Kauno technologijos universitetas

Informatikos fakultetas

Prieigos valdymo politikos automatizuoto įgyvendinimo sistema

Baigiamasis magistro studijų projektas

Vaidas Kazragis

Projekto autorius

Prof. Algimantas Venčkauskas

Vadovas

Kaunas, 2020 m.

Kauno technologijos universitetas

Informatikos fakultetas

Prieigos valdymo politikos automatizuoto įgyvendinimo sistema

Baigiamasis magistro studijų projektas

Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vaidas Kazragis

Projekto autorius

Prof. Algimantas Venčkauskas

Vadovas

doc. Tomas Adomkus

Recenzentas

Kaunas, 2020 m.

Kauno technologijos universitetas

Informatikos fakultetas

Vaidas Kazragis

Prieigos valdymo politikos automatizuoto įgyvendinimo sistema

Akademinio sąžiningumo deklaracija

Patvirtinu, kad mano, Vaido Kazragio, baigiamasis projektas tema „Prieigos valdymo politikos automatizuoto įgyvendinimo sistema“ yra parašytas visiškai savarankiškai ir visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka)	(parašas)

Kauno technologijos universitetas

Informatikos fakultetas

Baigiamojo magistro projekto užduotis

Projekto tema: Prieigos valdymo politikos automatizuoto įgyvendinimo sistema

Reikalavimai ir sąlygos (tikslinti pavadinimą pagal poreikį)

Vadovas / Vadovė

(vadovo pareigos, vardas, pavardė, parašas) (data)

Kazragis, Vaidas. Prieigos valdymo politikos automatizuoto įgyvendinimo sistema. / Magistro studijų baigiamasis projektas / vadovas prof. Algimantas Venčkauskas; Kauno technologijos universitetas, informatikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Informacijos ir informacinių technologijų sauga (kodas 621E10003).

Reikšminiai žodžiai: Prieigos sauga, prieigos saugos politika, automatizavimas, prieigos teisės, XML, RBAC, rolės, ACL, prieigos valdymas, prieigos valdymo politika.

Kaunas, 2020 m. 71 p. (be priedų)

Santrauka

Informacijos ir informacinių technologijų apsauga – tai įrankių ir sprendimų visuma, taikoma siekiant apsaugoti tai, kas dabar svarbiausia – informaciją. Dėl įvairių išorinių ir vidinių veiksnių nuolat kyla grėsmė šiam turtui būti tyčia ar netyčia pažeistam, pakeistam ar sunaikintam. Apsauga neapsiriboja vien tik fiziniu pačios įrangos saugumu, dabar plačiai taikomos papildomos programinės priemonės, kurios didiną saugumą ir kontrolę, ir tik kompleksiškas ir apgalvotas tokių priemonių naudojimas užtikrina informacijos vientisumą, prieinamumą ir konfidencialumą.

Be gausybės technologinių sprendimų, rinkoje siūlomi geruųjų informacinės saugos praktikų rinkiniai, kurių tinkamas pritaikymas organizacijose yra net svarbesnis nei skirtingų apsaugos mechanizmų ar taikomųjų programų duodama nauda. Dauguma šios srities specialistų sutaria, kad gerai įgyvendinta informacinės saugos politika yra kritiškai svarbus visapusiškos saugos elementas. Deja, ne kiekviena įmonė pasiruošusi tokios politikos pritaikymui dėl įvairių priežasčių – nepakankamas noras keistis, atsisakyti ydingų įpročių ir praktikų, verslo modelio nesuderinamumas su bandoma pritaikyti politika, tinkamų specialistų trūkumas ir pan., o kur dar priežiūra ir palaikymas po politikos įgyvendinimo, auditas, ar viskas atlikta tinkamai ir taip, kaip politika reikalavo. Todėl svarbu iškilusius iššūkius spręsti, bandant panaudoti automatizavimo galimybes, kas palengvintų administratorių ir organizacijos vadovų darbą, sąnaudas bei visą tai leistų nukreipti į kitas silpnesnes saugos sritis.

Prieigos saugos politika yra bene pagrindinė politika iš viso rinkinio ir jos įgyvendinimas duoda didžiausią naudą, todėl kaip įmanoma supaprastinus ir automatizavus jos pritaikymą, būtų galima visoms organizacijoms pasiūlyti ją susidiegti ir taip paskatinti pradėti rūpintis savo informacinių šaltinių apsaugą.

Kazragis, Vaidas. System of Automated Implementation of Access Control Policy. / Master's Final Degree Project / supervisor prof. Algimantas Venčkauskas; Faculty of Informatics, Kaunas University of Technology.

Study field and area (study field group): Security of Information and Information Technology (Reference 621E10003).

Keywords: Access security, access security policy, automation, access permissions, XML, RBAC, roles, ACL, access control policy, access control.

Kaunas, 2020. 71 pages (ex. Annexes).

Summary

Security of information and information technologies – that's a collection of tools and solutions to reach the highest possible security level to protect the most valuable resource – information. Because of many different external and internal factors there is constant threat for this asset to be modified, leaked or deleted. The security is never only physical perimeter protection, it is a combination of physical and cyber security, and only this kind of approach could help organization stick to CIA model.

Despite all the security software and hardware out there in the market, there are also sets of best practices which provide great value if implemented properly. Many IT security professionals agree that well implemented information security policy is crucial for any organization. Unfortunately, not everyone is prepared to handle this kind of task because of its complexity, confrontation with business model, lack of specialists and so on. Moreover, it has to be well maintained and audited, so it is important to solve similar issues by using automation where possible. That could save effort and money for business.

Access security policy is fundamental for all the security policy, so it would give a great value if organization could implement at least that one. So automatization of the process would let many other organizations have this implementation finally available and that could be a great start to take care of information security.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

Santrumpos:

ACL (Access Control List) – prieigos valdymo sąrašas.

CIA (Confidentiality, Integrity, Availability) – konfidencialumas, vientisumas ir prieinamumas.

DAC (Discretionary Access Control) – diskretinis prieigos valdymo modelis.

ISMS (Information Security Management System) – informacinės saugos valdymo sistema.

RBAC (Role-Based Access Control) – rolėmis grįstas prieigos valdymas.

SDLC (System development life cycle) – sistemos vystymo gyvavimo ciklas.

XML (Extensible Markup Language) – plečiama duomenų struktūrų aprašomoji kalba.

ACL (Access Control List) – prieigos valdymo sąrašas.

ĮVADAS

Darbo problematika ir aktualumas

Informacijos ir informacinių technologijų apsauga – tai įrankių ir sprendimų visuma, taikoma siekiant apsaugoti tai, kas dabar svarbiausia – informaciją. Dėl įvairių išorinių ir vidinių veiksnių nuolat kyla grėsmė šiam turtui būti tyčia ar netyčia pažeistam, pakeistam ar sunaikintam. Apsauga neapsiriboja vien tik fiziniu pačios įrangos saugumu, dabar plačiai taikomos papildomos programinės priemonės, kurios didiną saugumą ir kontrolę, ir tik kompleksiškas ir apgalvotas tokių priemonių naudojimas užtikrina informacijos vientisumą, prieinamumą ir konfidencialumą.

Organizacijose, ypač tose, kurios dirba su užsienio partneriais, vis dažniau įgyvendinamos įvairių tarptautinių standartų organizacijų teikiamos metodikos ar jų rinkiniai (ISO27001, NIST, COBIT, British Standard ir kt.). Labai dažnai tai būna būtina sąlyga tęsti komercinei veiklai. Viena iš sudedamųjų šių metodikų ar geruų praktikų dalių yra prieigos valdymas, kuris padeda apsaugoti duomenis tiek nuo netyčinių informacijos naudotojų veiksmų, tiek ir nuo tikslinių atakų. Infrastruktūros, kuriose nėra arba prastai įgyvendinta prieigos valdymo politika, patirs daug didesnius intelektualinius bei materialinius nuostolius bet kurios iš šių atakų atveju.

Darbo tikslas ir uždaviniai

Tikslas: sukurti paprastą ir efektyvų prieigos valdymo politikos įgyvendinimo metodą, kuris leistų automatizuoti organizacijos vadovų patvirtinto prieigos politikos dokumento panaudojimą prieigos taisyklių prie informacinių resursų nustatymui.

Uždaviniai

1. Išanalizuoti informacijos saugos politikos formavimo metodus;
2. Nustatyti efektyviausius prieigos valdymo modelius;
3. Suformuoti automatizuoto prieigos valdymo politikos įgyvendinimo metodą;
4. Sudaryti natūralia kalba parašyto dokumento konvertavimo į mašininį kodą modelį;
5. Sudaryti prieigą įgyvendinančių scenarijų formavimo proceso modelį;
6. Realizuoti sukurtą prototipą virtualioje infrastruktūroje.

Darbo struktūra

Šis darbas suskirstytas į tokias dalis:

- Pirmoje dalyje atliekama informacijos ir informacinių technologijų saugos sprendimų analizė, apžvelgiamos grėsmės ir rizikos. Gilinamasi į informacinės saugos politikas ir jas aprašančius standartų rinkinius. Analizuojami prieigos valdymo modeliai ir jų pritaikymas šiame darbe.
- Antroje dalyje formuojamas automatizuoto prieigos valdymo įgyvendinimo metodas, kuris diktuoja sąlygas tolimesniam prototipo kūrimui ir realizavimui.
- Trečioji dalis skirta prototipo kūrimui, funkcinių ir nefunkcinių reikalavimų nustatymui bei jo realizavimui virtualioje infrastruktūroje;

- Paskutinėje darbo dalyje pateikiami atlikti tyrimai ir eksperimentai bei aptariami jų rezultatai.
- Pateikiamos darbo išvados;
- Darbo pabaigoje pateikiamas naudotos literatūros sąrašas, kuriame šaltiniai lietuvių ir anglų kabomis.

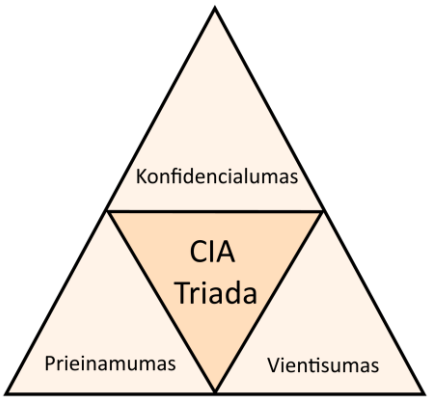
1. INFORMACINĖS SAUGOS POLITIKOS ĮGYVENDINIMO ANALIZĖ

1.1. Informacijos sauga

Jau seniai praeityje tie laikai, kai kompiuterio, asmeninio ar įmonės, apsauga paliekama paties vartotojo atsakomybei, o pagrindinis ginklas kovai su kibernetinėmis grėsmėmis – antivirusinė programa. Šiuolaikiniame pasaulyje, kai organizacijų turimi informaciniai sistemų pajėgumai ir duomenų kiekiai nuolat auga, nebeužtenka bazinio požiūrio į informacijos ir technologijų apsaugą, nes šie resursai yra kritiniai įmonių veiklos tęstinumui. Akivaizdu, kad augant šios informacijos svarbai, auga ir piktavalių noras ją užvaldyti, pakeisti ar sunaikinti, o dabartinės informacinių technologijų galimybės senąsias gynybos taktikas gali paversti neįgaliomis. Dėl šios priežasties informacijos saugos apibrėžimai einant laikui įvairiuose šaltiniuose vis pasikeičia, nes tampa vis platesnis, abstraktesnis ir sudėtingesnis, tačiau iš esmės tai - informacijos ir informacinių sistemų apsauga nuo neteisėtos prieigos, naudojimo, atskleidimo, sutrikdymo, modifikavimo ar sunaikinimo. Šis apibrėžimas paremtas fundamentiniu CIA saugos modeliu, kuriuo vadovaujantis kuriami standartų rinkiniai ir gerosios praktikos, užtikrinančios visapusišką įmonės informacinio turto apsaugą.

1.1.1. CIA modelis ir jo reikšmė informacijos saugumui

CIA triadą sudaro konfidencialumas, vientisumas ir prieinamumas. Kompiuterinės sistemos ne tik jungia verslo procesus, tačiau juos ir valdo. CIA yra gerai žinomas informacijos saugumo vystymo modelis, kuris taikomas įvairiose situacijose, siekiant nustatyti problemas ir trūkumus, bei nustatyti ir įgyvendinti saugumo sprendimus. Nors verslo turtas gali būti vertinamas pagal jo darbuotojus, pastatus ar valdomus pinigus, tačiau didžioji turto dalis yra saugoma informacijos forma kaip elektroniniai duomenys ar rašytiniai dokumentai.



1.1 pav. CIA triados modelis

Jei ši informacija atskleidžiama pašaliniams asmenims, ji yra netiksli arba prireikus nepasiekiama, įmonė gali patirti didžiulę žalą, pavyzdžiui, prarasti klientų pasitikėjimą, neįvykdyti sutarties sąlygų, prarasti rinkos dalį ir pan. Blogiausiu atveju, nesugebėjimas įmonėje kontroliuoti informacijos, gali sukelti didelių finansinių nuostolių arba reguliavimo apribojimų, susijusių su galimybe verstis verslu [1].

1.1.2. Informacijos saugos problemos ir grėsmės

Informacijos saugos strategija ir metodai priklauso nuo organizacijos identifikuotų grėsmių jos veiklai, intelektualinei nuosavybei, turtui ir informacijai. Tik įvardinus šias grėsmes bus galima daug kokybiškiau formuoti informacijos saugos politiką, o to nepadariusios įmonės atveria didžiules spragas piktavaliams tiesiog sunaikinti net ir sėkmingiausią verslą.

Įvardinus grėsmes, suformuojamas aiškus vaizdas, kurie duomenys yra jautriausi įmonės veiklos tęstinumui. Informacijos svarbai nusakyti yra naudojamos įvairios kategorijos, į kurias ji yra suskirstoma. Pavyzdžiui, JAV vyriausybė naudoja penkių lygių informacijos klasifikacijos sistemą [2]:

1. neklasifikuota informacija;
2. viešojo pasitikėjimo;
3. konfidenciali;
4. slapta;
5. visiškai slapta.

Priklausomai nuo priskirto konfidencialumo lygio, informacijai taikomi ir atitinkami prieigos ir redagavimo apribojimai, saugojimo, atsarginių kopijų darymo taisyklės, archyvavimo sąlygos ir pan. Kai kurios organizacijos tam taiko net papildomus klasifikatorius, kurie apibrėžtų atitinkamas sąlygas.

Rekomenduotina apžvelgti ir galimus atakos vektorius, kuriais didžiausia tikimybė sulaukti atakų. Dažniausiai, tą sufleruoja silpniausios infrastruktūros grandys, personalo žinios, jautriausios informacijos tipas ir saugojimo būdas. Organizuojamos atakos priežastys:

- siekiama asmeninės naudos;
- siekiama atkeršyti ar pakenkti;
- dėl politinės veiklos;
- netyčinė pavojinga veikla;
- asmeninių ambicijų tenkinimas;
- siekiant sutrikdyti sistemų veiklą
- šnipinėjimas;
- asmeninės informacijos vagystė;
- kita nusikalstama veika.

Verizon kompanijos paskelbtoje 2019 metų saugumo incidentų ir įsilaužimų apžvalgoje galima įžvelgti dominuojantį atakų tikslą, kuris nukreiptas į finansinę naudą užvaldant įmonės finansinius ar intelektualinius turtus. Net 71% visų atakų, anot Verizon saugumo specialistų, buvo grindžiamos finansine nauda, o kas ketvirta ataka – siekiant įgyti konkurencinį pranašumą rinkoje arba pasisavinti intelektualinę nuosavybę. Pateiktame paveiksle (1.2 pav.) taip pat matoma, kad du trečdaliai atakų įvykdytos įsilaužėlių iš išorės, o pusė jų – priklauso nusikalstamoms organizacijoms.

1.2 pav. 2019 metų įsilaužimų apžvalga [3]

Taip pat šioje kasmetinėje Verizon saugumo apžvalgoje pateikiamos įžvalgos, kad pastaruoju metu itin auga socialinio pobūdžio kenkėjiška veikla, kuri pasireiškia tiek klaidinančių svetainių spąstais, tiek apgavikiškais elektroniniais laiškais su prašymais paviešinti informaciją ar atlikti finansines operacijas.

1.2. Informacinės saugos politika

Organizacijos sėkmė kovoje su grėsmėmis informacijos ir technologijų saugumui prasideda nuo informacijos saugos politikos, kuri apibrėžiama kaip aukšto lygio organizacijos pareiškimas, kuriame atsispindi jos įsitikinimai, siekiai ir tikslai, įgyvendinimo. Šalia politikos visada turi būti įdiegti standartai, procedūros ir gairės, kurios padėtų pačią politiką geriau įgyvendinti [4]. Yra laikoma, kad organizacija, kuri investuoja į saugumo sprendimus neturėdama saugumo politikos yra labiau pažeidžiama, nei ta, kuri turi aiškią ir gerai įgyvendintą saugumo politiką, tačiau mažiau galimybių investuoti pinigus į technologinius sprendimus, ir taip yra todėl, kad ji žino, kaip elgtis vienoje ar kitoje situacijoje, ką konkrečiai saugo ir kaip palaipsniui tą saugumą didinti.

Dažnu atveju tai yra bendrinis dokumentas, be specifinių detalių, tačiau galintis turėti žemiau pateiktą struktūrą.

1. Informacinės saugos politikos tikslas. Aprašoma kuriam tikslui yra rengiama informacinės saugos politika, pvz. aprašyti bendruosius informacijos saugos principus organizacijoje, apsaugoti organizacijos reputaciją ir t.t.

2. Informacinės saugos politikos taikymo imtis. Idealiu atveju informacinė saugos politika turėtų apimti visą informaciją, informacines sistemas, organizacines ir technines priemones bei procesus kurie yra vyksta organizacijoje. Tačiau taikymo imtis gali būti koreguojama pirmajame punkte iškeltiems tikslams pasiekti.

3. Organizacijos personalo pareigos įgyvendinant informacinės saugos politiką. Įvertinus organizacijos personalo gebėjimus, procesus, kurie vyksta organizacijoje, organizacijos vidines tvarkas ar taisykles, ir organizacijos struktūrą, turi būti aiškiai ir paprastai apibrėžiamos personalo rolės ir atsakomybės sritys įgyvendinant saugos politiką.

4. Valdymo ir prieigos kontrolė. Pagal organizacijos struktūrą ir pareigybes turi būti identifikuojamos prieigos teises prie antrame punkte nustatytos imties. Turi būti aišku koks asmuo kokią teisę turi ir kas jam yra draudžiama (pvz. projektų vadovas gali susipažinti su informacija įgyvendinant jam priskirtus projektus, tačiau neturi teises pasiekti jam nepriskirtų projektų).

