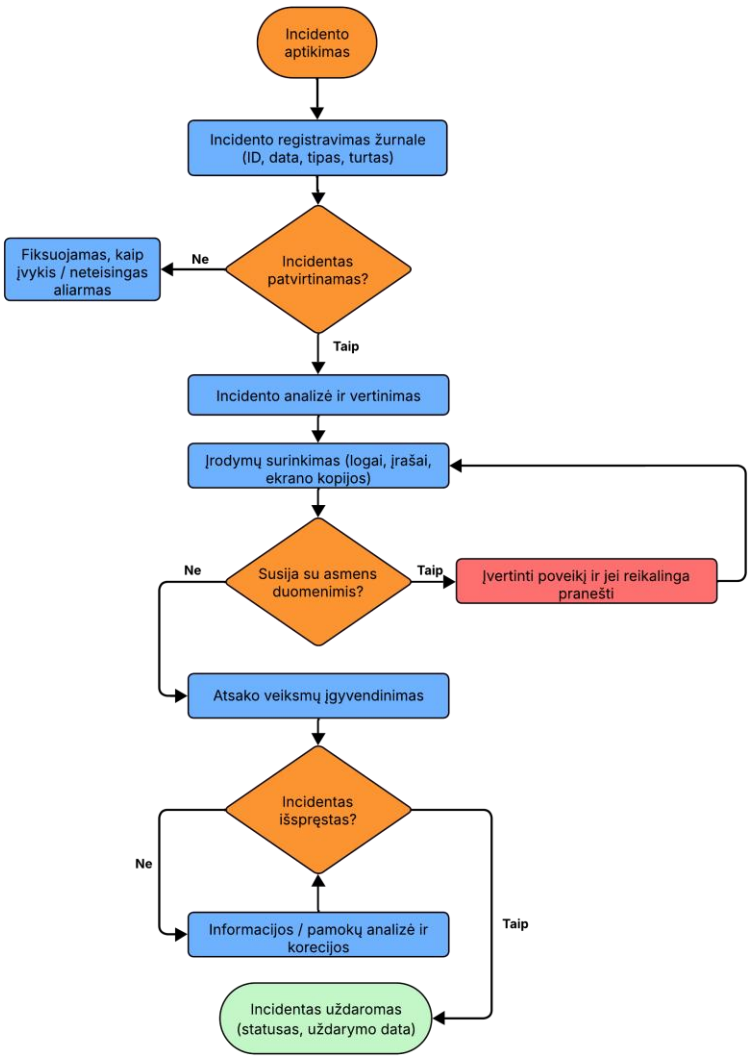
Kad stebėsena būtų ne vien „patikrinimas“, bet ir valdymo pagrindas, įmonei rekomenduojama turėti minimalų incidentų žurnalą. Tai praktinis tikslas kaupti įrodymus, matyti bepasikartojančios tendencijas ir pagrįsti, kodėl tam tikros kontrolės priemonės yra laikomos prioritetinėmis.

Incidentų žurnalo galimi minimalūs laukai:

- Data ir laikas:
- Incidento ID (numeris):
- Incidento tipas(„phising, virusas, gedimas, NVR sutrikimas):
- Kas pastebėjo ir kada:
- Paveiktas turtas (įrenginys, paskyra, sistema):
- Trumpas aprašymas ir požymiai:
- Atlikti veiksmai (identifikavimas, suvaldymas, atkūrimas):
- Ar buvo peržiūrėti/eksportuoti vaizdo įrašai (kas atliko, kokiu tikslu);
- Pasekmės (neveikimas, nuostoliai, praradimas):
- Statusas (aktyvus/uždarytas ir uždarymo tada):
- Pamokos ir komentarai (kas atlikta, kad nesikartotų):

7 pav. Incidentų valdymo proceso schema

(Sudaryta autoriaus)



7 paveikslo pateiktoje schemoje pavaizduotas incidentų valdymo procesas mažoje įmonėje, nuo incidento aptikimo ir registravimo iki jo uždarymo. Procesas apima incidento patvirtinimą, analizę, įrodymų fiksavimą, reagavimo veiksmus, taip pat numatytas sprendimo taškas, kur leidžiama įvertinti ar incidentas susijęs su asmens duomenimis ir jeigu reikalinga inicijuojami veiksmai pagal BDAR reikalavimus.

Svarbu, kad jei incidentas susijęs su duomenimis, BDAR įpareigoja, ne tik taikyti atitinkamas technines ir organizacines priemones, bet ir turėti gebėjimą laiku reaguoti bei prireikus pranešti apie nustatytą pažeidimą, per nustatytą terminą[13].

Taip pat stebėsenos metu surinkti duomenys gali būti periodiškai vertinami, kad būtų aišku, ar pritaikytos priemonės realiai veikia. ISO 27001 numato, kad organizacija vertina savo

informacijos saugos veiksmingumą, vykdo vidinius auditus, nustačius neatitiktis taikomi korekciniai veiksmai [4].

Žemės ūkio įmonės atžvilgiu siūlomas minimalus praktinis įvertinimo principas:

- Kartą per ketvirtį peržiūrėti stebėsenos žurnalus ir incidentų žurnalą.
- Nusistatyti kelias pasikartojančias problemas.
- Priimti įmonei priimtiniausią ir paprasčiausią sprendimą.

Apibendrinant, galima teigti, kad stebėsena ir incidentų žurnalas mažoje įmonėje yra praktiškiausias būdas užtikrinti, jog saugos priemonės nebūtų taikomas tik formaliai, reguliarus tikrinimas ir trumpas duomenų fiksavimas leidžia laiku pastebėti nuokrypius, įvertinti priemonių veiksmingumą, bei priimti paprastus korekcinius sprendimus. Tokiu būdu mažinamas likusios rizikos lygis, o saugos valdymas tampa nuoseklus, bei lengviau valdomas net esant ribotiems ištekliams.

2.8 Praktinės dalies santrauka

Praktinėje dalyje įvertinama žemės ūkio įmonės informacinė aplinka ir jos esama informacijos saugos būklė remiantis ISO 27001 ir ISO 27005 principais. Atlikta įmonės IT aplinkos aprašymo ir taikomų techninių, organizacinių, bei fizinių priemonių vertinamoji analizė, vėliau identifikuoti pagrindiniai trūkumai, bei pažeidžiamumai kurie gali turėti įtakos įmonės veiklos tęstinumui.