5. Duomenų klasifikavimas ir darbas su tokiais duomenimis. Kiekvienoje organizacijoje duomenims galima suteikti klasifikaciją ir kaip su kokia informacija turi būti dirbama. Šalies, kurioje veikia organizacija, teisės aktai gali reglamentuoti tam tikrų duomenų tvarkymą ir saugojimą, todėl tokio tipo duomenys privalo būti identifikuoti ir suklasifikuoti, o duomenys, kurie yra sukuriami pačios organizacijos ir kurių tvarkymo nereglamentuoja teisės aktai gali būti klasifikuojami pagal pačios organizacijos nustatytus kriterijus.

6. Bendrieji informacinių technologijų saugumo reikalavimai. Yra nurodomi gana abstraktūs reikalavimai kokia informacinė sistema organizacijoje turi būti, kas ją turi sudaryti, kur turi būti įrengta ir kaip turi funkcionuoti. Elementarus pavyzdys galėtų būti: kompiuterinėse darbo vietose turi būti įdiegta nuolatos atnaujinama antivirusinė programinė įranga, užtikrinamas operacinės sistemos ir įdiegtos programinės įrangos nuolatinis centralizuotas atnaujinamas, tarnybinės stotys ir tinklo įranga turi būti įrengiama patalpose su seifo tipo durimis ir t. t.

7. Atitiktis teisės aktams. Rengiant informacinės saugos politiką svarbu aiškiai identifikuoti kokie šalyje galiojantys teisės aktai ar kiti dokumentai yra privalomi organizacijai. Verta atkreipti dėmesį, kad ne tik galiojantys šalies įstatymai nusako prievolę jų laikytis organizacijai, tačiau ir pačios organizacijos santykis su partneriais ar klientais. T.y. jei organizacija A gauna informaciją iš organizacijos B, turinčios aiškiai suformuotą ir įgyvendintą informacinės saugos politiką, tikėtina, kad organizacija A negalės tinkamai užtikrinti informacinės saugos, jei jos informacinės saugos politika bus suformuota pernelyg abstrakčiai ir neįgyvendinta.

Formuojant informacinės saugos politiką yra dažniausiai susiduriama su keturiomis pagrindinėmis iššūkių grupėmis:

1. Informavimas apie informacinės saugos politiką.

2. Informacinės saugos politikos nepritaikomumas.

3. Informacinės saugos politikos valdymas ir atnaujinimas.

4. Šešėlinė informacinė saugos politika.

Organizacijos saugumo politika yra visos organizacijos reikalas, kuris turi būti derinamas ir kontroliuojamas aukščiausiu lygiu, nes tai neatsiejama kokybiškos ir patikimos apsaugos nuo informacijos praradimo dalis.

1.2.1. Organizacijos saugumo politikos formavimas

Saugumo politiką nustato aukščiausia organizacijos vadovybė. Rekomenduojama, kad sudarant saugumo politiką dalyvautų visi arba bent dalis vadovaujančių organizacijos darbuotojų. Saugumo politikos formavimo procese labai didelis vaidmuo tenka IT skyriaus vadovui ir informacijos saugumo vadovui. Kitų padalinių vadovai didžiausias problemas ir prioritetus mato savo veiklos sektoriuje: vyr. finansininkui svarbiausi yra buhalteriniai duomenys, pardavimo vadovui – ryšių su klientais ir pardavimo sistema, gamybos vadovui – resursų valdymas, IT skyriaus vadovui – nenutrūkstama kompiuterinių sistemų veikla. Todėl lemiamą sprendimą ir politikos kryptį turi nustatyti organizacijos vadovas, nes tik jis geriausiai žino ilgalaikius ir strateginius organizacijos tikslus.

Geros saugumo politikos esminės savybės [5]:

- Lengvai suprantama. Paruošti dokumentai turi būti lengvai skaitomi ir suprantami paprastiems vartotojams. Dažnai pasitaikanti klaida, kai saugumo politikos dokumentai paruošiami tos srities ekspertų ir pateikiami paprastiems vartotojams, kurių kompiuterinis raštingumas žemas, susipažinti, tad akivaizdu, kad kils daug papildomų klausimų.
- Pritaikoma. Neretai beruošiant politiką yra pasinaudojama kitose įmonėse jau taikoma praktika ir naudojama dokumentacija, tačiau reikia būtinai įsitikinti, kad tai, kas parašyta, atitinka konkrečios įmonės reikalavimus.
- Įvykdoma. Politika turi atitikti verslo poreikius ir jį saugoti, tad turi būti pasirinktas ir atitinkamas tos politikos griežtumas, kad ji taptu įgyvendinama.
- Priimama etapais. Prieš oficialią naujos politikos įgyvendinimo pradžią svarbu duoti organizacijai su ja susipažinti ir tik tada pradėti palaipsniui diegti.
- Iniciatyvi. Politika turėtų apibrėžti, ko tikimasi iš kiekvieno darbuotojo ir kokios jo funkcijos.
- Diplomatiška . Reikėtų vengti griežtų pareiškimų, kategoriškumo ir visko, kas darbuotojui galėtų nuskambėti nepagarbiai ar grėsmingai.

1.2.2. Informacinės saugos politikos įgyvendinimas

Iškilusias saugumo grėsmes organizacijoms reikia kažkaip atremti, todėl labai svarbu tinkamai įgyvendinti įmonės informacinės saugos politiką. Tam galima naudoti jau sukurtus saugos mechanizmus ir praktikas. Dauguma saugumo specialistų pataria visų pirma remtis jau sukurtais saugumo šablonų, standartų rinkiniais ir pan., kurių paruošimui, tobulinimui ir atnaujinimui saugumo specialistai skyrė daugybę valandų darbo, todėl jų metodai patikimi, o visa informacija sukomplektuota vienoje vietoje, tad ir patogu. Plačiausiai žinomi ISO, NIST, COBIT, ITIL vardai, tad lieka išsirinkti labiausiai atitinkantį įmonės saugos kryptį, nors dėl panašumų jie gali būti ir

derinami tarpusavyje, norint pasiekti palankiausią saugumo ir verslo poreikio santykį. Žemiau trumpai apžvelgiamos šių rinkinių ypatybės.

COBIT

Tikslas: COBIT yra aukšto lygio struktūra, kuri aprašo IT procesus taip, kad verslo vadovai galėtų sėkmingai įgyvendinti pagrindines politikas ir procedūras. Ši struktūra leidžia kur kas platesnę taikymo sritį, atsižvelgiant į visus IT valdymo procesus.

Panaudojimas: COBIT dažniausiai pasitelkiamas verslo vadovų tam, kad sėkmingai įgyvendinti esmines politikas ir procedūras. Be to, ji dažnai naudojama siekiant susieti organizacijos kontrolės, rizikos ir techninius klausimus. Rekomenduojama naudoti, kai organizacija siekia sukurti struktūrą, kuri nukreipta ne tik į informacijos saugumą.

Stiprybės: COBIT kuruojamas ir prižiūrimas ISACA organizacijos, kuri nuolat atnaujina struktūra pagal šios dienos tendencijas. Tai visuotinai pripažintas standartas, kuris aprėpia daug daugiau nei vien tik informacijos saugumą, kuo kitos struktūros pasigirti negali. Taip pat ji gana lengvai įgyvendinama etapais.

Silpnybės: Dėl itin plačios taikymo srities gali pasitaikyti spragų ir nepakankamo detalumo lygio trūkumų.

Atitikimas: ISACA organizacija numato keturis COBIT sertifikavimo lygius – CISA (sertifikuotas informacinių sistemų auditorius), CISM (sertifikuotas informacinių sistemų valdytojas), CGEIT (sertifikuotas įmonės IT valdytojas), CRISC (sertifikuotas rizikos ir informacinių sistemų valdyme).

ITIL

Tikslas: Tai gerųjų praktikų rinkinys, kuris gali būti pritaikytas įmonės tikslams pasiekti. ITIL pateikiamas penkiais esminiais etapais, kurių kiekvienas atitinka įmonės IT būseną duotuoju metu. Dokumentacija pateikia procesus, užduotis ir kontrolinius sąrašus, kurie nebūdingi konkrečiai organizacijai, tam, kad ji galėtų nusistatyti ribą, nuo kurios bus diegiama kontrolė ir stebimi pokyčiai.

Panaudojimas: ITIL sukurta Junginėje Karalystėje tad ir geriausiai pritaikoma šioje teritorijoje, tačiau dabar ji laikoma visuotinai pripažįstamu standartu ir naudojama daugelyje įmonių visame pasaulyje. Dažnai taikomas įmonėms, kurios kartu nori naudoti ir ISO standartą nebandant gauti ISO 27001.

Stiprybės: ITIL sukurtu ir valdoma JK valdžios, todėl natūraliai ypatingai tinka toje teritorijoje veikiančioms organizacijoms. Dėl universalumo naudojama visame pasaulyje, o organizacijose jaučiama teigiama įtaka efektyvumui ir ekonomijai.

Silpnybės: Orientuota tik į informacijos saugumą, todėl dažnai taiko nuorodas į žemesnio lygio rinkinius dėl detalesnio tam tikrų sričių išaiškinimo ir taikymo.

Atitikimas: ITIL siūlo keturių lygių sertifikavimo galimybes – pamatinis, vidutinis, ekspertinis, meistro.

ISO 27002

Tikslas: Pateikti gerosios praktikos rekomendacijas ISMS sistemai.

Panaudojimas: Dažniausiai naudojama IT departamento, kuriam skiriamas visas dėmesys. Šis struktūra suteikia įmonėms tarptautinį pripažinimą, atpažinimą ir suderinamumą. Kai kurios organizacijos net reikalauja savo partnerių, kad įsidiegtų ISO standartus taip pat, sėkmingam tolimesniam bendradarbiavimui.

Stiprybės: Struktūra susieta su labai gerbiamu ir pripažįstamu ISO 27001 standartu, tad taip pat įgyja šias charakteristikas. Ji leidžia sistemos valdytojams aptikti ir apriboti sistemos spragas bei sutapimus.

Silpnybės: ISO 27002 yra tikslingai nukreiptas į informacijos saugą ir nusileidžia pritaikymo srities pločiu tokioms struktūroms kaip COBIT.

Atitikimas: Gali būti pritaikoma įvairaus dydžio organizacijoms. Susietasis ISO 27001 standartas suteikia galimybę sertifikuotis, nors ir realiai atliekamas retai.

NIST

Tikslas: JAV produktas saugumo valdymui ir užtikrinimui, kuris privalomas visose su saugumu susijusiose Federalinėse institucijose.

Panaudojimas: JAV valdžios institucijos privalo vadovautis šiuo rinkiniu, kad atitiktų federalinius įstatymus. Jį galima naudoti ir ne valstybinėse organizacijose, tačiau dėl savo specifikos gali būti sunku pritaikyti.

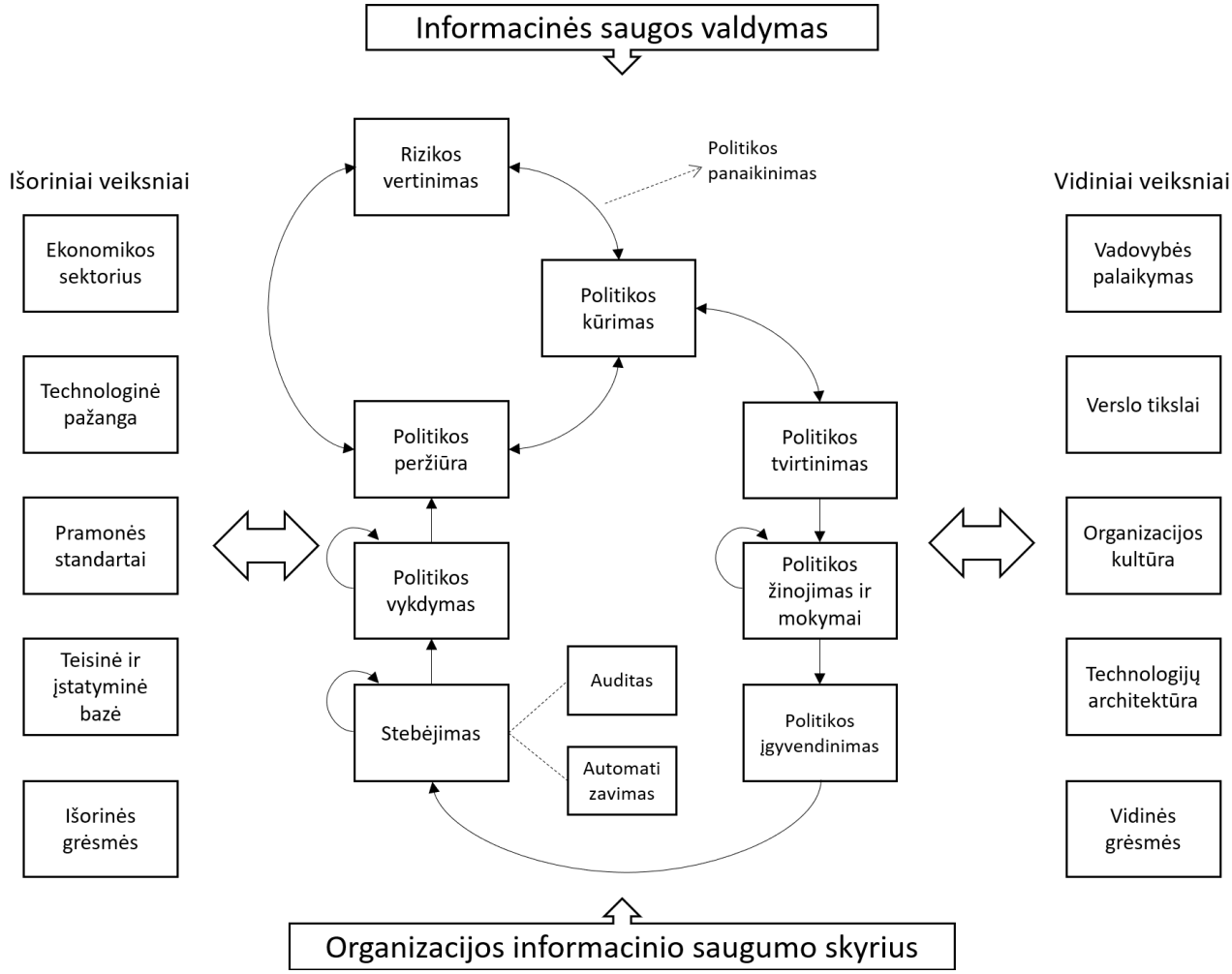
Stiprybės: Didelis detalumo lygis.

Silpnybės: Kaip ir ISO 27002, taip ir NIST nusileidžia savo taikymo sritimi ir aprėpia tik informacijos saugą, todėl gali atsirasti saugumo spragų neaprašytose srityse.

Atitikimas: Reikalaujama atitikimo FISMA reikalavimams.

1.2.3. Informacinės saugos politikos gyvavimo ciklas

Organizacijos informacinės saugos politiką reikėtų įsivaizduoti kaip nenutrūkstamą procesą, kurio metu vis grįžtama į tam tikrus etapus, atliekami pakeitimai, peržiūrima ir patikrinama, ar neprarado savo aktualumo, ir vėl paleidžiama vykdyti. Paveiksle žemiau pateikiamas toks saugos politikos gyvavimo ciklo modelis.



1.3 pav. Informacinės saugos politikos gyvavimo ciklas. [6]

Šio modelio centre pavaizduotas ciklas, kurio metu saugos politika nuo jos sukūrimo etapo, susidedančio iš trijų žingsnių – rizikos vertinimo, politikos sukūrimo ir jos peržiūros, keliauja per kitus esminius etapus iki tol, kol vėl pasiekia reguliarų ir suplanuotą peržiūrą. Sukurtai politikai visada reikalingas organizacijos vadovų ir atsakingų darbuotojų patvirtinimas, kas leis užtikrinti, jog numatytų saugos priemonių bus laikomasi aukščiausiu lygiu. Po patvirtinimo svarbu organizacijos darbuotojus supažindinti su planuojamomis įgyvendinti procedūromis ir priemonėmis, o jei būtina, reikia personalą ir papildomai apmokyti. Šis etapas turi būti besikartojantis, nuolat primenant apie taikomus metodus, nes darbuotojai linkę pamiršti ir atsipalaiduoti, tuomet tokia politika susilpnėja. Po supažindinimo pereinama prie politikos įgyvendinimo, o po jo – užtikrinamas nuolatinis jos laikymasis stebint taikomosiomis programomis bei atliekant auditus. Vienas svarbesnių etapų, tačiau dažnai užmirštamas, yra užtikrinimas, kad politikos yra laikomasi. Tam pasitarnauti galėtų reguliarūs organizacijos vadovų priminimai apie taikomas saugumo priemones ir taisykles, nesilaikančiųjų drausminimas, besilaikančiųjų skatinimas. Po visų šių etapų yra numatytas grįžimas prie politikos peržiūrėjimo ir įvertinimo, ar vis dar atitinka pasikeitusius verslo poreikius, naujas grėsmes, saugumo sprendimus ir tendencijas bei pan. Tad šis ciklas kartojasi vėl iš naujo ir tik toks procesas užtikrina, kad organizacijos taikoma informacinės saugos politika yra vis dar aktuali ir efektyvi.

Taip pat svarbu paminėti, kad didelę įtaką prieš tai minėtam ciklui daro ir išoriniai bei vidiniai veiksniai. Pavyzdžiui, pasikeitus valstybės, kurioje vykdoma veikla, įstatyminei bazei, pasikeis ir organizacijos vidinė saugumo politika. Arba pasikeitus verslo tikslams, gali tapti dalis procesų nebeaktualūs, tad keisis ir saugos politika.

1.3. Prieigos teisių valdymas

Informacijos saugos politika neįsivaizduojama be vieno iš savo fundamentinių komponentų – prieigos valdymo, siekiant apsaugoti kritinę infrastruktūrą ir informaciją nuo neautorizuoto atskleidimo ar modifikavimo. Tai suponuoja, kad leidimai suteikiami tik toms sistemoms ar vartotojams, kurie yra autorizuoti pasiekti atitinkamus resursus [5]. Šią sąlygą galima taikyti tiek fizinės prieigos kontrolei, tiek kibernetinei.

Tinkamai įgyvendinti prieigos kontrolę, būtina identifikuoti kiekvieną informacija besinaudojantį vartotoją, priskiriant jam unikalius duomenis, pagal kuriuos jis gali būti vienareikšmiškai atskirtas nuo kitų vartotojų. Šie duomenys dažniausiai vadinami identifikatoriais. Šie unikalūs duomenys kartu su autentifikavimo procesu, autorizuoja vartotojus ir taip suteikia jiems prieigą prie priskirtų resursų.

1.3.1. Prieigos teisių valdymas pagal ISO 27001:2013 standartą

Apžvelkime, ką apie prieigos valdymą sako ISO 27001 standarto aprašymas.

Informacijos saugojimas visų pirma prasideda nuo fizinio saugumo ir taikomos fizinio ir aplinkos saugumo politikos. Šis standartas pateikia rekomendacijas ir šiai dedamajai (1.1 lentelė).

1.1 lentelė. Fizinis ir aplinkos saugumas

Fizinis ir aplinkos saugumas		
Saugiosios vietos		
Tikslas: išvengti neteisėtos fizinės prieigos, žalos bei trukdžių organizacijos informacijai ir informacijos apdorojimo priemonėms.		
1	Fizinė perimetro apsauga	Perimetro apsaugos priemonės turi būti numatytos ir naudojamos, siekiant apsaugoti vietas, kuriose laikoma įslaptinta ar ypatingai svarbi informacija arba informacijos apdorojimo priemonės.
2	Fizinė įėjimo kontrolė	Saugiosios vietos turi būti apsaugotos tinkamomis įėjimo kontrolės priemonėmis, kurios užtikrintų tik įgalioto personalo įleidimą.
3	Įstaigų, patalpų ir priemonių apsauga	Turi būti numatyta ir taikoma įstaigų, patalpų ir priemonių fizinė apsauga.
4	Apsauga nuo išorinių ir aplinkos grėsmių	Turi būti numatytos ir pritaikytos fizinės apsaugos priemonės nuo nepalankių situacijų, tyčinių užpuolimų ar nelaimingų atsitikimų.
5	Darbas saugiosiose vietose	Turi būti numatytos ir pritaikytos procedūros, skirtos darbui saugiosiose vietose.
6	Pristatymo ir krovimo vietos	Siekiant išvengti neteisėtos prieigos, prieigos vietos, pavyzdžiui, pristatymo ir krovimo zonos ar kitos vietos, pro kurias leidimo neturintys asmenys galėtų patekti į patalpas, turi būti kontroliuojamos ir, esant galimybei, atskiriamos nuo infrastruktūros, skirtos informacijai apdoroti.

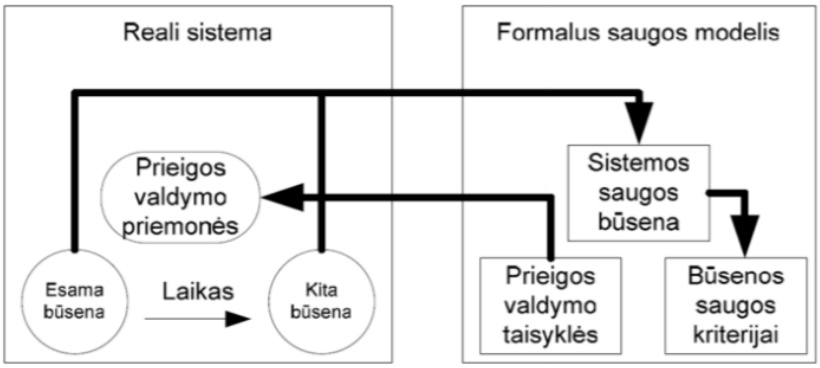
Įgyvendinus fizinę informacijos ir informacijos apdorojimo priemonių apsaugą galima pereiti prie technologinio prieigos prie informacijos valdymo, kurio gairės pateikiamos ISO 27001 standarte (1.2 lentelė):

1.2 lentelė. Prieigos valdymas

Prieigos valdymas		
Veiklos reikalavimai prieigos valdymui		
Tikslas: apriboti prieigą prie informacijos ir jos apdorojimo priemonių		
1	Prieigos valdymo politika	Vadovaujantis veiklos ir informacijos saugumo reikalavimais turi būti numatyta, dokumentuota ir peržiūrima prieigos valdymo politika.
2	Prieiga prie tinklų ir tinklo paslaugų	Naudotojams prieiga turi būti suteikiama tik prie tų tinklų ir tinklo paslaugų, kuriomis naudotis jiems buvo konkrečiai suteikta teisė.
Naudotojų prieigos valdymas		
Tikslas: užtikrinti sankcionuotą naudotojų prieigą ir išvengti neteisėtos prieigos prie sistemų ir jų paslaugų.		
1	Naudotojų registravimas ir išregistravimas	Turi būti įgyvendinta oficiali naudotojo registravimo ir išregistravimo procedūra, siekiant suteikti prieigos teises.
2	Prieigos naudotojams suteikimas	Turi būti įgyvendinta oficiali teisių naudotis visomis sistemomis ir jų paslaugomis suteikimo ir atšaukimo visų tipų naudotojams procedūra.
3	Prieigos teisių valdymas	Prieigos teisių paskyrimas ir naudojimas turi būti apribotas ir valdomas.
4	Slaptos naudotojų tapatumo nustatymo informacijos valdymas	Slaptos naudotojų tapatumo nustatymo informacijos paskyrimas turi būti valdomas vadovaujantis oficialia valdymo procedūra.
5	Naudotojų prieigos teisių priežiūra	Priskirtieji turto valdytojai turi nustatytu reguliarumu peržiūrėti naudotojų prieigos teises.
6	Prieigos teisių pašalinimas arba keitimas	Pasibaigus įdarbinimo ar samdos sutarčių arba kitų susitarimų galiojimo laikui ar jiems pasikeitus, visų darbuotojų ir išorinių naudotojų prieigos prie informacijos bei jos apdorojimo priemonių teisės turi būti panaikintos.
Prieigos prie sistemų ir taikomųjų programų valdymas		
Tikslas: išvengti neteisėtos prieigos prie sistemų ir taikomųjų programų.		
1	Prieigos prie informacijos ribojimas	Prieiga prie informacijos ir taikomųjų programų funkcijų turi būti apribota vadovaujantis prieigos valdymo politika
2	Saugiosios prisijungimo procedūros	Ten, kur prieigos valdymo politika reikalauja, prieiga prie sistemų ir taikomųjų programų turi būti valdoma naudojant saugiąją prisijungimo procedūrą.
3	Slaptažodžių tvarkymo sistema	Slaptažodžių tvarkymo sistemos turi būti interaktyvios ir užtikrinti kokybiškų slaptažodžių naudojimą.
4	Padidintos rizikos paslaugų programų naudojimas	Sisteminių programų, kurios galėtų nepaisyti sistemoms ir taikomosios programoms taikomų valdymo priemonių, naudojimas turi būti apribotas ir griežtai valdomas.
5	Prieigos prie pirminio programų teksto valdymas	Turi būti valdoma prieiga prie pirminio programų teksto.

1.3.2. Prieigos saugos valdymo modeliai

Saugos modelių tikslas yra apibrėžti autorizuotas ir neautorizuotas, saugias ir nesaugias sistemos būsenas ir apriboti sistemos perėjimą į neautorizuotą būseną. Ryšys tarp realios sistemos ir formalaus saugos modelio vaizduojamas 1.4 pav. [6]



1.4 pav. Ryšys tarp sistemos ir formalaus saugos modelio [6]

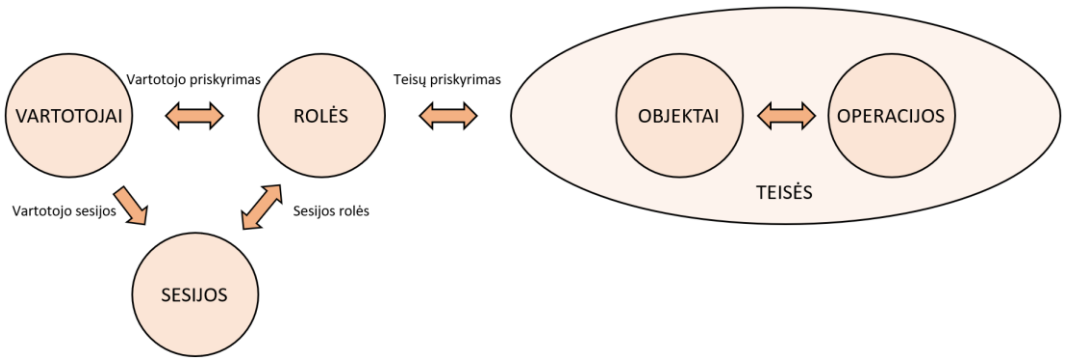
Saugos modeliai:

- **DAC** (angl. *Discretionary Access Control*) – diskrecinis prieigos valdymo modelis, kuriame objekto savininkas nustato, kas gali prieiti prie jo turimo objekto [7]. DAC modelio savybės:
    - Kiekvienas objektas turi savininką;
    - Pirminis objekto savininkas – objekto kūrėjas;
    - Savininkas gali perleisti savininko teises kitam subjektui;
    - Prieigos teises prie objekto nusako savininkas.

  Šis modelis dažniausiai įgyvendinamas naudojant prieigos valdymo sąrašą ACL (angl. *Access Control List*). Prieiga yra ribojama atsižvelgiant į vartotojų teises, kurias jie gavo autorizacijos metu. DAC buvo panaudota ankstyvosiose komercinėse programose, ypač operacinėse sistemose ir reliacinėse duomenų bazių sistemose. Pagrindinė DAC idėja yra ta, kad objekto savininkas, kuris yra paprastai jo kūrėjas, turi savarankišką valdžią, t. y. DAC apima savininkais pagrįstą prieigos teisių administravimą. [8]
- **MAC** (angl. *Mandatory Access Control*) – tai yra prieigos valdymo modelis, nusakomas sistemos, bet ne objekto savininko, t. y. prieigos teisės negali būti pakeistos vartotojo arba savininko. MAC yra naudojamas sistemose, saugančiose kelių slaptumo lygių (pvz., konfidencialu, slapta, visiškai slapta) informaciją. Dažniausiai ją taiko valstybinės ir karinės organizacijos. MAC modeliu pagrįstose sistemose visi objektai ir subjektai turi turėti priskirtas saugumo etiketes (angl. *label*). Subjekto etiketė nurodo sistemos pasitikėjimo juo lygį, t. y. kokį minimalų pasitikėjimo lygį turi turėti subjektas, norėdamas gauti priėjimą prie objekto. Subjektas, turintis tam tikrą pasitikėjimo lygį, gali prieiti prie pagal lygį lygių ar žemesnių saugumo kategorijos objektų. MAC modelis draudžia rašyti į objektą aukštesnio

įslaptinimo lygmens informaciją negu to objekto įslaptinimo lygmuo. MAC modelyje apibrėžiamas nustatytas prieigos valdymo lygis. Šiame prieigos valdymo modelyje vartotojams suteikiama mažai laisvės sprendžiant, kas gali prieiti prie jų turimų duomenų. Objekto lygį gali pakeisti tik administratorius, tačiau ne objekto savininkas. Sistema pati sprendžia, kaip turi būti dalinamasi duomenimis. Tam tikras teises turintis subjektas galės prieiti prie tam tikro įslaptinimo lygmens objektų atsižvelgiant į „reikia-žinoti“ principą. MAC laikomas saugesniu modeliu nei DAC, tačiau jį sudėtingiau konfigūruoti ir įgyvendinti. [8]

- **TBAC** (angl. *Task-based Authorization Controls*) – šis modelis labai panašus į RBAC, o didžiausias skirtumas tame, kad vietoj vienos rolės priskyrimo vartotojui, yra priskiriamos kelios rolės, kurios susijusios su darbo užduotimis priskirtomis asmeniui susietomis su vartotojo paskyra. TBAC modelyje prieiga vis dar paremta taisyklėmis (darbo užduotimis) ir orientuota į prieigos valdymą priskiriant užduotis vietoj vartotojo identifikacijos [9].
- **RBAC** (angl. *Role-Based Access Control*) – rolėmis pagrįstas autorizuotų vartotojų prieigos valdymo modelis, kuriame sprendimai priimami atsižvelgiant į subjektų roles. Tai alternatyva MAC ir DAC modeliams. Modelis pagrįstas vartotojų vaidmenų sukūrimu, kurie tiesiogiai išreiškia jų pareigas, t. y. teisės vartotojams nėra suteikiamos tiesiogiai, bet priskiriant vieną ar kelis vaidmenis, kuriuose yra apibrėžtos konkrečios pareigybės teisės. Palyginti su tradiciniais prieigos teisių sąrašais (ACL), naudojamais DAC modelyje, RBAC suteikia daug didesnį detalizacijos lygį, pvz., ne vien leisti skaityti, rašyti, vykdyti rinkmeną, bet ir vykdyti tam tikrus veiksmus sistemoje, tokius kaip vartotojų kūrimas. Rolės, o tai reiškia, ir leidimai, nustatomi atsižvelgiant į vartotojo pareigas, kompetenciją, autorizaciją ir atsakomybę. Tai leidžia subjektams pasiekti tik tam tikrus objektus. Rolės vartotojams lengvai kuriamos, keičiamos ar atšaukiamos grupėmis, nereikia atnaujinti privilegijų kiekvienam atskirai. Visą teisių valdymą atlieka sistemos administratorius.



1.5 pav. RBAC modelis

Modelio pagrindiniai elementai: [10]

- Vartotojai – procesas, žmogus, įrenginys, tinklas, autonominis agentas, kuris naudoja sistemą;
- Rolės – organizacijoje atliekamo darbo funkcija. Subjekto priskyrimas rolei reiškia tam tikrą vadovybės suteiktą atsakomybę;
- Teisės – tai leidimas atlikti tam tikrą operaciją su vienu ar keliais objektais;

- Operacijos – tai procesas, vykdomasis programos atvaizdas, kurį iškvietus atliekamos tam tikros subjektui reikalingos funkcijos;
- Objektai – tai esybė, kuri turi arba gauna informaciją.

Savybės:

- Subjektams suteikiamos teisės per roles;
- Palaiko *daug-su-daug* subjektų rolių priskyrimą;
- Palaiko *daug-su-daug* teisių priskyrimą;
- Palaiko subjektų rolių priskyrimo apžvalgą;
- Subjektai gali naudotis skirtingų rolių teisėmis vienu metu.

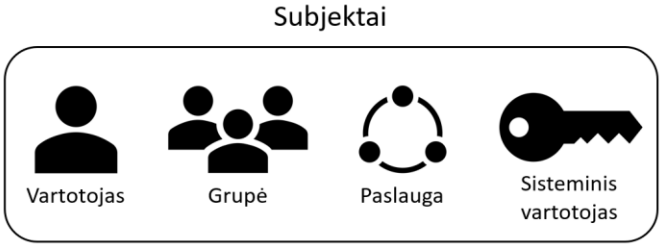
Sesija jungia subjektą su aktyvuotų rolių rinkiniu. Sesijos rolės ryšys parodo sesijos metu aktyvuotas roles, o subjekto sesijų ryšys parodo visas su subjektu susietas sesijas. Subjektui taikomos tos teisės, kurios priskirtos subjekto sesijos metu aktyvuotai rolei. [10]

1.3.3. RBAC realizacija informacinėse sistemose

Kaip ir minėta anksčiau, vieni didžiausių RBAC modelio privalumų – lankstumas ir administravimo paprastumas. Šis modelis gali būti realizuojamas priskiriant vartotojams teises priklausomai nuo to, kokias pareigas įmonėje jie užima ir kokias roles vykdo. Darbuotojui leidžiama pasiekti tik tą informaciją, kuri reikalinga tiesioginėms funkcijoms ir darbo užduotims atlikti (mažiausių teisių principas).

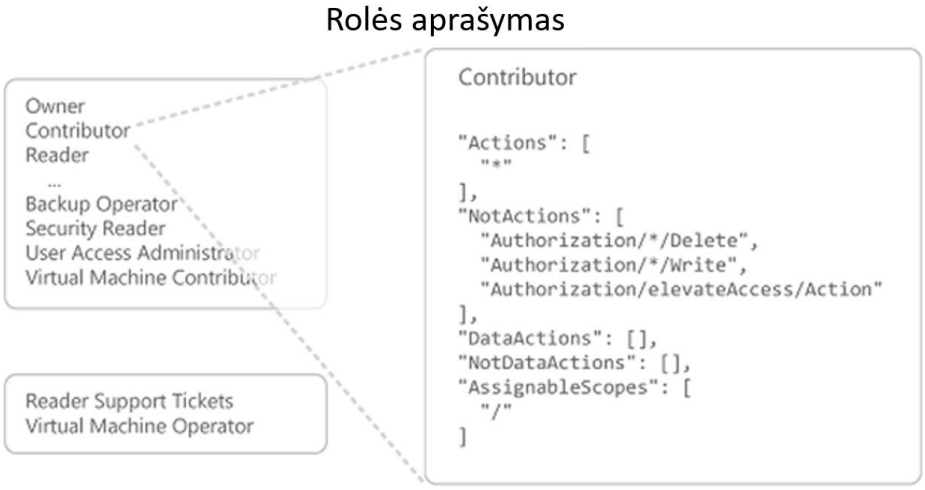
Galima plačiau panagrinėti rolėmis grįsto modelio įgyvendinimą *Microsoft Azure* sistemoje. RBAC veikimas pagrįstas rolių priskyrimu, kuris susideda iš trijų elementų: subjektas, objektas (taikymo sritis) ir rolė.

Subjektas - tai vartotojas, vartotojų grupė, paslauga ar sisteminis vartotojas, kurie reikalauja prieigos prie *Azure* sistemos resursų. Subjektams priskiriamos rolės.



1.6 pav. Subjektas Azure sistemoje.

Rolės – tai leidimų rinkinys, kuris nurodo, kokias operacijas subjektas gali atlikti (skaityti, rašyti, trinti). Rolės gali būti aukšto lygio, pavyzdžiui, informacijos šaltinio savininkas (angl. *Owner*), arba labai specifinės, pavyzdžiui, virtualios mašinos operatorius (angl. *Virtual machine operator*).



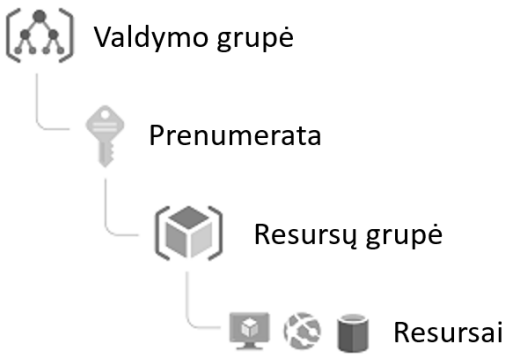
1.7 pav. Rolė Azure sistemoje.

Azure siūlo kelias jau iš anksto numatytas roles, kurios gali būti panaudotos prieigos prie informacijos valdymui:

1. **Autorius** (*Owner*) – turi pilną prieigą prie visų sistemos resursų, įskaitant galimybę deleguoti prieigos teisę kitiems subjektams.
2. **Pagalbininkas** (*Contributor*) – turi teisę kurti ir valdyti visų tipų Azure resursus, tačiau neturi teisės suteikti prieigos kitiems subjektams.
3. **Skaitytojas** (*Reader*) – gali peržiūrėti informaciją.
4. **Vartotojų prieigos administratorius** (*User Access Administrator*) – leidžia valdyti tik vartotojų prieigos teises.