Rizikų vertinimas atskleidė, kad didžiausią reikšmę mažai įmonei turi rizikos kurios yra susijusios su duomenų praradimu, neteisėta prieiga ar žmogiškuoju faktoriumi, taip pat išlieka aktualios rizikos ir su darbo vietų techninės įrangos gedimais, slaptažodžių sauga, vaizdo įrašų praradimais ir fizinėmis grėsmėmis. Remiantis gautais rezultatais, sudarytas rizikų registras, bei jų valdymo sprendimų suvestinė, kuri leidžia paprastai nustatyti prioritetines kontrolės priemones ir jų taikymą.

Praktinei kontrolei užtikrinti pasiūlytas minimalus stebėsenos principas ir incidentų žurnalo pildymas, kas sudaro pagrindą periodiškai vertinti ar įmonės taikomos priemonės realiai veikia, ar rizikos mažėja. Tai atitinka NIST gairėse akcentuojamą principą, kad saugumo funkcijos privalo išlikti nuolatinė sistemos gyvavimo ciklo dalimi [8].

Pagal praktinės dalies rezultatus, galime pateikti siūlomas informacijos saugos gerinimo planą, kuriame numatomos prioritetinės priemonės, jų įgyvendinimo eiga ir minimalus valdymo modelis, kuris pritaikytas mažos įmonės poreikiams.

3 INFORMACIJOS SAUGOS TOBULINIMO PLANAS IR MODELIS

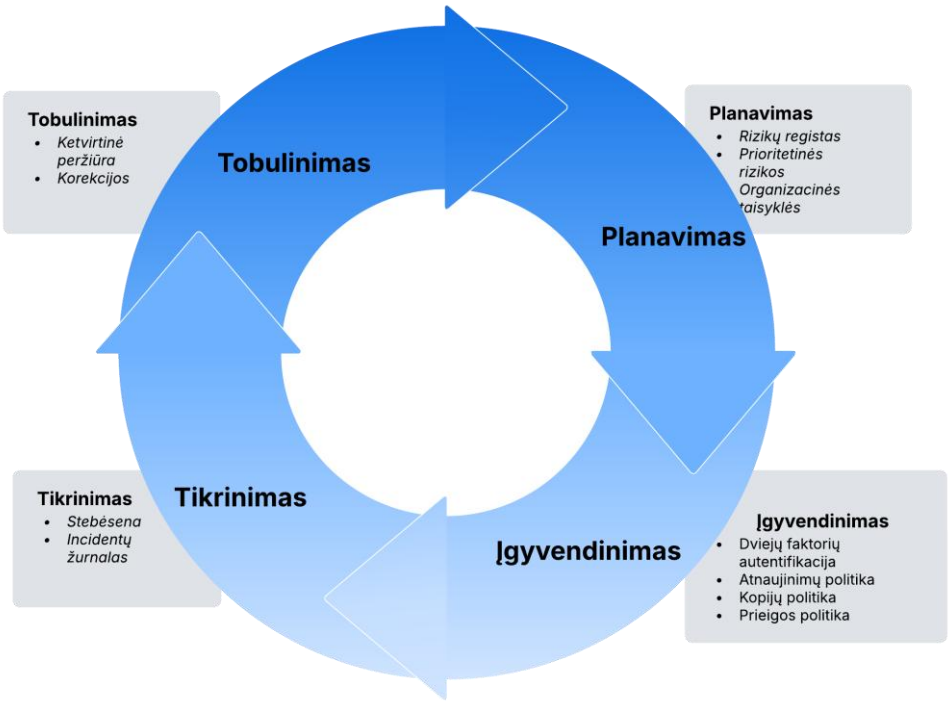
Šiame skyriuje remiantis antrojo skyriaus praktinės dalies rezultatais, pateikiamas mažos žemės ūkio įmonės informacijos saugos gerinimo planas. Praktinėje dalyje buvo įvertinta įmonės informacinė aplinka, identifikuotos pagrindinės rizikos, sudarytas rizikų registras ir parengta rizikų valdymo sprendimų suvertinė, taip pat aptarti stebėsenos ir incidentų fiksavimo priemonės, paskirstytos atsakomybės, numatyti įgyvendinimo etapai ir apibrėžtas minimalus stebėsenos mechanizmas, kuris užtikrina, kad saugos priemonės būtų taikomos nuosekliai su galimybe vertinti jų veiksmingumą.

3.1 Siūlomas minimalus ISVS modelis mažai įmonei

Praktinėje dalyje nustatyta, kad didžiausią įtaką įmonės saugai sudaro kelios pagrindinės rizikos, kurios gali būti suskaidytos į grupes, tai: duomenų praradimas, neteisėta prieiga, klientų duomenų nutekinimas ir socialinės inžinerijos atakos. Todėl siūlomas informacijos saugos valdymo modelis turi būti orientuotas į paprastą, bet nuoseklią tvarką, aiškias atsakomybes, periodines patikras, įrodymų fiksavimą ir korekcinius veiksmus, tokia logika atitinka ISO 27001 principą [4], kad organizacija turi nusistatyti, ką stebėti, ką matuoti, kada analizuoti rezultatus, ką pažymėti į registrą ir kas už šias procedūras yra atsakingas.

Mažos įmonės kontekste, siūloma taikyti minimalų PDCA modelį, bet pritaikyta konkrečiai mažos žemės ūkio įmonės situacijai:

8 pav. PDCA pagrįstas ISVS modelis mažai žemės ūkio įmonei
(Sudaryta autoriaus)



- Plan (Planavimas): Rizikų registras, prioritetų nustatymas, minimalios slaptažodžių, kopijų ir incidentų taisyklės.
- Do (Įgyvendinimas): Konkrečios techninės ir organizacinės priemonės, kaip MFA, atnaujinimai, kopijos, prieigos valdymas.
- Check (Tikrinimas): Vykdoma stebėsena pagal minimalų planą ir incidentų žurnalo pildymas, renkami įrodymai.
- Act (Tobulinimas): Numatytu laiko periodu, kaip kas ketvirtį peržiūrėti žurnalus, identifikuoti pasikartojančias problemas ir pritaikyti paprasčiausias korekcijas.

3.2Atsakomybės ir vaidmenų pasiskirstymas

Kad modelis funkcionuotų tinkamai, reikalinga iš anksto susitarti dėl atsakomybių. Praktinėje dalyje numatyta, kad stebėsenoje dalyvauja vadovas ar priskirtas asmuo ir kai reikalinga IT specialistas, todėl siūlomas paprastas principas: **Įmonės viduje – kontrolė ir sprendimai, išorėje – techninė pagalba pagal reikalingą poreikį.**

14 lentelė. Atsakomybių paskirstymas ISVS valdyme

(Sudaryta autoriaus)

Veikla	**Atsakingas asmuo**	**IT specialistas**	**Fiksavimas**
Rizikų registro ir suvestinės peržiūra	Vadovas/Priskirtas asmuo	Konsultuoja	Peržiūros įrašas
Paskyrų kontrolė	Vadovas/Priskirtas asmuo	Padeda konfigūruoti	Įrašas stebėsenos žurnale
Atnaujinimų patikra ir diegimas	Priskirtas asmuo	Diegia/Tikrina išimtinais atvejais	Atnaujinimų žurnalas
Atsarginių kopijų kontrolė	Priskirtas asmuo	Automatizuoja/Tikrina išimtinais atvejais	Kopijų įrašas
Atkūrimo testas	Priskirtas asmuo	Vykdo pats, arba padeda jį vykdyti	Kopijų įrašas
NVR būklė	Priskirtas asmuo	Peržiūri NVR nustatymus	Kopijų įrašas
Incidentų registravimas	Priskirtas asmuo	Analizuoja sudėtingais atvejais	Incidentų žurnalas

Atlikus atsakomybių paskirstymą įmonėje išvengiama situacijos, kai saugos incidento metu, sauga tampa „niekėno reikalu“, taip pat galimas krūvio išlyginimas pagal personalo kiekį.

3.3 Priemonių parinkimo ir įgyvendinimo logika

Rizikų registras praktinėje dalyje sudarytas vadovaujantis ISO 27005 principu, kad rizikos vertinamos pagal tikimybę ir poveikį, o gauti rezultatai naudojami rizikų tvarkymo sprendimams

parinkti[6]. Remiantis registru ir rizikų tvarkymo suvestine, pirmiausia reikalinga orientuotis į tas rizikas, kurios mažoje įmonėje gali sukelti didžiausias pasekmes, kaip duomenų praradimas, neteisėta prieiga, asmens duomenų atskleidimas ir socialinės inžinerijos atakos. Kad priemonių taikymas būtų aiškus ir realiai įgyvendinamas, siūloma laikytis trijų parastų parinkimo taisyklių:

1. **Pirmiausia diegiamos tik tos priemonės, kurios mažina aukšto prioriteto rizikas.** Tai užtikrina, kad įmonė sprendžia svarbiausias problemas, o ne pradeda nuo smulkių, mažai reikšmingų rizikos mažinimo veiklų.
2. **Pirmenybė teikiama toms priemonės, kurias galima įgyvendinti greitai ir su minimalios investicijomis.** Tai mažoje įmonėje ypač svarbu, nes didžioji dalis saugos veiklų atliekama greta kitų darbų.
3. **Priemonės siejamos su stebėsena ir įrodymais.** Kiekvienam sprendimui turi būti numatyta, kaip bus tai tikrinama ar priemonė veikia, kaip atnaujinimų patikra, kopijų būklė, MFA statusas, NVR būklės įrašas, incidentų žurnalas.

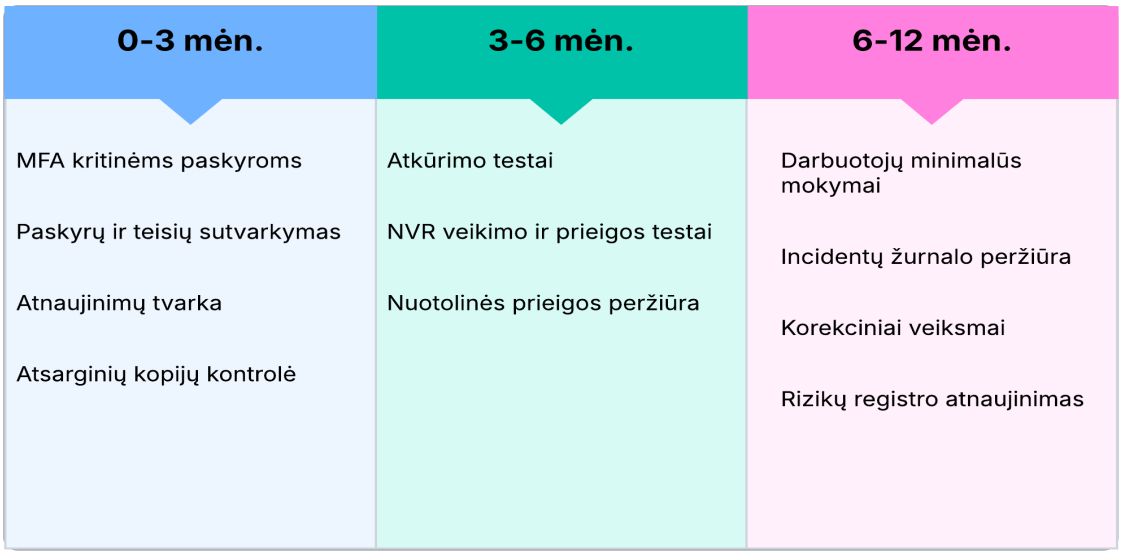
Pagal tokią logiką priemonės sugrupuojamos į įgyvendinimo etapus:

- **Pirmajame etape (0-3 mėn.)** - Nusimatomi baziniai sprendimai, kurie duoda greitą rizikos sumažėjimą. (Paskyrų ir prieigų sutvarkymas, MFA atnaujinimo tvarka, kopijų kontrolė).
- **Antrajame etape (3-6 mėn.)** – Diegiami sprendimai, kurie reikalauja daugiau nuoseklumo ir patikrinimų. (Kopijų atkūrimo testas, NVR veikimo patikra).
- **Trečiajame etape (6-12 mėn.)** – Stiprinamos organizacinės priemonės ir įtvirtinama periodinė priežiūra, kad saugos valdymas taptų nuolatine praktika.

Tokiu būdu priemonių parinkimas tampa tiesiogiai susietas su rizikų registru ir rizikų tvarkymo suvestine, sprendimai pasirenkami pagal rizikos prioritetą, įgyvendinami etapais ir nuolat tikrinami stebėsenos ir incidentų fiksavimo priemonėmis.