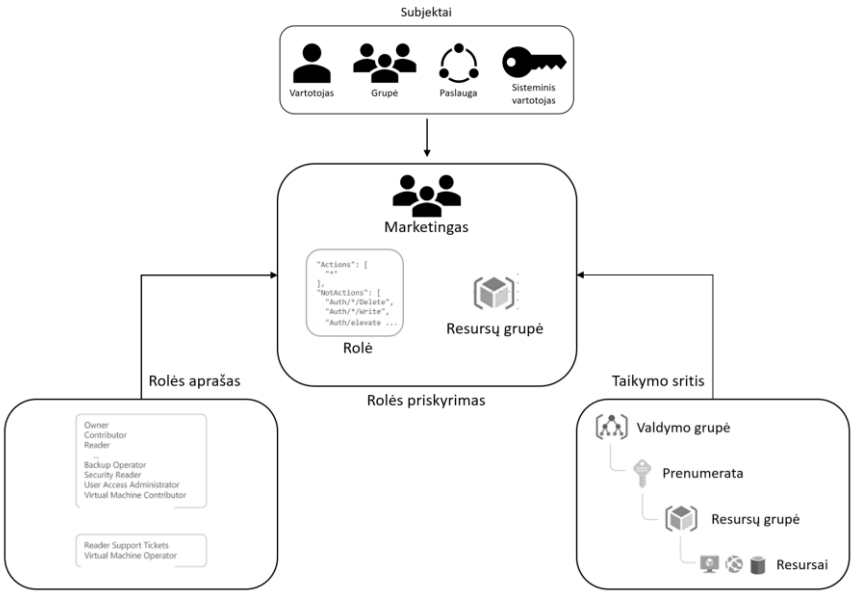
Jei iš anksto numatytosios rolės neatitinka administratoriaus poreikių, galima sukurti naujas roles su tik joms būdingomis teisėmis.

Taikymo sritis – tai ribos, kuriose galioja suteikta prieiga vartotojui. Azure sistemoje taikymo sritį galima aprašyti keliose lygiuose. Čia taip pat galioja teisių paveldimumo sąlyga.



1.8 pav. Taikymo sritis Azure sistemoje

Visas šias dalis apjungia procesas, vadinamas rolės priskyrimu. Tai toks procesas, kai vartotojui, grupei, paslaugai ar sisteminiam vartotojui suteikiamos konkrečios rolės garantuojamos teisės tam tikroje taikymo srityje. Pavyzdyje žemiau vizualiai pavaizduojamas rolės priskyrimas.



1.9 pav. Rolės priskyrimas.

Kelių rolių priskyrimas gali sudaryti situaciją, kai rolių suteikiamos teisės persidengia, todėl subjektui suteikiama visų šių teisių suma.

Jei rolių aprašuose yra prieigą draudžiančių taisyklių, tuomet pirmenybė suteikiama prieigos blokavimui, net jei kitos rolės suteikia prieigos teisę prie konkretaus resurso.

1.3.4. Saugumo politikos valdymo įrankiai

Dėl itin didelio aktualumo ir paklausos rinkoje yra pasiūlyta nemažai saugumo politikos valdymo įrankių, kurios palengvina administratorių darbą, taupo kaštus bei padeda įgyvendinti pasirinktų standartų rinkinių reikalavimus ir įgyti reikiamus saugumą patvirtinančius sertifikatus. Didžioji dauguma šių sprendimų yra gana kompleksiški ir aprėpia visas (ar beveik visas) organizacijos saugumo sritis, pradedant įmonės fizine sauga ir baigiant prieigos prie informacijos kontrole.

„Policy Minder“ – produktas, kuris išleistas kompanijos *„Powertech“*.

- Automatinis atitikties auditas – visų sistemų auditavimas ir pažeidžiamumų nustatymas remiantis taikoma saugumo politika;
- Automatinis atitikties atstatymas – aptiktų saugumo spragų automatinis taisymas ir atitikties atstatymas;
- Ataskaitos – duomenų analizė vykdoma pačioje programoje ir administratoriui pranešami tik tie įvykiai, kurie reikalauja atskiro dėmesio;

- Saugumo politikos dokumentacija – programa audituoja faktinę sistemos konfigūraciją ir parametrus, kuriuos galima naudoti nustatant bazinį lygį arba dokumentuojant saugumo politiką;
- Integruotas scenarijų valdymas – pašalina neatitikimus tarp serverių centralizuojant jų lokaciją ir paleidimo parametrus.
- Daugiaplatformis palaikymas ir kt.

Kai nustatymus reikia keisti rankiniu būdu arba naudojant scenarijus keliuose serveriuose, atitiktis saugumo politikai tampa sunkiai patikrinama ir valdoma, todėl „*Policy Minder*“ gali tai atlikti automatiškai. Kelios automatizavimo galimybės, kurias siūlo ši programa:

- Saugumo politikos pritaikymas naujiems įmonės IT įrenginiams;
- Prieigos prie failų ir katalogų valdymas;
- Naujų failų ar pakeistų failų nustatymo galimybės;
- Neaktyvių vartotojų paskyrų nustatymo galimybė ir kt.

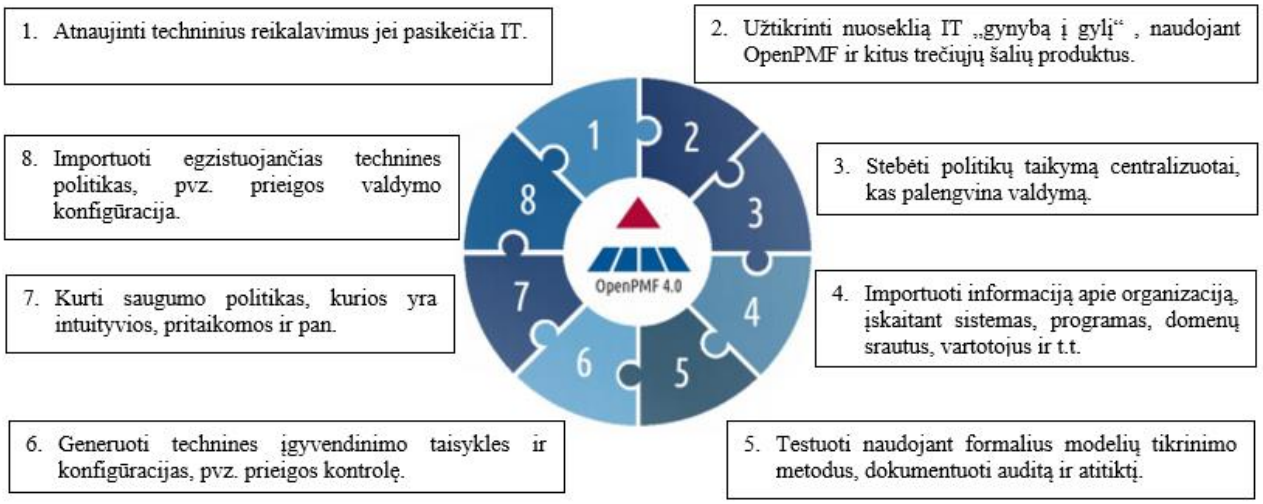
Pritaikymo sritys:

- Katalogų ir dokumentų teisės:
    - Teisės
    - Savininkai
    - Atributai
        - SUID
        - SGID
        - SVTX
    - Išplėstinės teisės
    - SUID / SGID dokumentai ir katalogai
- Globalūs saugumo nustatymai:
    - Audito atributai
    - Grupių atributai
    - Prisijungimų numatytieji parametrai
    - Slaptažodžių atributai
    - Vartotojų paskyrų sukūrimo numatytieji parametrai
    - Ir kt.
- Vartotojų paskyrų nustatymai:
    - Audito atributai
    - Grupių atributai
    - Prisijungimų numatytieji parametrai
    - Slaptažodžių atributai
    - Ir kt.
- TCP/IP procesai
- Eksportuoti katalogai
- Vartotojų aprašytos politikos

„OpenPMF“ – dar vienas panašus produktas, kurį pasiūlė kompanija „*ObjectSecurity“*, tačiau pastarasis labiau orientuotas į viso proceso automatizavimą, sprendžiant dažniausiai pasitaikančias saugumo politikos įgyvendinimo problemas. Šis įrankis pasižymi šiomis savybėmis:

- Automatiškai skaičiuoja ir peržiūri atitinkančias IT infrastruktūros technines roles bei nustatymus savo agentų pagalba;
- Galinga ir lanksti – savaime adaptuojasi keičiantis pačiai infrastruktūrai;
- Padeda įgyvendinti prieigos valdymo politikas;
- Mažina kaštus, didina saugumo lygį;
- Greitina saugumo politikos įgyvendinimą ir palaikymą.

Šis įrankis leidžia įgyvendinti ir valdyti geresnę prieigos kontrolę: galima griežtai taikyti reikalingą prieigos politiką visame IT tinkle, remiantis plačių galimybių, pritaikomais atributais.



1.10 pav. „*OpenPMF“* funkcionalumas.

Dėl visų apžvelgtų savybių šių produktų kūrimas yra sudėtingas ir ilgai trunkantis procesas, todėl niekas nesiūlo pasinaudoti nemokamai. Be to, jie apima kelis ar net keliolika skirtingų saugumo politikos įgyvendinimo sričių, kurių tam tikrais atvejais gali ir neprireikti. Pavyzdžiui, norint įgyvendinti bei valdyti prieigos kontrolę patogiau būtų naudotis tik tam skirtu įrankiu, todėl projektui pasirinktas būtent toks modelis, kuris gana paprasta ir aiškia forma leistų organizuoti saugos politikos prieigos valdymo modulio įgyvendinimą realioje infrastruktūroje. Taipogi, šie įrankiai, kaip ir dauguma kitų, nesiūlo prieigos politikos įgyvendinimo susieti su įmonės vadovų patvirtintu dokumentu, kuriame būtų aprašyta prieigos politika, kuri galėtų būti panaudota automatizuotam prieigos prie informacijos šaltinių suteikimui.

1.3.5. Prieigos valdymo iššūkiai

Platus taikomųjų programų pasirinkimas diktuoja, kad informacijos saugos, o tuo pačiu ir prieigos saugos, valdymas yra gana komplikuotas ir sudėtingas procesas, kuriam reikia papildomų darbuotojų arba papildomos įrangos, o kartais ir vieno, ir kito.

D. Holme, *Microsoft* profesionalas, vienoje iš savo knygų [11] aprašo dažniausiai pasitaikančius atvejus, kada organizacijos, netaisyklingai įgyvendinusios prieigos kontrolę, vargsta spręsdamos kasdienius uždavinius, neužtikrina reikiamos saugos ir sistemos lankstumo.

- Atsiradus naujam darbuotojui, reikiamos prieigos suteikimas gali užtrukti ne vieną dieną, o ir egzistuoja didelė tikimybė, kad vis tiek kartas nuo karto vartotojas kreipsis į IT personalą, nes kažkas buvo praleista.
- Pasikeitus darbuotojo pareigoms, ar norint suteikti tokias pačias teises, kaip turi kitas tam tikros srities darbuotojas, nėra paprasta išsiaiškinti, kokias iš tiesų teises reikėtų priskirti ir kokius informacinius išteklius tie vartotojai pasiekia.
- Laikinos prieigos suteikimas taip pat sukelia nepatogumų, nes sunku sukontroliuoti, kuriuose šaltiniuose turi būti priskirtas laikinas leidimas, pasibaigus leidimo galiojimui – komplikuotas jo ištrynimas.
- Audito metu be specialios programinės įrangos sudėtinga išrikiuoti kiekvieno vartotojo prieigos teises, nes, pavyzdžiui, *Microsoft Active Directory* neturi galimybės atvaizduoti vartotojo priklausomybių grupėms, jei jis priskirtas per kitą grupę (t.y. grupė grupėje).
- Didelė klaidos tikimybė, kai darbo rezultatas priklauso nuo administratoriaus kruopštumo ir atidumo.
- Stambiose organizacijose dėl didelio kompleksiškumo sunku kontroliuoti, kur ir kokios teisės vartotojams suteikiamos.
- Ruošiant naują infrastruktūra labai daug laiko ir pastangų reikalauja jos paruošimas darbui, tinkamų teisių priskyrimas ir pan.
- Dar daug kitų sunkumų ir iššūkių.

Visa tai veda prie IT departamento darbo laiko sąnaudų, o tai – prie tiesioginių įmonės nuostolių. Daugumą iš šių iššūkių sprendžia rolėmis grįstas prieigos valdymo modelis. Remiantis juo ir pasitelkiant prieigos politikos dokumento automatizuotą įgyvendinimą, galima tikėtis labai sėkmingo rezultato.

1.4. Išvados

Išanalizavus informacinės saugos politikos įgyvendinimo ir taikymo principus, atsirandančius iššūkius ir problemas, galima padaryti kelias išvadas:

1. Informacinės saugos politika yra vienas svarbiausių organizacijos saugumą užtikrinančių įrankių, kurio duodama nauda pranoksta laiko ir finansines sąnaudas. Yra laikoma, kad organizacija, kuri investuoja į saugumo sprendimus neturėdama saugumo politikos yra labiau pažeidžiama, nei ta, kuri turi aiškią ir gerai įgyvendintą saugumo politiką, tačiau mažiau galimybių investuoti pinigus į technologinius sprendimus, ir taip yra todėl, kad ji žino, kaip elgtis vienoje ar kitoje situacijoje, ką konkrečiai saugo ir kaip palaipsniui tą saugumą didinti. Saugumo politiką nustato aukščiausia organizacijos vadovybė. Rekomenduojama, kad sudarant saugumo politiką dalyvautų visi arba bent dalis vadovaujančių organizacijos darbuotojų.

2. Informacijos saugos politikos metodikos aprašomas standartų rinkiniais, kuriuos platina tokios organizacijos, kaip NIST, ISACA, ISO ir pan. Jų pagrindų aprašomos individualios organizacijų politikos.
3. Viena svarbiausių visos saugumo politikos dalių yra prieigos valdymo politika, kuri įgyvendinama, siekiant apsaugoti kritinę infrastruktūrą ir informaciją nuo neautorizuoto atskleidimo ar modifikavimo - leidimai suteikiami tik toms sistemoms ar vartotojams, kurie yra autorizuoti pasiekti atitinkamus resursus
4. Prieigos saugos politikos įgyvendinimas yra gana sudėtingas procesas, reikalaujantis nemažai pastangų ir laiko, todėl daugelio įmonių yra ignoruojamas, todėl būtina pasitelkti šio proceso automatizavimą, politikos dokumento formalizavimą.

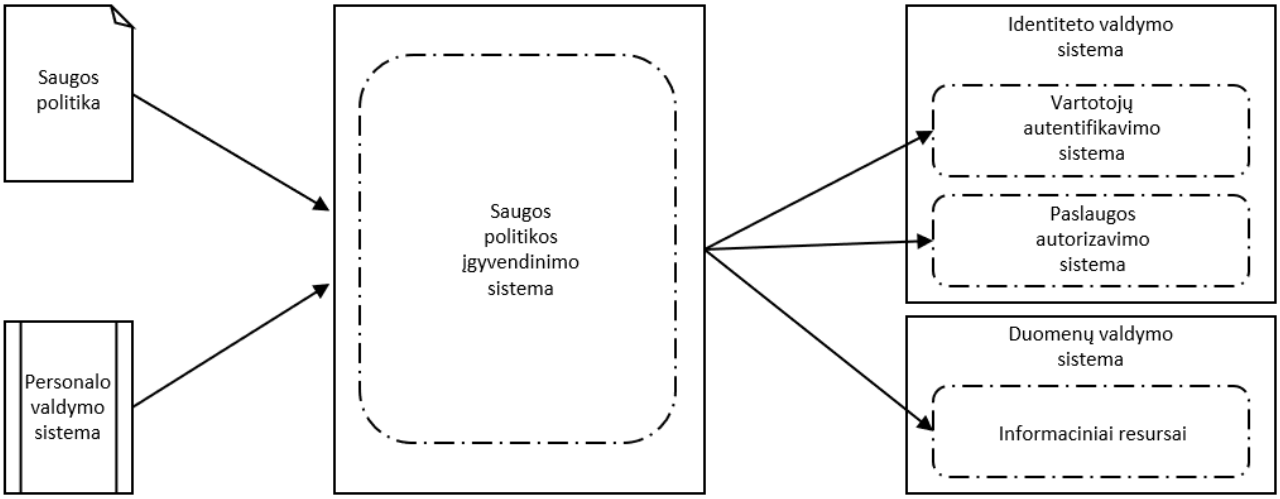
2. PRIEIGOS VALDYMO POLITIKOS AUTOMATIZUOTO ĮGYVENDINIMO METODAS

Prieigos valdymo politika, kaip viena iš pagrindinių saugos politikos sudedamųjų dalių, savo reikšme organizacijos saugumui prilygsta ugniasienėms, antivirusinėms programos, tinklo segmentavimui ir kitoms bazinėms priemonėms, tad kritiškai svarbu turėti ją tinkamai įgyvendintą. Kadangi procesas labai kompleksiškas, pradinis diegimas sudėtingas ir ilgai trunkantis, o administravimas komplikuotas, patogu turėti galimybę šią veiklą automatizuoti – pradedant automatiniu naujos infrastruktūros paruošimu ir baigiant pakeitimų valdymu ar auditavimu.

Kuriamo metodo pagrindą sudaro trys, vienas nuo kito priklausantys, etapai:

1. pradinių duomenų apdorojimas;
2. scenarijų formavimas;
3. scenarijų vykdymas.

Žemiau pateikiamame paveiksle pavaizduotas šio projekto modelis, kur šie trys etapai ir išskirti.



2.1 pav. Projekto modelis

2.1. Prieigos politika ir RBAC modelis

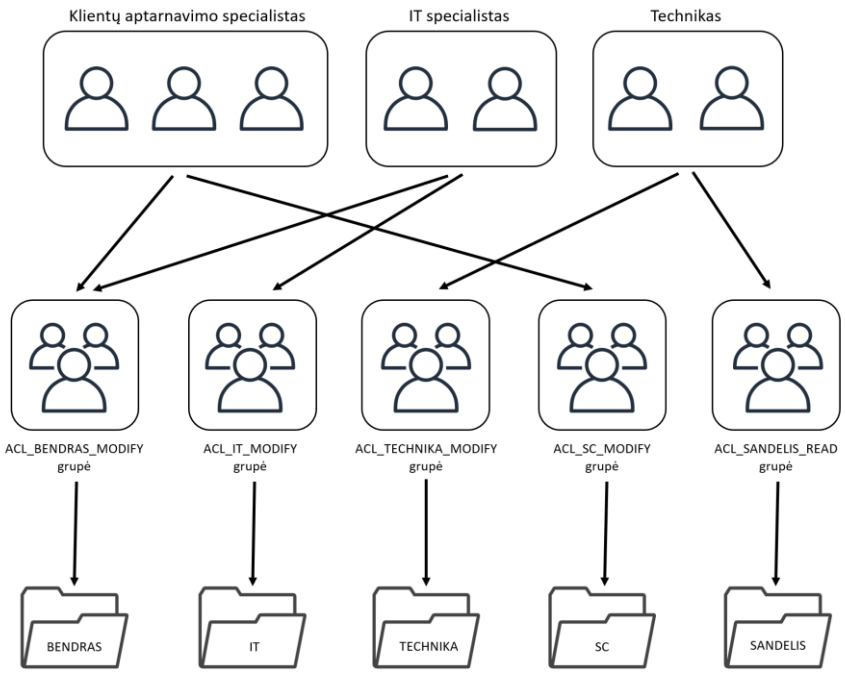
Šiam metodui įgyvendinti pasirinktas rolėmis grįstas prieigos valdymas, kurio lankstumas ir administravimo paprastumas leis užtikrinti tikslų prieigos teisių priskyrimą, auditavimą ir priežiūrą.