9 pav. Priemonių įgyvendinimo etapai

(Sudaryta autoriaus)



0-3mėn. Greiti, didžiausią efektą duodantys veiksmai:

- **Paskyros ir prieigos:** Sutvarkomi prisijungimai, pašalinti bendri prisijungimai, įjungiamas MFA kur įmanoma.
- **Atnaujinimų tvarka :** Susitarti, kas ir kada tikrina operacinės įrangos, maršrutizatoriaus, NVR atnaujinimus ir viską fiksuoja žurnale.
- **Atsarginių kopijų kontrolė:** Nustatomas grafikas, kur laikomos kopijos, kaip tikrinama ar kopija susikūrė be klaidų.
- **Incidentų žurnalo pradžia:** Pradedama fiksuoti visus, net ir minimaliausius incidentus, kaip įtartini laiškai, gedimai, NVR sutrikimai.

3-6 mėn. Patikrinimų etapas

- **Kopijų atkūrimo testas:** Periodiškai tikrinama ar pavyksta atkurti bent vieną failą, katalogą.
- **NVR patikra:** Fiksuojama disko būklė, įrašymo būsena, klaidos.
- **Tinklo bazinis atskyrimas:** Pagal galimybes atskiriamas darbo ir klientų wifi.
- **Trumpi darbuotojų mokymai/instruktažas:** Pateikiamos taisyklės, dėl įtartinų laiškų, pakeistų sąskaitų, bei apibendrinamos kitos saugaus elgesio taisyklės informacinėje erdvėje.

6-12 mėn. Įtvirtinimas, kad sauga taptu nuolatine praktika įmonėje.

- **Minimalios taisyklės raštu:** Kaip elgiamasi su slaptažodžiais, prieigomis, incidentų fiksavimu.

- **Periodinė peržiūra:** Kartą per ketvirtį peržiūrimi stebėsenos ir incidentų žurnalai, nustatomos pasikartojančios problemos ir priimami korekciniai sprendimai remiantis PDCA logika.
- **Rizikų registro atnaujinimas:** Atnaujinamas registras po pokyčių, ar periodiškai (Kas metus jei niekas neįvyksta).

3.4 Minimalūs dokumentų paketas

Praktinėje dalyje suformuoti pagrindiniai valdymo elementai, rizikų registras, rizikų tvarkymo suvertinė, stebėsenos principai ir incidentų registravimo logika. Kad šie rezultatai netaptų tik vieną kartą peržvelgti, reikalingas minimalus, bet aiškus dokumentų paketas. Mažoje įmonėje svarbiausia ne duomenų apimtis, o tai, kad būtų aiškiai apibrėžta, kas ką daro ir kur fiksuojami rezultatai. Mažos žemės ūkio įmonės atveju siūloma laikytis principo, kad kiekviena priemonė turi turėti bent vieną patikrinimo ir įrodymo formą, kaip įrašas žurnale, atliktos patikros rezultatas, ar ekrano nuotrauka. Tokiu būdu sukuriamas paprastas, bet praktikoje veikiantis kontrolės mechanizmas, kur galima greitai patikrinti ar priemonė taikoma ir identifikuoti esamas spragas.

Dokumentai ir registrai turėtų būti laikomi vienoje vietoje, bendrame vietiniame ar debesijos kataloge, o prieiga suteikiama tik pagal poreikį, tai sumažina riziką, kad atsiras kelios skirtingos dokumentų versijos su skirtingais įrašais netinkamoje laiko skalėje.

15 lentelė. Minimalus dokumentų rinkinys

(Sudaryta autoriaus)

Dokumentų grupė	Minimalus turinys	Atnaujinimas arba pildymas
Planavimo dokumentai	Rizikų registras; Rizikų mažinimo suvestinė ir prioritetai	Rizikų registras – 1 kartą per metus ir po pokyčių; suvestinė – 1 kartą per ketvirtį.
Taisyklės	Slaptažodžių ir prieigos taisyklės; Atsarginių kopijų taisyklės; Incidentų valdymo taisyklės	Kas 12 mėn, arba pasikeitus procesams ar vidaus infrastruktūrai
Kontrolės žurnalai	Stebėsenos žurnalas; Atnaujinimų žurnalas; Atsarginių kopijų žurnalas; Incidentų žurnalas	Pildoma pagal nusistatytą grafiką 1sav./1mėn.
Peržiūros įrašai	Peržiūros santrauka, sprendimai, korekcijos, atsakomybės	Pagal nusistatytą grafiką, arba kas 3 mėn.

Kad šis dokumentų paketas būtų realiai naudojamas, rekomenduojama iš anksto nusistatyti paprastą atsakomybės principą, kas už dokumentus yra atsakingas, dažniausiai mažoje įmonėje už

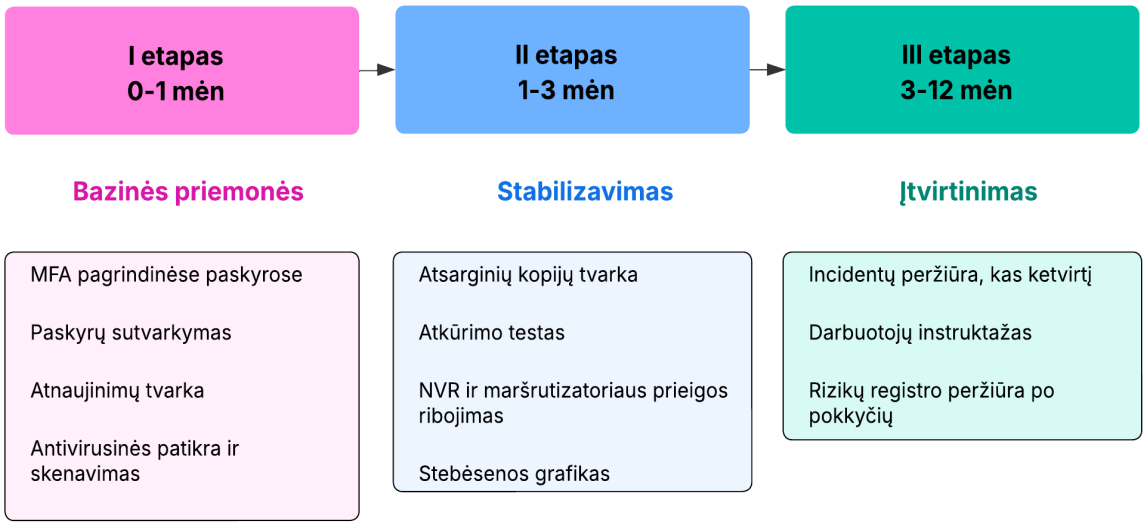
tai atsakingas asmuo yra vadovas, arba jo paskirtas darbuotojas, o techninė pagalba, jeigu reikalinga perkama pagal poreikį iš išorės. Svarbu, kad atsakomybė būtų aiški ir pastovi.

Taip pat, kad palengvinti praktiką, siūloma iš anksto susikurti aiškią dokumentų laikymo vietą, tai leidžia įmonės darbuotojais greitai rasti reikalingus dokumentus ir palaikyti tvarką kompiuteryje ar ant darbo stalo.

3.5 Įgyvendinimo planas

Kas siūlomas informacijos saugos valdymo modelis būtų pritaikomas realiai, priemonės turi būti įgyvendinamos ne iš karto, o etapais. Mažoje įmonėje svarbu pasirinkti tokį planą, kuris nereikalautų daug laiko ir papildomo personalo, bet vis tiek duotų didžiausią rizikos sumažinimą. Todėl aprašytos priemonės suskirstomos į tris etapus, kaip greiti veiksmai (0-1mėn.), stabilizavimas (1-3 mėn.) ir įtvirtinimas (3-12 mėn.). Kiekvienai priemonei pagal galimybes numatomas atsakingas asmuo ir aiškus įrašas, kad priemonė taikoma. Priemonių įgyvendinimo eiga per laiką pateikta 10 paveiksle.

10 pav. Priemonių įgyvendinimo "Kelias" per laiką.
(Sudaryta autoriaus)



Paveiksle matyti, kad pirmame etape numatomi greitai įgyvendinami veiksmai, kurie mažina didžiausias rizikas, antrajame etape dėmesys skiriamas įmonės informacinės erdvės stabilumui, o trečiajame, tai priemonių įtvirtinimas skirtas atlikti periodines peržiūras ir kitus registro atnaujinimus. Taip pat siekiant, kad priemonių įgyvendinimas būtų valdomas praktiškai, kiekvienai priemonei yra nustatomas atsakingas asmuo, terminas, kuriame žurnale paliekamas įrašas apie darbus. Detalus priemonių įgyvendinimo planas pateiktas 16 lentelėje.

16 lentelė. Priemonių įgyvendinimo planas mažai žemės ūkio įmonei

(Sudaryta autoriaus)

Etapas	Priemonė	Atsakingas asmuo	Terminas	Įrašas
1 etapas (0-1mėn.)	Įjungiamas MFA: el.paštas, debesija.	Vadovas/Priskirtas asmuo/IT specialistas	Per 2 savaites	Stebėsenos
1 etapas (0-1mėn.)	Paskyrų tvarkymas: kiekvienas dirba su savo paskyra, nėra bendrų slaptažodžių	Vadovas	Per 1 mėn.	Peržiūros žurnalas (Kas keista)
1 etapas (0-1mėn.)	Nustatyti atnaujinimų tvarką: windows, NVR, tinklo įranga, kita įranga	Priskirtas asmuo	Per 1 mėn.	Atnaujinimų žurnalas
1 etapas (0-1mėn.)	Antivirusinės būklės patikra ir periodinis skenavimas	Priskirtas asmuo	Per 1 mėn.	Stebėsenos žurnalas
2 etapas (1-3mėn.)	Atsarginių kopijų įdiegimas ir jų tvarka, grafikas, laikymo vieta	Priskirtas asmuo IT specialistas	Per 2 mėn.	Kopijų žurnalas
2 etapas (1-3mėn.)	Atkūrimo testas bent vieno failo/aplanko	Priskirtas asmuo	Kas 3 mėn.	Stebėsenos žurnalas
2 etapas (1-3mėn.)	NVR, maršrutizatoriaus prieigos ribojimas, kas turi teises	Vadovas IT specialistas	Per 3 mėn.	Peržiūros žurnalas
2 etapas (1-3mėn.)	Stebėsenos grafikas, kas tikriname kas savaitę/mėnesį	Priskirtas asmuo	Per 2 mėn.	Stebėsenos žurnalas
3 etapas (3-12mėn.)	Incidentų peržiūra kas ketvirtį, kas kartojasi, kokie veiksmai	Vadovas	Kas 3 mėn.	Peržiūros žurnalas
3 etapas (3-12mėn.)	Darbuotojų instruktažas: phishing, slaptažodžiai, kaip elgtis incidento atveju	Vadovas IT specialistas	1 – 2 kartus per metus	Instruktažo įrašas
3 etapas (3-12mėn.)	Rizikų registro peržiūra po pokyčiu, įranga, programos, procesai	Vadovas	Pagal poreikį	Stebėsenos žurnalas

Toks planas yra pritaikytas mažai įmonei, atsakomybės paprastos, terminai realūs, o kiekvienas veiksmas yra fiksuojamas. Tai svarbu tam, kad būtų galima parodyti, ne tik kas buvo planuota, bet ir tai kas yra atlikta.

Šis įgyvendinimo planas leidžia įmonei nebandyti padaryti visko iškarto, o nuosekliai įgyvendinti svarbiausias priemones pirmiausia, svarbiausia dalis šiame plane, kad yra aiškios atsakomybės ir kur turi būti paliekami įrašai apie atliktus darbus, nes būtent įrašai parodo, kad priemonės yra vykdomos praktikoje.

3.6 Prieš ir po vertinimas

Kad siūlomas informacijos saugos valdymo modelis būtų pagrįstas praktiškai, reikalinga įvertinti ne tik, kokios priemonės numatytos, bet ir koks realus pokytis yra pasiekiamas, kai jos pradedamos taikyti. Šiame skyrelyje pateikiamas paprastas „prieš ir po“ palyginimas, pritaikytas mažos įmonės situacijai.

Vertinimas atliekamas kokybiniu principu.

- Prieš – esama būklė, kai priemonės nėra taikomos, arba taikomos nenuosekliai.
- Po – būklė, kai priemonės įgyvendintos pagal 3.5 skyriuje pateikta planą, o jų taikymas patvirtintas įrašais kontrolės žurnaluose.

Būsena „po“ reiškia ne idealų saugumą, o valdoma, patikrinimą ir palaikomą saugos lygį.