Teises prie informacinių šaltinių suteikia funkcinės grupės, kurios nustato, ką ir kur vartotojas gali daryti. Šios grupės priskiriamos tiesiogiai informaciniams resursams ir kiekviena jų turi savo unikalų tikslą, todėl suformuojami tokių grupių rinkiniai, kurie leidžia lanksčiai valdyti prieigos prie tų resursų teises. Šių grupių pavadinimas sudaromas iš priskirto identifikatoriaus „ACL“, informacijos resurso pavadinimo ir suteiktos teisės identifikatoriaus.

Vartotojų rolių funkciją atlieka darbuotojų pareigybių pagrindu sudarytos grupės. Jų pavadinimai atitinka prieigos politikos dokumente aprašytas pareigybes. Šios rolių grupės įtraukia darbuotojus, kurie darbuotojų duomenų bazėje turi priskirtas rolių grupes atitinkančias pareigas. Jos

apsprendžia, kokias funkcijas ir teises vartotojas įgyja jei priklauso vienai iš tų grupių. Šias teises rolių grupėms suteikia funkcinės grupės, kurioms priklauso rolių grupė.

Vizualus šio metodo atvaizdavimas pateikiamas paveikslėlyje žemiau.



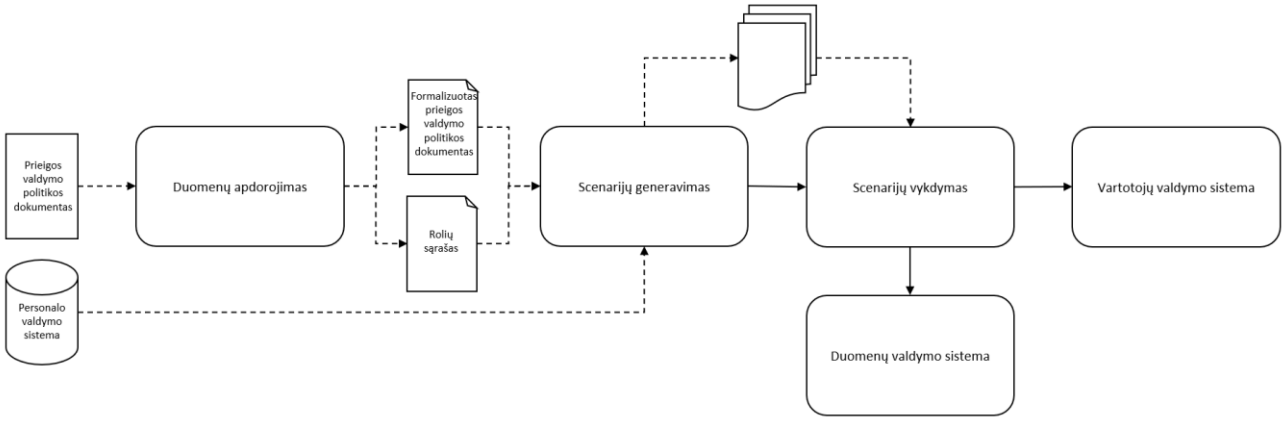
2.2 pav. Rolėmis grįstas prieigos modelis formuojamame metode.

Po atliktos procedūros kiekvienas iš vartotojų pasieks tik tuos resursus, kuriuos jiems suteikia priskirtos rolės. Skyriui pasipildžius nauju darbuotoju jam užteks priskirti kažkurią iš rolių pagal jo pareigas ir visa reikiama prieiga bus suteikta. Taip pat, realu, kad peržiūrėjus prieigos politikos dokumentą bus nuspręsta papildyti naujomis pareigybėmis, informacijos šaltiniais ar pan., tad pakartojus procedūrą su nauja prieigos politikos dokumento redakcija, duomenys bus atnaujinti tiek vartotojų duomenų bazėje, tiek duomenų serveryje.

2.2. Procesų modelis

Siekiant detaliau aprašyti kuriamą metodą, panaudojamas metodo procesų modelis, kuris gana smulkiai išskiria kiekvieną atliekamą funkciją ir jos sąryšį su kitais metodo elementais ir etapais. Paveiksle, pateiktame žemiau, šis modelis ir atvaizduotas.

Pradiniai duomenys – prieigos valdymo politikos dokumentas ir personalo duomenų failas – panaudojami kaip pirminiai šaltiniai tolimesniam prieigos taisyklių formavimui. Nors jų apdorojimas atliekamas skirtinguose etapuose, tačiau jie vienas kitą papildo ir yra būtini geram metodo rezultatui gauti.



2.3 pav. Metodo procesų modelis.

Pirmas žingsnis – prieigos politikos dokumento importavimas ir apdorojimas, siekiant gauti formalų dokumentą XML formatu, kas leistų vėlesniuose etapuose paprasčiau operuoti duomenimis.

Kitame žingsnyje įterpiamas antrasis išorinis duomenų šaltinis – organizacijos personalo duomenys – kuris su jau anksčiau paruoštu formaliu prieigos politikos dokumentu panaudojamas scenarijų generavimui ir išsaugojimui atskirais failais.

Galiausiai, pereinama prie scenarijų vykdymo ir automatizuoto prieigos saugos politikos įgyvendinimo panaudojant rolėmis grįstą prieigos valdymo modelį. Šiame etape vykdomi scenarijai, kurie pagal komandas ir papildomus parametrus atlieka kreipinius į vartotojų valdymo bei duomenų valdymo sistemas. Šiose sistemose atlikti įrašai suformuoja taisykles, kurios atitinka prieigos politikos dokumente formuojamą prieigos politiką.

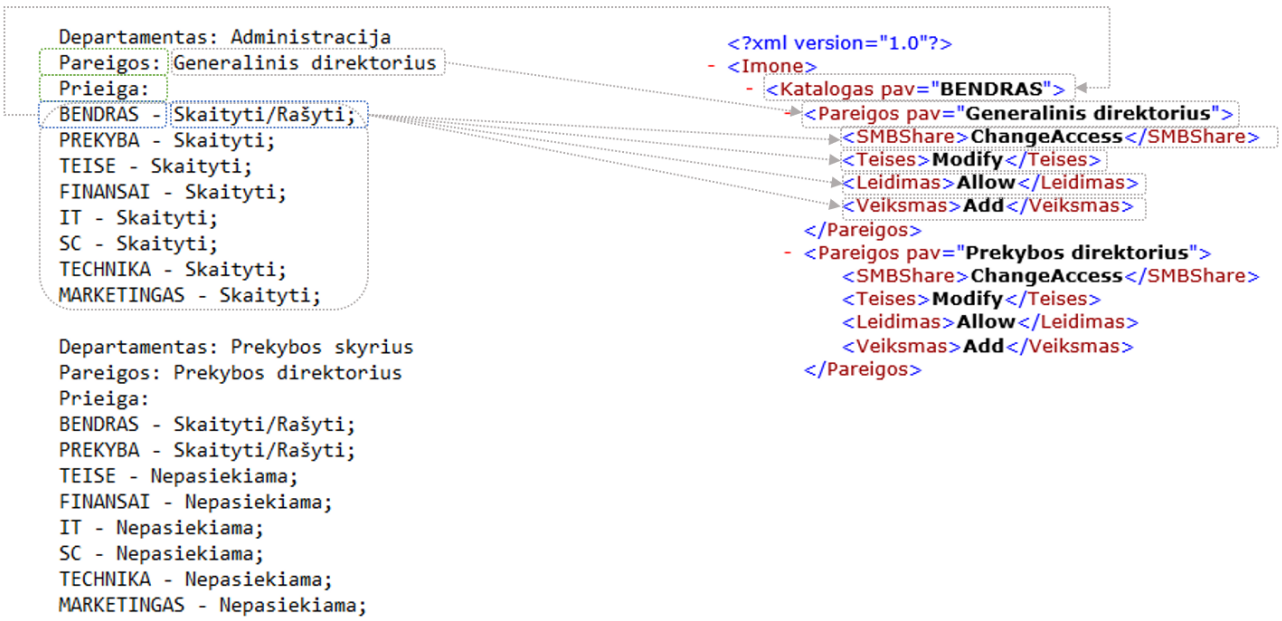
2.3. Prieigos valdymo politikos dokumento konvertavimas

Organizacijose, kuriose taikoma informacijos saugos politika, būtinai turėtų būti ir prieigos politikos dokumentas, kuris aprašytų ir fizinės saugos sąlygas, ir kibernetinės ar informacinės saugos taisykles. Kaip numato „ISO 27001“ standartas, šis dokumentas turėtų būti reguliariai peržiūrimas, atnaujinamas bei tvirtinamas aukščiausių vadovų, o pastarieji, arba jų įgalioti asmenys, turėtų užtikrinti, kad šio dokumento reikalavimų yra laikomasi ir jis tinkamai įgyvendinamas. Tačiau ne retai šioje vietoje iškyla didžiausi iššūkiai, nes įmonės vadovas/-ai dažniausiai šiais užduotis perduoda pavaldžių skyrių vadovams, o šie – savo pavaldiniams. Kartais tokių užduočių perskirstymas paliečia kelias vadovų ir pavaldinių grandis, tad atsiranda didelė tikimybė prarasti dalį informacijos, padaryti klaidų ar neužtikrinti atlikto darbo kokybės, todėl geriausias sprendimas būtų tiesiogiai naudoti prieigos politikos dokumentą, kurį patvirtino vadovybė, prieigos taisyklių formavimui. Toks užduoties pateikimas leis panaudoti informaciją iš pirminio šaltinio - sistemų administratoriui liks gautą dokumentą importuoti į programą, o ši atliks visus likusius veiksmus.

Tokiam procesui sudėtingumo įneša tai, kad sunku panaudoti nestruktūrizuotus duomenis automatizuotam prieigos suteikimui, todėl prieigos politikos dokumentą reikėtų konvertuoti į tokią formą, kokią suprastų programa. Dažniausiai naudojami json, xml, csv formatai, kurie savo struktūra griežtai aprašo naudojamus duomenis, todėl gana paprasta programiniam kodui juos nuskaityti ir interpretuoti.

Šiame metode pasirinkta XML duomenų aprašymo struktūra, kurios savybės leidžia lanksčiai valdyti duomenų laukus, yra puikiai suprantamas ne tik programiniam kodui, tačiau ir žmogui.

Dokumento konvertavimas atliekamas išfiltruojant tik reikiamą tekstą iš dokumento. Tai atliekama ieškant raktinių žodžių, kurie padeda identifikuoti svarbius duomenis. Atliktus šių svarbų duomenų atskyrimą nuo pašalinio teksto, jie yra interpretuojami ir pradedama formuoti XML struktūra.



2.4 pav. Dokumento konvertavimas į xml.

Suformuota struktūra su duomenimis ir duomenų laukų pavadinimais saugoma atskirame dokumente tolimesniam naudojimui.

Šis procesas reikalauja, kad būtų laikomasi tam tikros struktūros pradiniame prieigos saugos valdymo politikos dokumente ir tik tokiu atveju galima sėkminga dokumento konversija.

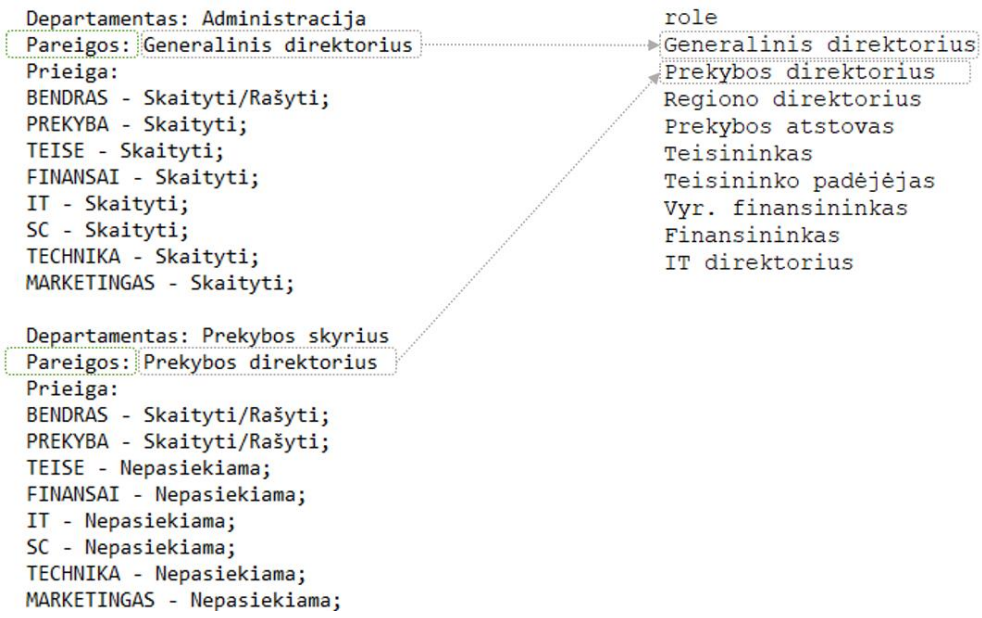
2.4. Scenarijų generavimas

Scenarijų generavimo etape panaudojamas jau formalizuotas prieigos politikos xml dokumentas bei pasitelkiamas personalo duomenų failas, kuris papildo duomenų aibę aktualiausiais organizacijos duomenimis, todėl tai užtikrina, kad visi realiai įmonėje dirbantys darbuotojai, kuriems turi būti suteikta vienokia ar kitokia prieiga prie informacijos šaltinių, bus įtraukti į prieigos valdymo įgyvendinimo procesą.

2.4.1. Grupių kūrimo scenarijai

Tam, kad pavyktų realizuoti rolėmis grįstą prieigos valdymo modelį, būtina turėti roles, kurios vartotojams suteiks atitinkamas teises atitinkamuose resursuose. Šiame metode rolių funkciją atlieka vartotojų grupės, kurios kuriamos darbuotojų pareigybių pagrindu. Visi darbuotojai, turintys tokias pačias pareigybes, bus priskirti tai pačiai grupei, o tai reiškia, turės priskirtą tą pačią rolę.

Rolių grupių scenarijų formavimui naudojamas pareigybių sąrašas, kuris prieigos saugos valdymo politikos konvertavimo metu išsaugomas atskiru dokumentu.



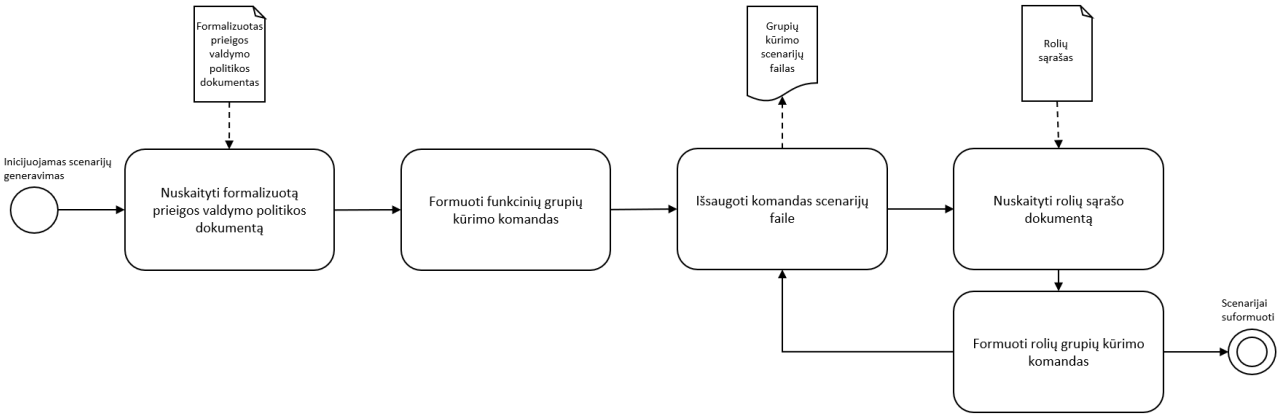
2.5 pav. Pareigybių sąrašas.

Rolių grupės savaime neįgyvendina RBAC modelio, nes joms dar nepriskirtos teisės informaciniuose resursuose, todėl pasitelkiamas antrasis grupių tipas – funkcinės grupės. Jų tikslas – kiekviename informaciniame šaltinyje aprašyti konkrečią funkciją. Šiame metode panaudojama keturių tipų funkcinės grupės kiekvienam iš resursų:

- READ – nustato teises atidaryti, skaityti bei kopijuoti failus ir katalogus tik read-only būsenoje. Ši teisė paveldi *ReadData, ReadExtendedAttributes, ReadAttributes* ir *ReadPermissions* teises.
- MODIFY – nustato teises skaityti, rašyti, išrikiuoti katalogų turinį, trinti katalogus ir failus, vykdyti programų failus. Ši teisė paveldi *ReadAndExecute, Write* ir *Delete* teises.
- FULL – visų teisių kombinacija leidžianti atlikti bet kokius veiksmus su katalogais ar failais.
- AUDIT – apjungia vartotojus, kurių veiksmus su informacijos šaltiniais registruos sistema.

Šių grupių kūrimui panaudojamas formalus prieigos politikos dokumentas, iš kurio traukiami resursų, kuriems taikomos prieigos taisyklės, pavadinimai. Kartu su keliais statiniais parametrais sukuriamos vartotojų valdymo sistemoje funkcinės grupės. Šios grupės kituose etapuose taip pat bus priskiriamos informaciniams šaltiniams.

Proceso modelis pateikiamas žemiau esančiame paveikslėlyje.



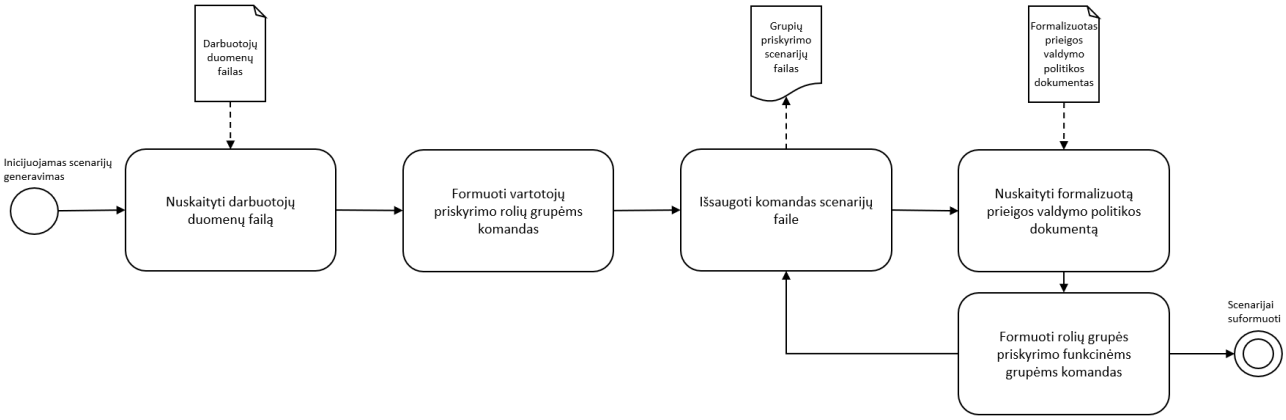
2.6 pav. Grupių kūrimo scenarijų formavimo proceso modelis.

2.4.2. Rolių priskyrimo scenarijai

Turint sukurtas rolių grupes ir funkcines grupes, metodas reikalauja jų susiejimo. Tai rolių grupes padaro rolėmis, nes šios jau savyje apjungia visas priskirtas taisykles. Rolių priskyrimo scenarijams formuoti dar kartą naudojamas formalizuotas prieigos valdymo politikos dokumentas ir personalo duomenų failas.

Šiame etape kuriamos dviejų tipų komandos – vartotojų prikyrimo rolių grupei komandos ir rolių grupės priskyrimo funkcinėms grupėms komandos.

Formuojamose komandose rolių grupės nurodomos pagal kiekvienam darbuotojui priskirtas pareigas, o funkcinės grupės formuojamos pagal politikoje nurodytas prieigos taisykles kiekvienai iš pareigybių.

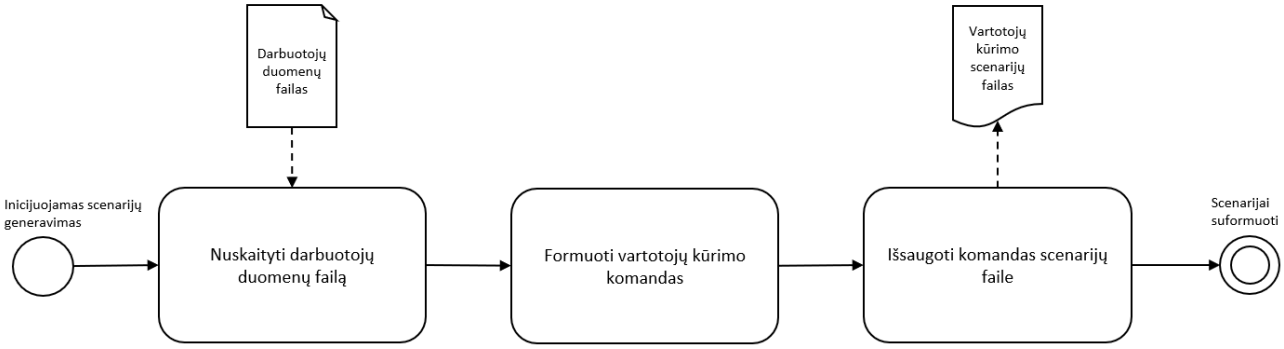


2.7 pav. Grupių priskyrimo scenarijų formavimo proceso modelis.

Proceso modelyje, pateiktame aukščiau, atvaizduojamas išorinių duomenų failų panaudojimas scenarijų generavimui. Dėl programai suprantamo formato, šie duomenų failai lengvai skaitomi ir jų duomenimis paprasta manipuliuoti, tad komandų struktūros formavimas vyksta gana greitai ir tiksliai. Rezultatas – gaunamas dar vienas konkrečia užduotį turintis scenarijų failas.

2.4.3. Vartotojų kūrimo scenarijai

Paskutiniame scenarijų generavimo etape panaudojamas tik darbuotojų duomenų failas, kuris leidžia formuoti komandas visiems organizacijoje tuo momentu esantiems darbuotojams, nepriklausomai nuo to, kada buvo paskutinį kartą peržiūrėta prieigos valdymo saugos politika. Tai užtikrina, kad bent vartotojų valdymo sistemoje bus sukurti visi vartotojai, kuriems leidžiama naudotis informacinėmis sistemomis.



2.8 pav. Vartotojų kūrimo scenarijų formavimo proceso modelis.

Šiuo etapu užbaigiamas trijų scenarijų rinkinių failų kūrimas.

2.5. Scenarijų vykdymas

Šio proceso metu inicijuojamas scenarijų failuose esančių komandų ir joms priskirtų parametrų vykdymas, todėl kreipiamasi į tikslines sistemas ir jose atliekami pakeitimai ar kuriami nauji įrašai. Šį etapą galima suskirstyti pagal sistemas, į kurias siunčiamos užklausos.

2.5.1. Vartotojų valdymo sistema

Ši sistema atsakinga už darbuotojams, procesams ar funkcijoms priskirtų vartotojų valdymą, autentifikavimą ir autorizavimą, todėl naujų vartotojų, rolių ir funkcinių grupių kūrimas vykdomas būtent čia. Scenarijuose aprašytos komandos vykdomos viena po kitos, taip kuriant naujus įrašus vartotojų valdymo sistemoje. Esant klaidingai suformuotai komandai, grąžinamas klaidos pranešimas ir pereinama prie kitos komandos vykdymo, kol pasiekiama scenarijų failo pabaiga.

Sukūrus naujus vartotojus ir grupes, vykdomas trečiasis scenarijų failas, kuris susieja šiuos subjektus tarpusavyje pagal prieigos politikoje aprašytas taisykles. Nuo šio momento rolių grupės įgyja tikrų rolių iš rolėmis grįsto prieigos valdymo modelio savybes.

2.5.2. Duomenų valdymo sistema

Prieigos valdymo saugos politikos įgyvendinimas užbaigiamas inicijuojant informacinių resursų, aprašytų politikoje, sukūrimu (jei infrastruktūra nauja ar dalis politikoje aprašytų šaltinių yra nauji). Tai atlieka paskutinysis scenarijų failas, kuris kuriamas iš prieigos politikos jos konvertavimo į formalizuotą dokumentą metu. Šiame etape taip pat atliekamas funkcinių grupių rinkinio priskyrimas kiekvienam iš kuriamų resursų.

2.6. Išvados

Prieigos valdymo politikos automatizuoto įgyvendinimo metodas sudarytas iš kelių, tampriai vienas su kitu susijusių, etapų. Išnagrinėjus kiekvieną jų galima padaryti tokias išvadas:

1. Prieigos valdymo saugos politikos įgyvendinimo automatizavimas yra būtinas, norint, kad kuo daugiau organizacijų tinkamai valdytų prieigą prie savo informacinių šaltinių;
2. Rolėmis grįstas prieigos valdymo modelis yra vienas patogesnių būdų valdyti organizacijos prieigos politiką, nes yra gana aiškus, lengvai audituojamas ir patogus;
3. Prieigos valdymo saugos politikos dokumento formalizavimas į programoms suprantamą formatą yra svarbus žingsnis siekiant proceso automatizavimo;
4. Automatizavimas ženkliai sumažina politikos įgyvendinimo laiko sąnaudas.

3. PRIEIGOS VALDYMO POLITIKOS AUTOMATIZUOTO ĮGYVENDINIMO SISTEMOS PROTOTIPAS

Projekto prototipui įgyvendinti iškeliami funkciniai ir nefunkciniai reikalavimai, kurie padės sudėlioti gaires prototipo kūrimui. Taip pat, aprašomi pradiniai duomenų failai, jų struktūra ir reikalavimai, sudaromas prototipo modelis ir aprašomas funkcionalumas.

3.1. Funkciniai reikalavimai

1. Prototipas turi gebėti atlikti naujos infrastruktūros prieigos modelio pagal saugos politiką įgyvendinimą.
2. Prieigos formavimui ir scenarijų kūrimui naudojami papildomi išoriniai duomenys – prieigos saugos politika ir personalo duomenų bazė.
3. Prieigos politikos dokumentas konvertuojamas į XML.
4. Konvertuotas prieigos politikos dokumentas eksportuojamas į atskirą XML failą, kuris bus naudojamas kituose etapuose.
5. Personalo duomenų failo importavimas.
6. Iš turimų duomenų formuojami scenarijai. Naudojama *Powershell* programavimo sintaksė.
7. Suformuotų scenarijų vykdymas.
8. Numatytam funkcionalumui įgyvendinti pasitelkiama grafinė vartotojo sąsają.
9. Realizacija vykdoma UAB „Įmonė“ įmonės infrastruktūroje.
10. Rezultatams vertinti naudojamas organizacijos struktūros modelis.
11. Realizacija vykdoma Windows operacinėje sistemoje, naudojant Microsoft *Powershell* programavimo kalbą.
12. Sukurtas metodas atliekamas sistemų administratoriaus ir tik aukščiausiomis teisėmis.
13. Operacijos vykdomos lokaliai tiksliniame serveryje.
14. Programa turi duoti grįžtamąjį ryšį apie funkcijos atlikimą ar pasirodžiusias klaidas.

3.2. Nefunkciniai reikalavimai

1. Vartotoja sąsaja turi būti aiški ir lengvai suprantama.
2. Metodas turi atlikti prieigos politikos įgyvendinimą tiksliai ir be klaidų.
3. Metodas turi pasižymėti dideliu atlikimo greičiu.
4. Operacijos atliekamos tik turint tinkamo formato pradinius duomenis.
5. Programos meniu išdėstymas turi būti logiškas – prioritetas nustatomas iš kairės į dešinę ir iš viršaus į apačia.
6. Pilnavertiškam užduoties atlikimui turi būti įvykdomos visos programoje numatytos funkcijos.

3.3. Pradiniai duomenys

Žinant reikalavimus prototipui, galima aprašyti pradines sąlygas ir duomenis, kuriuos turint bus vykdomos užduotys. Organizacinė struktūra ir darbuotojų duomenys gaunami iš organizacijos atsakingos skyriaus ar specialisto, o prieigos saugos politika iš organizacijos vadovo.

3.3.1. Organizacinė struktūra

Organizacinė struktūra – tai visuma priemonių, skirtų darbui suskirstyti į skirtingas užduotis ir šių užduočių vykdymą koordinuoti. Tai taip sutvarkytas vadovavimo lygių ir funkcijų bendradarbiavimas, kad organizacijos tikslų būtų siekiama veiksmingiausiu būdu. Jos esmė – vienų vadovų ar padalinių pavaldumas kitiems. Su struktūra glaudžiausiai susietos dvi koncepcijos: darbo paskirstymo ir kontrolės [13].

Šiame darbe svarbu nustatyti įmonės organizacinę struktūrą, pagal kurią bus galima įvertini projekto rezultatus. Struktūroje vyrauja hierarchinė pavaldumo sistema, kurios viršuje – įmonės direktorius. Einant iš viršaus žemyn sutinkami organizacijos skyrių vadovai ir direktoriai, tada dar žemiau – jiems pavaldūs vadovai ar darbuotojai. Tokia struktūra padės įvertinti, ar prieigos politika atitinka organizacijos hierarchiją, ar metodo sudarytos taisyklės neprasilenkia su schemoje nurodytais skyrių pavadinimais, pareigybėmis, paveldimumu ir pan. Schema pateikta priede Nr. 2.

3.3.2. Organizacijos informacinės saugos prieigos politika

Šis dokumentas turėtų egzistuoti kiekvienoje įmonėje, nes nusako, ką kiekvienas organizacijos subjektas gali daryti ir už ką yra atsakingas. Tokius dokumentus dažniausiai patvirtina aukščiausia organizacijos valdžia bei reguliariai peržiūri ir tvirtina atsiradusius pasikeitimus. Šis dokumentas bus naudojamas suformuoti scenarijų rinkiniui, prieigai prie informacijos konfigūruoti. Iš organizacijos informacinės saugos politikos pasiimant prieigą reglamentuojantį dokumentą gaunama svarbi informacija apie taikomas taisykles prieigos valdymui. Prieigos politikos dokumentas pateikiamas priede Nr.1.

Kuriamas metodas reikalauja, kad prieigos politikos dokumente būtina išlaikytas tam tikras formatas:

1. prieigos teisėms aprašyti naudojamas informacijos šaltinio pavadinimas ir „Skaityti“, „Skaityti/Rašyti“, „Nepasiekiama“ raktinės žymos;
2. prieš išvardinant prieigos teises, nurodyti žyme „Prieiga:“;
3. prieš nurodant pareigybes, pažymėti žyme „Pareigos:“;

Programa, naudodama šiuos raktinius žodžius, galės nustatyti reikšmingus informacijos laukus, tą informaciją išsaugoti ir panaudoti formuojant XML formato dokumentą.

3.3.3. Darbuotojų duomenys

Vienas iš kuriamo metodo funkcinių reikalavimų numato, kad būtų panaudoti vidiniai įmonės darbuotojų duomenys iš žmogiškųjų išteklių ar pan. duomenų bazių. Šie duomenys panaudojami realių vartotojų bei grupių kūrimui informacinėse sistemose.

Kuriamas metodas reikalauja, kad darbuotojų duomenų faile būtų išlaikytas tam tikras formatas:

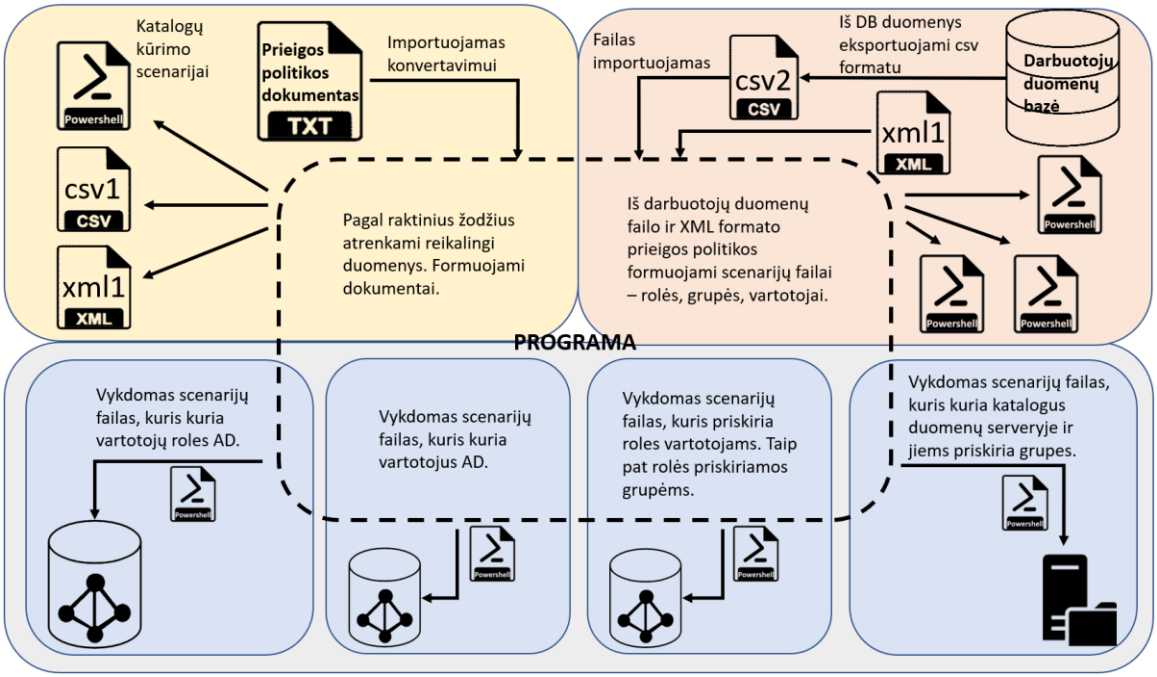
1. Duomenų failas pateikiamas CSV formatu.
2. Duomenų laukai atskirti kabliataškiu.

3. Pirmoje eilutėje nurodyti duomenų laukų pavadinimai:
    a. darbuotojo vardas (privalomas) – „vardas“;
    b. darbuotojo pavardė (privalomas) – „pavarde“;
    c. pareigos (privalomas) – „title“;
    d. įmonės pavadinimas (neprivalomas) – „org“;
    e. departamento pavadinimas (neprivalomas) – „department“;
    f. el. pašto adresas (neprivalomas) – „email“;
    g. telefono numeris (neprivalomas) – „phone“;
    h. kiti duomenų laukai (neprivalomi).

3.4. Modelis

Programa talpinama modifikuojamoje sistemoje, „Windows“ operacinės sistemos C:\ skirsnyje. Pagrindinis katalogas vadinamas „Prototipas“, kurio viduje talpinamas pagrindinis programos kodas bei du papildomi darbiniai katalogai – „*Input*“ ir „*Output*“. Pastarajame saugomi visi proceso metu sugeneruoti failai, o „*Input*“ – pradiniai duomenų šaltiniai, kurie importuojami.

Siekiant vizualiai pavaizduoti visą proceso eigą, pateikiama prototipo veikimo loginė schema (3.1 pav.), kurioje išskirti pagrindiniai automatizuoto prieigos politikos įgyvendinimo etapai.



3.1 pav. Projekto schema.

Visa eiga gali būti suskirstyta į 3 dalis:

1. prieigos politikos dokumento konvertavimas į XML formatą.
    a. prieigos politikos dokumento importavimas;
    b. XML struktūros formavimas;
    c. XML eksportavimas į xml failą;
    d. pareigų pavadinimų eksportavimas į csv failą;

e. katalogų kūrimo scenarijų formavimas;
f. katalogų kūrimo scenarijų eksportavimas į *Powershell* failą.

2. Darbuotojų duomenų importavimas ir scenarijų generavimas.
   a. darbuotojų duomenų failo importavimas;
   b. prieigos saugos politikos xml failo importavimas;
   c. vartotojų kūrimo scenarijų formavimas;
   d. vartotojų kūrimo scenarijų eksportavimas į *Powershell* failą;
   e. grupių kūrimo scenarijų formavimas;
   f. grupių kūrimo scenarijų eksportavimas į *Powershell* failą;
   g. vartotojų priskyrimo grupėms scenarijų formavimas;
   h. vartotojų priskyrimo grupėms scenarijų eksportavimas į *Powershell* failą.
3. Sukurtų scenarijų vykdymas, prieigos politikos taisyklių realizavimas.
   a. vykdomas vartotojų grupių kūrimo scenarijų failas;
   b. vykdomas vartotojų kūrimo scenarijų failas;
   c. vykdomas vartotojų priskyrimo grupėms scenarijų failas;
   d. vykdomas katalogų kūrimo scenarijų failas.

Šie trys etapai visiškai realizuoja prieigos valdymo politikos automatizuotą įgyvendinimą – nuo dokumento konvertavimo, panaudojimo scenarijams kurti iki vykdymo.

3.5. Prieigos politikos dokumento konvertavimas

Pirmasis etapas – tai prieigos politikos dokumento konvertavimas į struktūrizuotą XML formatą. Kaip ir minėta anksčiau, XML kalba pasirinkta todėl, kad gali griežta struktūra aprašyti naudojamus duomenis, yra lengvai plečiama ir redaguojama bei puikiai tinka duomenų perdavimui programoms.

Prieigos politikos dokumentas (priedas Nr.1), kuris atitinka šiame metode keliamus reikalavimus, importuojamas į programą. Visi importuojami dokumentai įkeliami į programos .*Input*\ katalogą.

Dokumento turinys nuskaitomas *Powershell* komanda *Get-Content.* Taip pat pridedamas parametras – *Encoding UTF8*, kuris užtikrina, kad visi dokumente esantys lietuviški simboliai taip pat bus taisyklingai nuskaityti. Šios funkcijos metu nuskaitomas visas dokumento turinys, todėl prieš pradedant apdoroti, turima daug perteklinės informacijos, kuri nereikalinga.