17 lentelė. Prieš ir po būklės palyginimas pagal pagrindines sritis

(Sudaryta autoriaus)

Sritis	Prieš	Po	Kaip patikrinama
Prieigos sauga	MFA netaikomas	MFA įjungta pagrindinėse paskyrose	Stebėsenos žurnalo įrašas, nustatymų patikra
Paskyrų tvarka	Naudojamos bendros paskyros ir bendri slaptažodžiai	Kiekvienas darbuotojas dirba tik su savo paskyra, vengiama bendrų slaptažodžių	Peržiūros žurnalo įrašas
Atnaujinimų valdymas	Atnaujinimai daromi nereguliariai, arba kada reikalauja pati programinė įranga	Nustatyta programinės įrangos atnaujinimų tvarka ir vykdoma periodinė patikra	Atnaujinimų žurnalo įrašas
Apsauga nuo kenkėjiškų programų	Kenkėjiškų programų patikra nevykdoma	Periodinė antivirusinės patikra ir skenavimas	Stebėsenos žurnalo įrašas
Atsarginės kopijos	Kopijos nedaromos	Daromos kopijos pagal aiškų grafiką, aiškią laikymo vietą	Kopijų žurnale
Atkūrimo galimybė	Atkūrimo testas neatliekamas	Atliekamas bent vieno failo/aplanko atkūrimo testas kas 3 mėn.	Stebėsenos žurnale
Kritinės įrangos prieinamumas	Neaišku, kas gali prisijungti prie maršrutizatoriaus ar NVR	Prieiga apribota, administratoriaus teisės tik atsakingiems asmenims	Peržiūros žurnale ir įrangos konfigūracijoje
Incidentų valdymas	Incidentai nefiksuojami, sprendžiami vietoje be įrašų	Incidentai registruojami ir peržiūrimi periodiškai	Incidentų žurnale

Lentelėje matyti, kad didžiausias pokytis pasiekiamas ten, kur rizika mažoje įmonėje paprastai būna didžiausia, tai: prieigos saugoje kuri susijusi su MFA ir paskyrų tvarka, atsarginių kopijų turėjimu ir atnaujinimų valdyme. Šios sritis tiesiogiai mažina rizikos tikimybę, atliekant programinės įrangos atnaujinimus, atsiranda mažiau pažeidžiamumų, o galimybė atkurti duomenis po incidento taip pat mažina ir galimą rizikos poveikį.

3.6.1 Pagerėjimo rodikliai užtikrinimas

Kad pagerėjimas būtų ne tik aprašytas, bet ir patikrintas, siūloma taikyti kelis paprastus patikros rodiklius. Kurie yra tinkami mažai įmonei, nes nereikalauja papildomos sistemos ar IT specialisto, pakanka patikrinti kontrolės žurnalus.

- **Atnaujinimų kontrolė:** Patikrinti ar per mėnesį atlikta bent viena patikra ir ar yra įrašas naujinimų žurnale (Taip/Ne).
- **Atsarginės kopijos:** Ar visos savaitės kopijos pažymėtos, kaip sėkmingos kopijų žurnale? (4/4 savaitės).
- **Atkūrimo testas:** Ar per 3 mėn. buvo atliktas bent vienas atkūrimo testas (Taip/Ne).
- **Incidentų registravimas:** Ar kiekvienas incidentas buvo pažymėtas incidentų žurnale? (Taip/Ne).
- **Kelių faktorių autentifikavimas:** Ar MFA įjungtas visose pagrindinėse paskyrose? (Taip/Ne).

Tokie rodikliai leidžia greitai ir lengvai įvertinti, ar saugos priemonės yra palaikomos nuolat, ar sudiegtos tik „tam kartui“.

3.6.2 Likutinė rizika

Įgyvendinus priemones pagal planą, dalis rizikų išlieka – likutinė rizika. Tai yra normali rizikų valdymo dalis, nes užtikrinti 100% saugą sunkiai įmanoma, o saugos sprendimai visuomet balansuoja tarp saugumo, patogumo ir finansų.

Likutinės rizikos logika aiškiai matoma ir standartuose. ISO 27001 6.1.3 punktas reikalauja, kad po rizikos tvarkymo būtų gautas rizikos savininkų pritarimas, ne tik planui, bet ir tam, kas lieka po priemonių pritaikymo [4]. Nis taip pat apibrėžia, kad likutinė rizika yra dalis, kuri lieka pritaikius sprendimus [8].

Praktikoje, mažos žemės ūkio įmonės atveju likutinė rizika pasireiškia, kaip:

- **Socialinė inžinerija (Phising):** Pilnai neišnyksta, bet MFA ir periodinis instruktažas/mokymai stipriai sumažina grėsmę, nes MFA dėka nutekintas slaptažodis nebus tinkamas pilnam prisijungimui.
- **Techninių gedimų rizika:** Duomenų diskai, elektros sutrikimai, įrangos neveikimas išlieka taip pat, tačiau kopijos ir atkūrimo galimybė sumažina veiklos neveikimo trukmę.
- **Kritinės įrangos pažeidimo rizika(NVR, maršrutizatorius):** Rizika išlieka, bet prieigos ribojimas ir periodinė peržiūra ją padaro labiau valdoma, mažėja tikimybė kad pažeidimas įvyks per netinkamas teises, ar silpną administravimą.

Šiame darbe „pasiekiamas rezultatas“ suprantamas, kaip praktiškai įgyvendinamas minimumas, kai visos svarbiausios rizikos yra sumažinamos iki priimtino lygio, o likutinė rizika yra aiškiai suprantama ir valdoma. Jei stebėsenos įrašuose arba incidentų žurnale matoma, kad tam tikros problemos kartojasi, tai tampa pagrindu koreguoti jau priimtas priemones, bet visi šie procesai atitinka nuolatinės stebėsenos idėją, kad sauga turi būti reguliariai vertinama ir prižiūrima, nes grėsmės ir pažeidžiamumai taip pat keičiasi. Tai taip pat dera ir su ISO 27001 nuostata, dėl nuoseklaus gerinimo ir korekcijų taikymo, kai nustatomos pasikartojančios problemos [4].

Bendrai apibendrinant, trečiajame skyriuje, remiantis antrojo skyriaus praktinės dalies rezultatais, buvo suformuotas mažos žemės ūkio įmonės minimalus informacijos saugos valdymo modelis, nustatytos prioritetinės priemonės, numatytas jų įgyvendinimas etapais, apibrėžtas minimalus dokumentų ir įrašų rinkinys, bei pateiktas poveikio vertinimas. Toks modelis yra realistiškas mažai įmonei, nes remiasi aiškia atsakomybe ir paprastais įrašais kurie leidžia matyti darbų eigą.

IŠVADOS

1. Išnagrinėjus informacijos saugumo ir rizikų valdymo teorinius modelius nustatyta, kad ISO 27001 ir ISO 27005 standarto principai sudaro aiškią logiką, kaip mažoje įmonėje sistemiškai valdyti saugą, tai, kad reikalinga apibrėžti kontekstą, identifikuoti rizikas, parinkti priemones ir nuosekliai vertinti rezultatus. Toks požiūris leidžia saugą vertinti ne kaip vienkartinį techninių sprendimų rinkinį, o kaip valdomą procesą.
2. Išanalizavus ir aptarus teisinį ir organizacinį informacijos saugumo valdymo aspektą, galima teigti, kad mažai įmonei svarbiausia yra praktinis aspektas, kaip aiškios atsakomybės, minimalios taisyklės prisijungimams prie sistemų ir duomenų tvarkymui, incidentų fiksavimui bei periodinėms patikroms. BDAR reikalavimai tiesiogiai siejasi su prieigos kontrole, duomenų apsauga ir įrašų turėjimu, o NKSC gairės padeda pasirinkti realistiškas organizacines ir technines priemones mažos įmonės kontekste
3. Įvertinus mažos žemės ūkio įmonės informacinės sistemos saugos būklė, nustatyta, kad bazinės priemonės egzistuoja, tačiau didžiausi trūkumai siejasi su taisyklių ir nuoseklių procesų nebuvimu. Praktiniu požiūriu labiausiai pažeidžiamos sritys yra prieigos, atsarginės kopijos, darbuotojų supratinimas, kas yra informacinė sauga ir stebėsena. Būtent šie aspektai lemia realų incidentų pasikartojimą ir veiklos tęstinumą.
4. Sudarius rizikų registrą ir įvertinus rizikų tikimybę bei poveikį pagal ISO 27005 metodiką, nustatyta, kad aukščiausio prioriteto rizikos yra duomenų praradimas, neteisėta prieiga prie tinklo ir sistemų, klientų duomenų nutekinimas, bei socialinės inžinerijos atakos. Vidutinio lygio rizikos daugiausiai siejasi su technine įranga, bei fizine sauga, kaip įrangos gedimai, vaizdo įrašų praradimas ar vagystė, todėl jos turi būti valdomos paprastomis, bet aiškiai aprašytomis priemonėmis.
5. Pasiūlius rizikų valdymo priemones ir parengus minimalų ISVS modelį nustatyta, kad mažai įmonei tinkamiausias būdas yra taikyti nuoseklų valdumą, paremta ISO 27001 kontrolėmis ir PDCA logika, tai aiškiai paskirstytos atsakomybės, apibrėžti stebėsenos objektai, incidentų žurnalas ir reguliarūs patikrinimai. Didžiausią poveikį duoda mažiausiai kainuojančios, bet tuo pačiu ir efektyvios priemonės, kaip MFA, slaptažodžių politika, periodinis darbuotojų instruktažas, tai mažina dažniausiai pasitaikančias grėsmes.

Apibendrinant galima teigti, kad darbo tikslas pasiektas – suformuotas rizikų vertinimo pagrindas, rizikų registras, praktiškai pritaikomas nuolatinio gerinimo modelis, kuris leidžia kontroliuoti likutinę riziką, per stebėseną, naujinimus, bei korekcinius veiksmus.

LITERATŪRA

1 *Algimantas Venčkauskas, Egidijus Kazanavičius. (2011). Informacinių technologijų saugos metodai: mokomoji knyga.*

2 *Georg Disterer (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information security, 2013, 4, 92-100.*

3 *Majerník M., Daneshjo N., Chovancová J., Sančiová G. (2017) Design of integrated management systems according to the revised iso standards. vol.15 no.1.*

4 *international standart ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems —Requirements. Third edition 2022-10.*

5 *British standard. Information security management systems – Part 3: Guidelines for information security risk management. BS 7799-3:2006.*

6 *Arief Prabawa Putra, Benfano Soewito. Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector.*

7 *Andrius Januta, Leonardas Marozas, Nikolaj Goranin. (2011) Informacinės saugos audito vykdymas remiantis ISO/IEC 27000 šeimos standartų reikalavimais.*

8 *Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri.(2017) NIST Special Publication 800-12 Revision. An Introduction to Information Security.*

9 *Arvydas Survila. (2015). Nepaprastųjų situacijų valdymas.*

10 *L. Pan & A. Tomlinson. (2016) A systematic review of information security risk assessment.*

11 *Cath Everett. (2011) A risky business: ISO 31000 and 27005 unwrapped.*

12 *NKSC. Kibernetinių grėsmių mažoms ir vidutinėms įmonėms vertinimas.*

13 *Europos sąjungos oficialus leidinys. (2016). dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).*

14 *CIS Controls. CIS Controls Lithuanian Translation. Version 7.*

15 *NKSC. (2024).Kibernetinio saugumo rekomendacijos kibernetinio saugumo objektams.*

16 NKSC, Nacionalinė kibernetinio saugumo būklės ataskaita. (2024) [žiūrėta 2025 11 01] Prieiga internete: https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2024.pdf

17 NKSC, Rekomendacijų leidinys (2025) [žiūrėta 2025 11 05] Prieiga internete: https://www.nksc.lt/doc/biuleteniai/Rekomendacija_10-leidinys.pdf

18 Valstybinė duomenų apsaugos inspekcija, Vaizdo stebėjimas pagal Bendrąjį duomenų apsaugos reglamentą: sąvokos ir paaiškinimai. (2020) [žiūrėta 2025 11 05] Prieiga internete: https://vdai.lrv.lt/uploads/vdai/documents/files/02_%20Lankstinukas%20Vaizdo%20stebejimas%202020-02-20.pdf

19 Lietuvos Respublikos Seimas, Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428. (2014). [žiūrėta 2025 11 10] Prieiga internete: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/gvublQsHZD?jfwid=

20 European DIGITAL SME Alliance. (2025) SME GUIDE: Implementation of ISO/IEC 27001:2022 on information security management. [žiūrėta 2025 11 10] Prieiga internete: https://sbs-sme.eu/wp-content/uploads/2025/12/SBS-Guide_Implementation-ISOIEC-27001_final.pdf

21 NKSC. (2024). Nacionalinė kibernetinio saugumo būklės ataskaita. [žiūrėta 2025 11 05] Prieiga internete: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2024.pdf

22 Valstybinė duomenų apsaugos inspekcija. (2025). Pranešimas apie asmens duomenų saugumo pažeidimą. [žiūrėta 2025 11 10] Prieiga internete: https://vdai.lrv.lt/lt/adsp-ir-dap/pranesimas-apie-asmens-duomenu-saugumo-pazeidima/