Svarbių duomenų filtravimui pasitelkiamas duomenų formato šablonas, kuris ieško raktinės žymės „Departamentas“ ir pažymi viską, kas dokumente žemiau jos. Toks būdas leidžia užtikrinti, kad programai reikalingi duomenys šio filtravimo metu nebus praleisti.

Kitas turimų duomenų apdorojimas vykdomas *ForEach-Object* ciklo komanda. Kartu su -*replace* parametru ši funkcija įgalina kiekvienai nuskaitytai eilutei priskirti kurią nors kitos eilutės reikšmę, o kadangi yra formuojamas XML dokumentas, privaloma išlaikyti griežtą struktūrą ir hierarchiją, todėl:

- informacijos šaltinių pavadinimai talpinami į XML elementų atributus „pav“, o priekyje pridedama žymė „Katalogas“;
- pareigybių pavadinimai taip pat traukiami į atributus „pav“, o priekyje pridedama žymė „Pareigos“;
- prieigos teisės keičiamos į formalesnius angliškus pavadinimus. Iš vieno parametro interpretuojant padaromi keturi:
    - „SMBShare“ elementas:
        - „Skaityti/Rašyti“ į „ChangeAccess“;
        - „Skaityti“ į „ReadAccess“;
        - „Nepasiekiama“ į „NoAccess“.
    - „Teises“ elementas:
        - „Skaityti/Rašyti“ į „Modify“;
        - „Skaityti“ į „Read“;
        - „Nepasiekiama“ į „Read“.
    - „Leidimas“ elementas:
        - „Skaityti/Rašyti“ į „Allow“;
        - „Skaityti“ į „Allow“;
        - „Nepasiekiama“ į „Deny“.
    - „Veiksmas“ elementas:
        - „Skaityti/Rašyti“ į „Add“;
        - „Skaityti“ į „Add“;
        - „Nepasiekiama“ į „Block“.
- Prieigos teisės įtraukiamos į elementą „Teises“;
- Kiekvienam elementui sukuriama jo pabaigos žymė;
- Visi elementai apgaubiami ženklais „<“ ir „>“.

Toks formatavimas leidžia sukurti pilnavertišką XML dokumentą. Dokumento struktūros fragmentas pateikiamas paveiksle žemiau, o visas konvertuotas dokumentas – priede Nr.3.

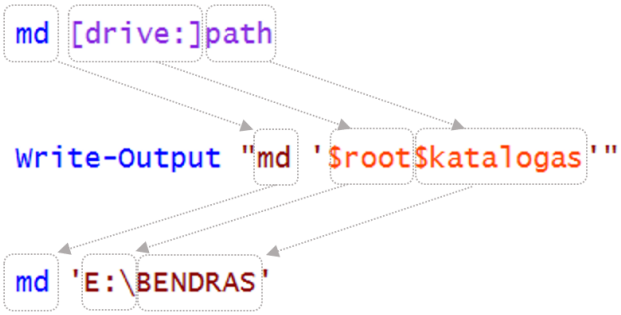
```
<?xml version="1.0"?>
- <Imone>
  - <Katalogas pav="BENDRAS">
    - <Pareigos pav="Generalinis direktorius">
        <SMBShare>ChangeAccess</SMBShare>
        <Teises>Modify</Teises>
        <Leidimas>Allow</Leidimas>
        <Veiksmas>Add</Veiksmas>
      </Pareigos>
    - <Pareigos pav="Prekybos direktorius">
        <SMBShare>ChangeAccess</SMBShare>
        <Teises>Modify</Teises>
        <Leidimas>Allow</Leidimas>
        <Veiksmas>Add</Veiksmas>
      </Pareigos>
    - <Pareigos pav="Regiono direktorius">
        <SMBShare>ChangeAccess</SMBShare>
        <Teises>Modify</Teises>
        <Leidimas>Allow</Leidimas>
        <Veiksmas>Add</Veiksmas>
      </Pareigos>
```

3.2 pav. XML dokumento fragmentas.

Suformuotas XML dokumentas saugomas programos .*Output*\ kataloge, iš kur vėliau bus naudojamas kitose funkcijose.

Po XML dokumento formavimo sukuriamas informacijos šaltinių scenarijų failas, kuris iš prieigos politikos dokumento išfiltruoja visus pavadinimus, kam bus taikomos prieigos taisyklės ir suformuoja tų informacijos šaltinių sukūrimo komandas.

Naudojama funkcija „md“, kurios sintaksė gana paprasta.



3.3 pav. Katalogų kūrimo komandų sintaksė.

Taip pat, atskiru csv failu išsaugomos tik „Pareigos“, kurios bus naudojamos kaip rolių sąrašas.

```
1  role
2  Generalinis direktorius
3  Prekybos direktorius
4  Regiono direktorius
5  Prekybos atstovas
6  Teisininkas
7  Teisininko padėjėjas
```

3.4 pav. Rolių sąrašo pavyzdys.

3.6. Darbuotojų duomenų importavimas

Šis etapas gali būti skirstomas į tris dalis, nes kiekvienoje jų sukuriamas scenarijų failas su skirtingomis užduotimis. Funkcijos iniciavimo pradžioje prašoma suvesti organizacijos domeno vardą.

3.6.1. Grupių kūrimas

Šioje *Powershell* funkcijos dalyje iš anksčiau sukurto rolių sąrašo ir prieigos politikos XML dokumento „*Foreach“* ciklo komandos pagalba formuojamas pirmasis scenarijų failas, kuriame kuriamos dviejų šiek tiek skirtingų tikslų komandos:

- Rolių kūrimas – iš anksčiau sukurto atskiro rolių (pareigybių) failo formuojamos komandos naujoms *Active Directory* vartotojų grupėms, kurios prilyginamos rolėms, sukurti. Šios grupės atliks vartotojų rolių funkciją. Formuojant panaudojama „*New-ADGroup“ Powershell* komanda bei papildomi statiniai parametrai. Taip pat,

panaudojamas funkcijos pradžioje nurodytas domeno vardas. Įrašai saugomi ps1 formato faile.

3.5 pav. *New-ADGroup* komandų pavyzdys.

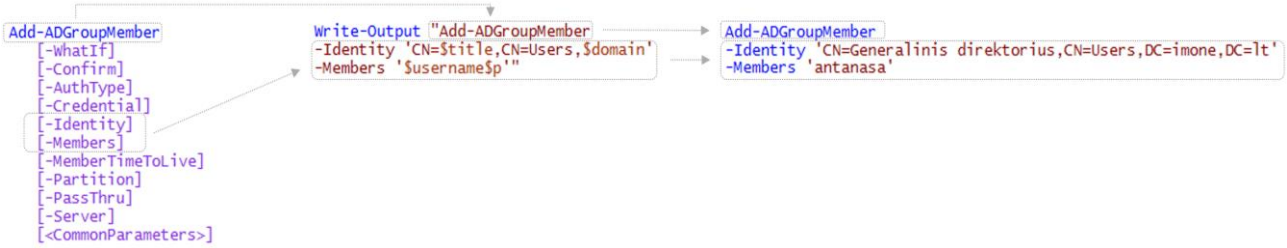
- Funkcinių grupių kūrimas – iš konvertuotos prieigos politikos failo *ForEach-Object“* ciklo komandos pagalba formuojamas dar vienas blokas scenarijų, skirtų *Active Directory* grupių kūrimui, tačiau šių grupių paskirtis kita – jos atliks rolių teisių nustatymo funkciją. Formavimui naudojama ta pati „*New-ADGroup“* komanda bei statinių parametrų rinkinys, tačiau pavadinimą sudarys ne pareigybė, o informacijos ištekliaus pavadinimas, „ACL_“ priešdėlis, nurodantis specialią grupių paskirtį bei „_READ“, „_MODIFY“, „_FULL“ arba „_AUDIT“ galūnės. Jos nurodo suteikiamų teisių ypatybes.
  Taip pat, panaudojamas funkcijos pradžioje nurodytas domeno vardas. Įrašai saugomi prieš tai jau suformuotame ps1 formato faile, kuris tik papildomas naujais įrašais. Suformuotų komandų pavyzdys pateikiamas žemiau.

3.6 pav. *New-ADGroup* komandų pavyzdys.

3.6.2. Rolių priskyrimas

Antroji dalis – rolių priskyrimo scenarijų formavimas – vykdomas iš darbuotojų duomenų failo bei prieigos saugos XML bylos. Ši funkcijos dalis taip pat kuria dviejų skirtingų tipų, tačiau struktūriškai panašias, komandas.

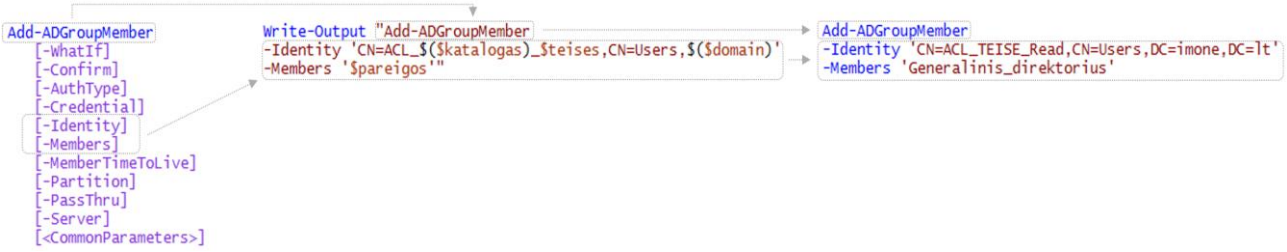
- Vartotojų priskyrimas rolėms. Pagal CSV faile esančius duomenų laukų pavadinimus duomenys išfiltruojami ir panaudojami *„Foreach“* cikle, kuris suformuoja komandas. Šiame etape naudojama *„Add-ADGroupMember“* komanda. Pavyzdys pateikiamas žemiau.



3.7 pav. *Add-ADGroupMember* komandų pavyzdys.

Šių komandų tikslas – darbuotojų vartotojus priskirti grupėms, kurios atitinka jų pareigas. Šios grupės tampa vartotojų rolėmis ir nusprendžia, ką ir kur vartotojas turi teisę daryti.
Formuojant taip pat panaudojamas anksčiau įvestas domeno vardas, o vartotojo vardas sudaromas iš darbuotojo vardo ir pavardės pirmos raidės. Įrašai išsaugomi PS1 formato faile.

- Rolių priskyrimas funkcinėms grupėms. Komandos struktūra išlieka tokia pati, tik vietoj rolės pavadinimo nurodomas funkcinės grupės pavadinimas, o rolė pakeičia vartotojo vardą. Pavyzdys žemiau.



3.8 pav. *Add-ADGroupMember* komandų pavyzdys.

Šios komandos atlieka rolių (vartotojų grupių) priskyrimą funkcinėms grupėms, kurios nulemia, kokias teises įgyja vartotojas prie tam tikro informacijos šaltinio. Kaip numatytasis parametras yra administratoriaus priskyrimas „FULL“ teisėms, visi kiti - pagal prieigos saugos politiką. Įrašai išsaugomi prieš tai sukurtame PS1 faile jį papildant.

3.6.3. Vartotojų kūrimas

Vartotojų kūrimo scenarijams suformuoti panaudojamas tik darbuotojų duomenų *csv* failas, kurio duomenys, filtruojant pagal duomenų laukų pavadinimus, „*Foreach*“ ciklo pagalba sudėliojami į komandas – panaudojama „*New-ADUser*“ komanda ir papildomi parametrai:

- **Name** – darbuotojo vardas ir pavardė (*csv* dokumente – „vardas“, „pavarde“);

- **ChangePasswordAtLogon** – reikalavimas pasikeisti slaptažodį pirmo prisijungimo metu;
- **Company** – įmonės pavadinimas (*csv* dokumente – „org“);
- **Department** – departamento, kuriame darbuotojas dirba, pavadinimas (*csv* dokumente – „department“);
- **Description** – vartotojo aprašymas. Panaudojamas pareigų pavadinimas (*csv* dokumente – „title“);
- **DisplayName** – vartojo atvaizdavimo vardas. Panaudojamas darbuotojo vardas ir pavardė (*csv* dokumente – „vardas“, „pavarde“);
- **EmailAddress** – el.pašto adresas (*csv* dokumente – „email“);
- **GivenName** – darbuotojo vardas (*csv* dokumente – „vardas“);
- **Surname** – darbuotojo pavardė (*csv* dokumente – „pavarde“);
- **Title** – darbuotojo pareigos (*csv* dokumente – „title“);
- **SamAccountName** – vartotojo vardas. Negali turėti tarpų, todėl sudaromas iš darbuotojo vardo ir pirmos pavardės raidės. Lietuviškos raidės pakeičiamos lotyniškomis (*csv* dokumente – „vardas“, „pavarde“);
- **Enabled** – nurodoma, jog kuriamas vartotojas iš karto tampa aktyviu;
- **AccountPassword** – nustatomas standartinis ir bendras slaptažodis, kuris pirmo prisijungimo metu bus pakeistas;
- **UserPrincipalName** – vartotojo vardas. Negali turėti tarpų, todėl sudaromas iš darbuotojo vardo ir pirmos pavardės raidės. Lietuviškos raidės pakeičiamos lotyniškomis (*csv* dokumente – „vardas“, „pavarde“). Pridedamas anksčiau įvestas domeno pavadinimas;

Įrašai saugomi atskirame PS1 formato *Powershell* faile. Įrašų pavyzdys pateikiamas žemiau.

3.9 pav. *New-AddUser* komandų pavyzdys.

3.7. Suformuotų prieigos scenarijų vykdymas

Trečiasis viso proceso etapas administratoriui leidžia pradėti vykdyti anksčiau suformuotų scenarijų vykdymą. Mažinant klaidų tikimybę ir palengvinant proceso eigą šį etapas dalinamas į keturis mažesnius etapus, kurie meniu juostoje eina iš eilės.

3.7.1. Grupių kūrimo scenarijų vykdymas

Pirmoji iš keturių funkcijų – grupių kūrimas. Vykdymo metu *Active Directory* duomenų bazėje sukuriamos vartotojų grupės, kurios taps rolėmis, ir funkcinės grupės, kurios aprašys, ką kiekviena iš rolių gali daryti.

3.7.2. Vartotojų kūrimo scenarijų vykdymas

Sekantis žingsnis – vartotojų kūrimas. Vykdymo metu *Active Directory* duomenų bazėje sukuriami nauji vartotojai, kurie, pagal darbuotojų duomenų failą, priskiriami kiekvienam darbuotojui asmeniškai.

3.7.3. Rolių priskyrimo scenarijų vykdymas

Trečiajame etape susiejami nauji vartotojai su naujomis rolėmis, o rolės – su naujomis funkcinėmis grupėmis. Viskas vykdoma pagal prieigos politikos dokumente nurodytas teises.

3.7.4. Duomenų serverio paruošimas

Paskutiniame etape inicijuojamas katalogų kūrimo komandų paleidimas bei funkcinių grupių priskyrimas kiekvienam iš jų. Kiekvienas naujas katalogas turės tokio paties tipo funkcinių grupių rinkinį su tokiomis pačiomis teisėmis, tačiau skirsis jų pavadinimai, priklausomai nuo šaltinio pavadinimo. Auditavimo grupė priskiriama analogiškai.

3.8. Išvados

Sukurtas prieigos valdymo saugos politikos automatizuoto įgyvendinimo prototipas, todėl galima padaryti šias išvadas:

1. Prieigos valdymas automatizuotu būdų yra žymiai efektyvesnis ir tikslesnis už žmogaus atliekamą tą patį darbą.
2. Prototipo darbo rezultatas labai priklauso nuo tvarkingai paruoštų pradinių duomenų failų, todėl itin didelis dėmesys turi tekti iškeltų reikalavimų sekimui.
3. Prototipo grafinė sąsaja visą procesą paverčia dar paprastesniu.
4. Pasirinkta Microsoft Windows platforma ir Windows Powershell programavimo kalba leidžia tiesiausiu keliu įgyvendinti užsibrėžtas užduotis, nes priklauso vienai šeimai ir yra sukurtos dirbti kartu.

4. TYRIMAS

Kad būtų galima įvertinti šio metodo teikiamą naudą, atliekamas prototipo kiekybinis ir kokybinis tyrimai.

4.1. Infrastruktūra

Prieš išbandant prototipą, sukuriama įmonės infrastruktūrą atitinkanti aplinka. Realizacijai bus reikalingas serveris ir vartotojo kompiuteris, kurie kuriami virtualizacijos pagalba. Tam naudojama „VMware Workstation 15 Player“ programinė įranga. Virtuolių mašinų programiniai ir aparatiniai parametrai pateikti lentelėse žemiau.

4.1 lentelė. Serverio parametrai.

Parametro pavadinimas	**Parametras**
Operacinė sistema	Windows Server 2016 Standard
Architektūra	64 bitų
Rolė 1	Active Directory serveris
Rolė 2	Duomenų serveris
Role 3	DNS
Pilnas kompiuterio vardas	SERVER.imone.lt
Operatyvinė atmintis	2 GB
Procesorius	2 branduoliai
Kietasis diskas 1 [C:\]	20 GB
Kietasis diskas 2 [E:\]	5 GB

4.2 lentelė. Vartotojo kompiuterio parametrai.

Parametro pavadinimas	**Parametras**
Operacinė sistema	Windows 10
Architektūra	64 bitų
Pilnas kompiuterio vardas	PC1.imone.lt
Operatyvinė atmintis	2 GB
Procesorius	2 branduoliai
Kietasis diskas 1 [C:\]	15 GB

Serveris (SERVER) yra pagrindinis domeno „imone.lt“ valdiklis. Prie šio domeno taip pat prijungiamas ir vartotojo kompiuteris, jam suteikiamas PC1 pavadinimas.

Duomenų serveryje jokios informacijos nėra, pasidalinta su domeno vartotojais E raide pažymėtas kietojo disko skirsnis. Domeno vartotojams suteiktos Read teisės, administratorių grupei – pilnos teisės, paveldimumas išjungtas.

Active Directory jokios papildomos konfigūracijos neturi, sukurtos tik numatytosios grupės ir vartotojai diegimo metu. Infrastruktūra paruošta.