23 Lietuvos Respublikos įmonių atskaitomybės įstatymas 4str. [žiūrėta 2025 11 20] Prieiga internete: https://www.infolex.lt/ta/30590:str4

24 Worl Economic Forum. (2025). Global Cybersecurity Outlook 2025. [žiūrėta 2025-10-15] Prieiga internete:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

25 E.Saugumas. Kaip vyksta duomenų viliojimas (angl. phishing)? [žiūrėta 2025 11 20] Prieiga internete: https://esaugumas.lt/articles/kaip-vyksta-duomenu-viliojimas-angl-phishing

26 NKSC. (2025) Rekomendacijos dėl elektroninio pašto saugumo kontrolės priemonių. [žiūrėta 2025 11 20] Prieiga internete: https://www.nksc.lt/doc/biuleteniai/Rekomendacijos%20dėl%20elektroninio%20pašto%20saugumo%20kontrolės%20priemonių.pdf

27 NKSC. Rekomendacijos, kaip suorganizuoti imitacines socialinės inžinerijos pratybas. [žiūrėta 2025 12 10] Prieiga internete: https://www.nksc.lt/doc/biuleteniai/rkgc_phishing_pratybu_rekomendacija.pdf

PRIEDAI

Priedas Nr. 1. Pilnas rizikų registras sudarytas autoriaus

18 lentelė. Pilnas rizikų registras

Nr.	Rizika	Grėsmės šaltinis	Paveikiamas turtas	Pažeidžiamumas	Tikimybė	Poveikis	Rizikos lygis
1	Duomenų praradimas	Įrangos gedimas, kenkėjiškos programos	Prekybos ir apskaitos duomenys	Nėra atsarginių kopijų	4	5	Aukšta
2	Neteisėta prieiga prie vidaus tinklo	Neautorizuoti asmenys	Vidiniai duomenys	Nėra tinklo segmentacijos	3	4	Aukšta
3	Klientų duomenų nutekinimas	Žmogiškoji klaida	Klientų duomenys	Nėra personalo mokymų	3	5	Aukšta
4	Kompiuterinės įrangos gedimas	Techninis gedimas	Darbo vieta	Nėra atsarginės įrangos	3	4	Vidutinė
5	Vaizdo įrašų praradimas	Techninis gedimas	Vaizdo stebėjimo įrašai	Nėra atsarginių kopijų	3	3	Vidutinė
6	Slaptažodžių vagystė	Silpni slaptažodžiai	Informacinių sistemų prieiga	Nėra tinkamos slaptažodžių politikos	3	4	Vidutinė
7	Socialinės inžinerijos atakos	Sukčiavimo laiškai	Prisijungimo duomenys	Nėra personalo mokymų	4	4	Aukšta
8	Vagystė	Fizinė grėsmė	IT ir kita įranga	Ribota fizinė apsauga	2	4	Vidutinė

Priedas Nr. 2. Pilna rizikų valdymo sprendimų suvestinė sudaryta autoriaus

19 lentelė. Pilna rizikų valdymo sprendimų suvestinė

Nr.	Rizika	Rizikos lygis	Valdymo būdas	Valdymo krypties pavyzdžiai	Prioritetas
1	Duomenų praradimas	Aukštas	Mažinimas	Įdiegiamas aiškus atsarginių kopijų darymo grafikas. Kopijas laikyti atskirai nuo pagrindinių kompiuterių, kaip išoriniame diske, ar kitoje vietoje. Periodiškai tikrinti kopijas, ar jos tiksliai atkuriamos	1
2	Neteisėta prieiga prie tinklo	Aukštas	Mažinimas	Pakeičiami Wi-Fi prisijungimai į unikalius, reguliariai atnaujinama programinė įranga, apribojamos nuotolinės administracijos prieigos iki būtiniausių. Atskiriami Wi-Fi tinklai, nuo darbo tinklo	1
3	Klientų duomenų nutekinimas	Aukštas	Mažinimas	Ribojama prieiga prie klientų duomenų tik tiems darbuotojams, kuriems jų reikia. Naudoti windows aplinkoje atskiras darbuotojų aplinkas. Nesaugoti klientų duomenų atsitiktinėse vietose, o nustatyti bendra jų laikymo vietą. Įvesti minimalios reikalingos informacijos kiekio taisyklę.	1
7	Socialinės inžinerijos atakos	Aukštas	Mažinimas	Darbuotojams paaiškinami dažniausi sukčiavimo būdai, kaip įtartini laiškai, nuorodos ar skubūs dokumentų pasirašymai. Įvesti taisyklę, kad gautus mokėjimo aš saskaitų pakeitimus papildomai tikrinti. Įvesti pranešimo tvarką, pastebėjus įtartiną pranešimą ar panašią situaciją.	1
4	Kompiuterinės įrangos gedimas	Vidutinis	Mažinimas/Perkėlimas	Reguliariai naujinama operacinė sistema ir programos, naudojama antivirusinė programinė įranga, periodiškai tikrinamas disko turinys ir pats kompiuterio veikimas. Nusimatyti atsarginį planą įrangos gedimo atveju, kaip laikinas kitas kompiuteris. Įsigyti pagal galimybes išorinę IT priežiūrą pagal poreikį.	2
5	Vaizdo įrašų praradimas	Vidutinis	Mažinimas	Apriboti prieigą prie NVR serverio, kaip atskiri prisijungimai su atskiromis rolėmis. Periodiškai tikrinti ar vyksta įrašymas. Stebėti diskų būklę ir atlikti atnaujinimus. Nusimatyti įrašų eksportavimą į kitą talpyklą kritiniu atveju.	2
6	Slaptažodž	Vidutinis	Mažinimas	Įvesti slaptažodžių taisykles, kaip pakankamas	2

Nr.	Rizika	Rizikos lygis	Valdymo būdas	Valdymo krypties pavyzdžiai	Prioritetas
	ių vagystė			ilgis, unikalus ir nenaudojamas kitur. Jei įmanoma įjungiamas MFA apsauga. Periodiškai tikrinti prieigas ir keisti slaptažodžius pasikeitus personalui arba įvykus ar įtariant incidentui.	
8	Vagystė	Vidutinė	Mažinimas/Perkėlimas/Priėmimas	Užtikrinti patalpų rakinimo ir raktų kontrolę. Laikyti vertingą IT įranga viešai neprieinamose vietose, naudoti užrakinamas spintas, seifus ir patalpas. Periodiškai tikrinti signalizacijos ir vaizdo stebėjimo sistemų veikimą. Įvertinti draudimo galimybę.	3