4.2. Kokybinis prieigos valdymo politikos įgyvendinimo tyrimas

Šiam eksperimentui keliami tikslai:

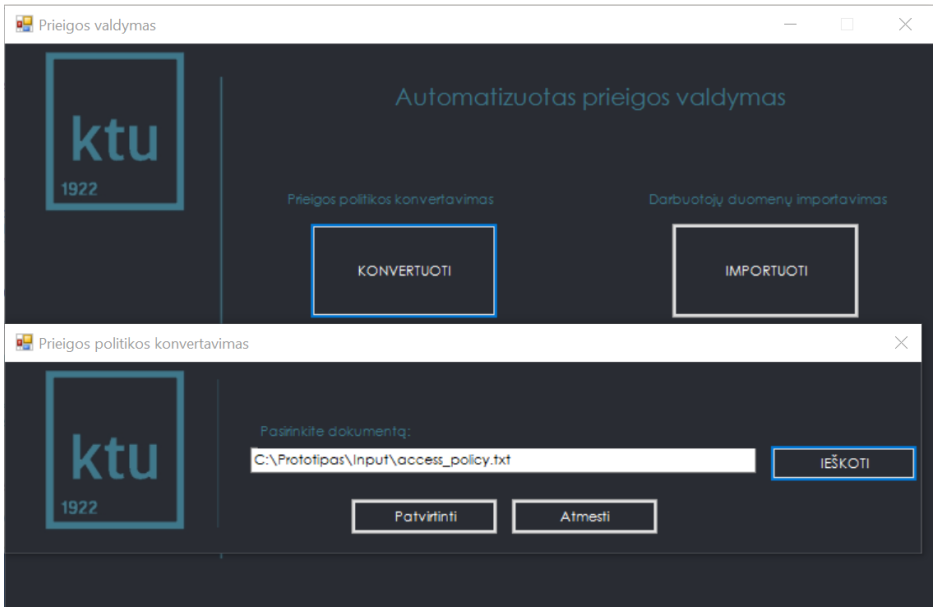
1. Nustatyti prototipo atliekamų funkcijų tikslumą;
2. Patikrinti įgyvendintos politikos veikimą realioje sistemoje;
3. Įvertinti metodui keliamų reikalavimų svarbą sėkmingam procesui užtikrinti.

Po infrastruktūros paruošimo pradedamas pasiruošimas darbui su prototipu. Tam reikalingi pradiniai duomenų failai ir prototipo programinio kodo perkėlimas į darbinę aplinką. Šiuo atveju viskas kopijuojama į serverį „SERVER.imone.lt“, C:\ skirsnį. Kaip ir minėta anksčiau, programos pagrindinis katalogas vadinasi „Prototipas“, o jame programinis kodas „prototipas_v10.ps1“ ir du darbiniai katalogai – „Output“ ir „Input“. Į pastarąjį perkeliami pradinių duomenų failai – prieigos valdymo politikos dokumento failas (access_policy.txt) ir darbuotojų duomenų failas (usr_db_output.csv).

Programa startuojama domeno administratoriaus teisėmis.

4.1 pav. Prototipo vartotojo meniu.

Startavusi programa leidžia pradėti visą procesą nuo prieigos valdymo politikos dokumento (pateikiamas priede Nr. 1) konvertavimo į XML struktūros failą. Mygtukas „KONVERTUOTI“ atveria pradinių duomenų failo pasirinkimo langą. Ieškomas reikalingas dokumentas, jis pasirenkamas ir spaudžiama „Patvirtinti“. Inicijuojamas konvertavimo procesas.



4.2 pav. Prieigos politikos dokumento importavimas.

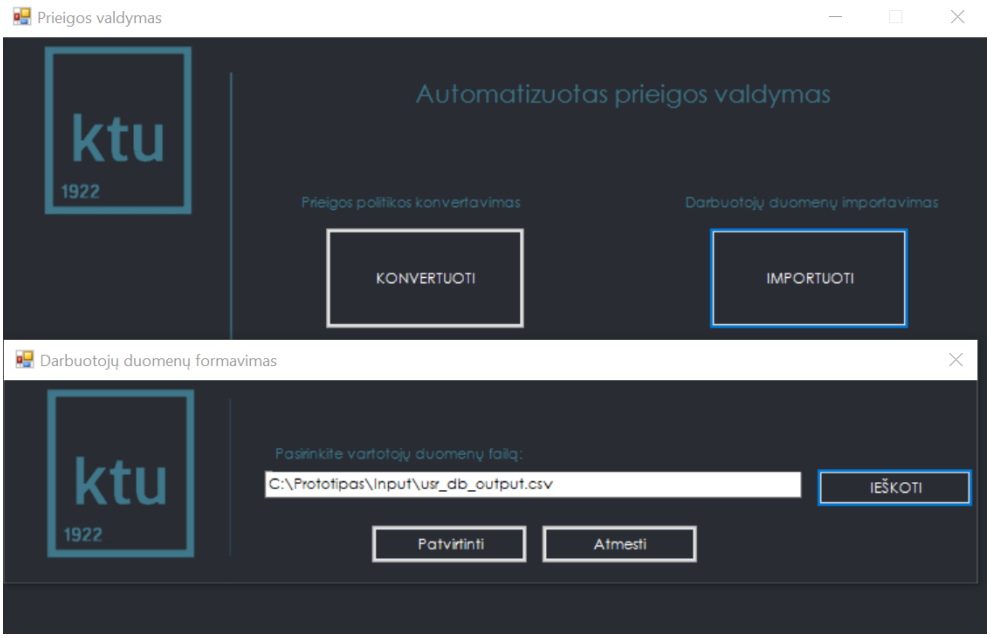
Po dokumento konvertavimo automatiškai startuoja katalogų kūrimo scenarijų formavimas, tad pasirodo klausimas - „Ar tikrai norite generuoti skriptus?“. Atsakius OK programa nukreipia į duomenų serverio skirsnio pasirinkimą, kuriame planuojama kurtį katalogų medį. Pasirenkamas E: skirsnis. Papildomas pranešimas perspėja, kad užduotis atlikta. Šios funkcijos rezultatas xml formatu (AP.xml) ir *Powershell* scenarijų failo formatu (adddirsec_out.ps1) atsiduria „C:\Prototipas\Output“ kataloge.

Po šio etapo vykdomas darbuotojų duomenų importavimas, tad spaudžiamas mygtukas „IMPORTUOTI“ ir atsidariusiame lange pasirenkamas reikalingas dokumentas, spaudžiamas patvirtinimo mygtukas. Darbuotojų duomenų bylos fragmentas pateikiamas žemiau.

```
eil_nr;vardas;pavarde;department;title;email;org;sex;phone;birth
1;Antanas;Antanaitis;Administracija;Generalinis direktorius;antanas@imone.lt;"UAB ""Įmonė""";Vyras;868888888;1986-11-10 00:00
2;Benas;Benauskas;Prekybos skyrius;Prekybos direktorius;benas@imone.lt;"UAB ""Įmonė""";Vyras;868888889;1986-11-11 00:00
3;Domas;Domauskas;Prekybos skyrius;Regiono direktorius;domas@imone.lt;"UAB ""Įmonė""";Vyras;868888890;1986-11-12 00:00
4;Elena;Elenytė;Prekybos skyrius;Prekybos atstovas;elena@imone.lt;"UAB ""Įmonė""";Moteris;868888891;1986-11-13 00:00
5;Fausta;Faustienė;Teisės skyrius;Teisininkas;fausta@imone.lt;"UAB ""Įmonė""";Moteris;868888892;1986-11-14 00:00
6;Giedrė;Giedrienė;Teisės skyrius;Teisininko padėjėjas;giedrė@imone.lt;"UAB ""Įmonė""";Moteris;868888893;1986-11-15 00:00
7;Henrikas;Henrauskas;Finansų skyrius;Vyr. finansininkas;henrikas@imone.lt;"UAB ""Įmonė""";Vyras;868888894;1986-11-16 00:00
8;Ignas;Ignauskas;Finansų skyrius;Finansininkas;ignas@imone.lt;"UAB ""Įmonė""";Vyras;868888895;1986-11-17 00:00
9;Jonas;Jonauskas;IT skyrius;IT direktorius;jonas@imone.lt;"UAB ""Įmonė""";Vyras;868888896;1986-11-18 00:00
10;Karolis;Karoliauskas;IT skyrius;IT projektų vadovas;karolis@imone.lt;"UAB ""Įmonė""";Vyras;868888897;1986-11-19 00:00
11;Laima;Laimutė;IT skyrius;IT Specialistas;laima@imone.lt;"UAB ""Įmonė""";Moteris;868888898;1986-11-20 00:00
12;Monika;Monikaitė;IT skyrius;DB administratorius;monika@imone.lt;"UAB ""Įmonė""";Moteris;868888899;1986-11-21 00:00
```

4.3 pav. Darbuotojų duomenų failas.

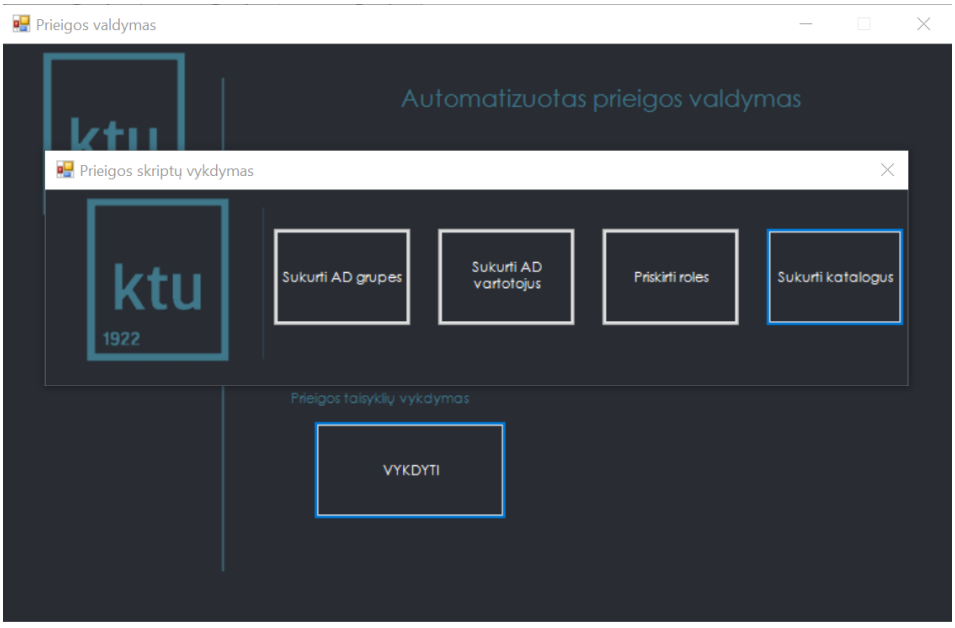
Šis failas taip pat importuojamas iš programos .*Input*\ katalogo.



4.4 pav. Darbuotojų duomenų importavimas

Programai paprašius, suvedamas domeno vardas – „imone.lt“. Neužilgo gaunamas patvirtinimas, kad duomenys importuoti ir scenarijų failai suformuoti sėkmingai. Scenarijų failai (addgroups_out.ps1, addroles_out.ps1, addgroups_out.ps1) eksportuojami į „C:\Prototipas\Output\ katalogą.

Paskutinis etapas – jau sukurtų scenarijų vykdymas. Iš meniu juostos eilės tvarka pasirenkamos užduotys, kurių kiekviena paleidžia tam tikrą scenarijų failą.



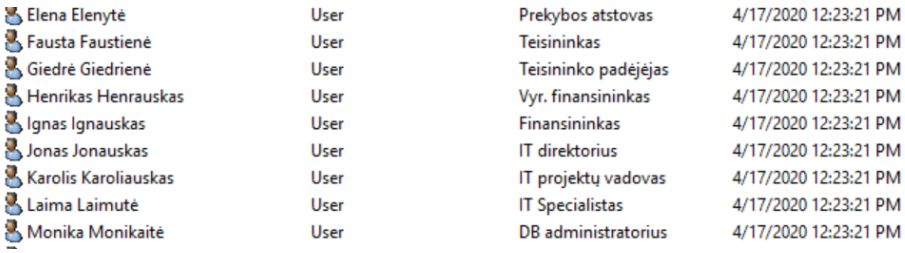
4.5 pav. Prieigos taisyklių vykdymas.

Sukurti AD grupes mygtukas inicijuoja „addgroups_out.ps1“ failo paleidimą. Programai sėkmingai įvykdžius ten aprašytas komandas, pasirodo tai patvirtinantis pranešimas, o vartotojų

duomenų bazėje jau galima matyti rezultatą. Žemiau pateiktame paveiksle matomos naujai sukurtos grupės, kurios atliks rolių ir funkcinių grupių funkcijas.

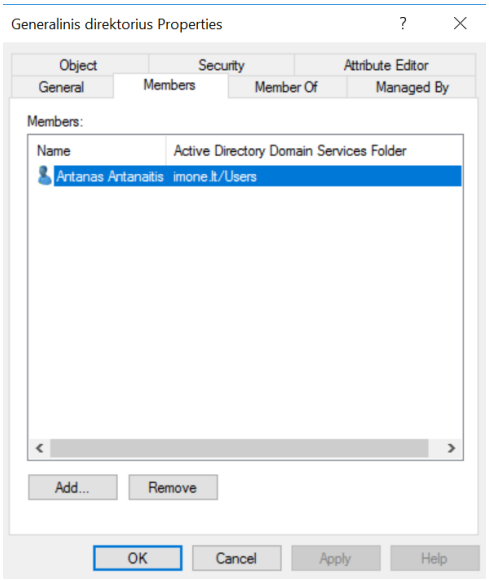
4.6 pav. Naujos grupės *Active Directory* duomenų bazėje.

Sukurti AD vartotojus paleidžia „addgroups_out.ps1“ failą ir ten aprašytos komandos sukuria naujus vartotojus duomenų bazėje. Žemiau pateikiamas rezultatas.



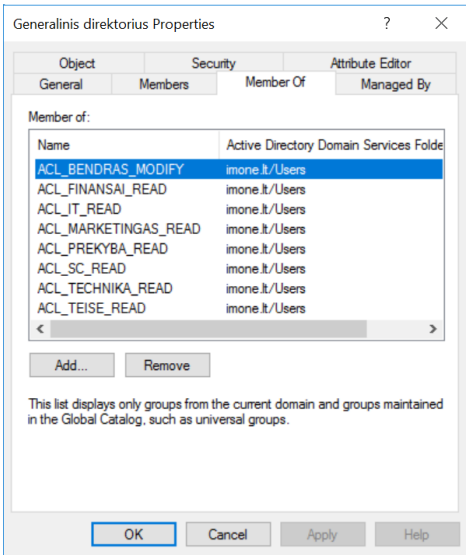
4.7 pav. Nauji vartotojai *Active Directory* duomenų bazėje.

Rolių priskyrimo mygtukas analogiškai paleidžia trečiąjį scenarijų failą – „addroles_out.ps1“ , kuris ką tik sukurtiems vartotojams priskiria rolių grupes. Kaip tai atrodo pavaizduota paveiksle žemiau.



4.8 pav. Rolės priskyrimas vartotojui.

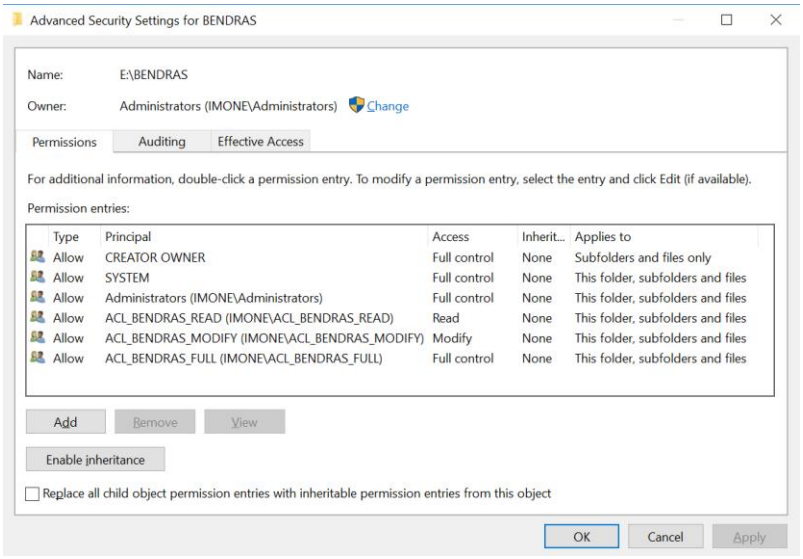
Šiuo atveju matyti, kad vartotojui „Antanas Antanaitis“ priskirta rolė „Generalinis direktorius“, todėl jis įgyja visas šiaip rolei suteiktas teises. Rolės teises įgyja iš priskirtų funkcinių grupių. Funkcinėms grupėms taip pat pagal „addroles_out.ps1“ faile aprašytas taisykles priskiriamos rolių grupės.



4.9 pav. Funkcinių grupių priskyrimas rolei.

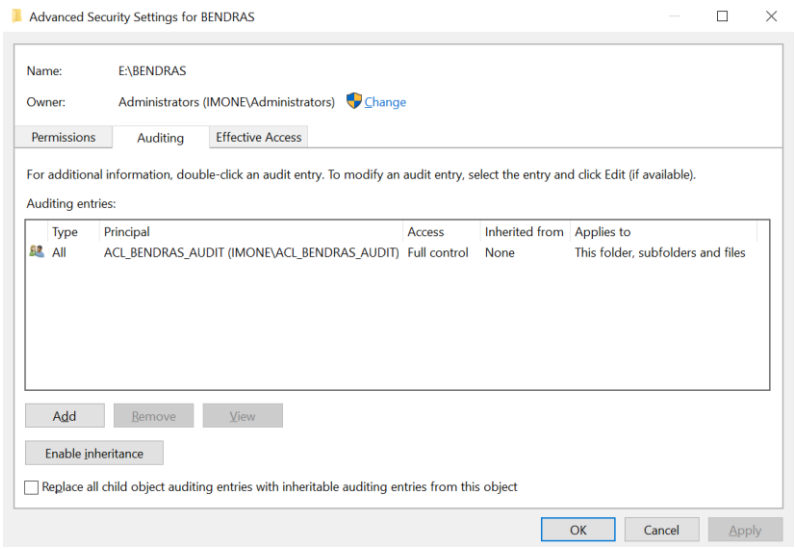
Iš aukščiau pateikto paveikslo matyti, kad rolei „Generalinis direktorius“ priskirtos kelios funkcinės grupės, kurios prie atitinkamų informacinių išteklių suteiks atitinkamas teises.

Galiausiai startuojamas katalogų medžio kūrimas anksčiau nurodytoje vietoje (E:\). Pagal aprašytas „adddirsec_out.ps1“ komandas sukuriami katalogai. Po to programa pasiteirauja, ar vykdyti funkcinių grupių priskyrimą. Atsakius OK, naujiems katalogams sudedamos funkcinės grupės, kurios įgalina atlikti jų leidžiamus veiksmus.



4.10 pav. Funkcinių grupių priskyrimas katalogui.

Taip pat ir auditavimo teisės.



4.11 pav. Auditavimo grupės priskyrimas.

Tipas „*All*“ nusako, kad bus registruojami tiek sėkmingi, tiek nesėkmingi bandymai duomenis pakeisti, ištrinti, sukurti ar pan. O „*Full control*“, jog bus fiksuojami visi įmanomi veiksmai.

Procesas užbaigtas, tad atliekamas priskirtų vartotojo rolių suteiktų teisių patikrinimas prisijungiant prie vartotojo kompiuterio tik jam žinomu vartotojo vardu ir slaptažodžiu bei bandoma pasiekti pagal prieigos valdymo politiką numatytus informacinius resursus.

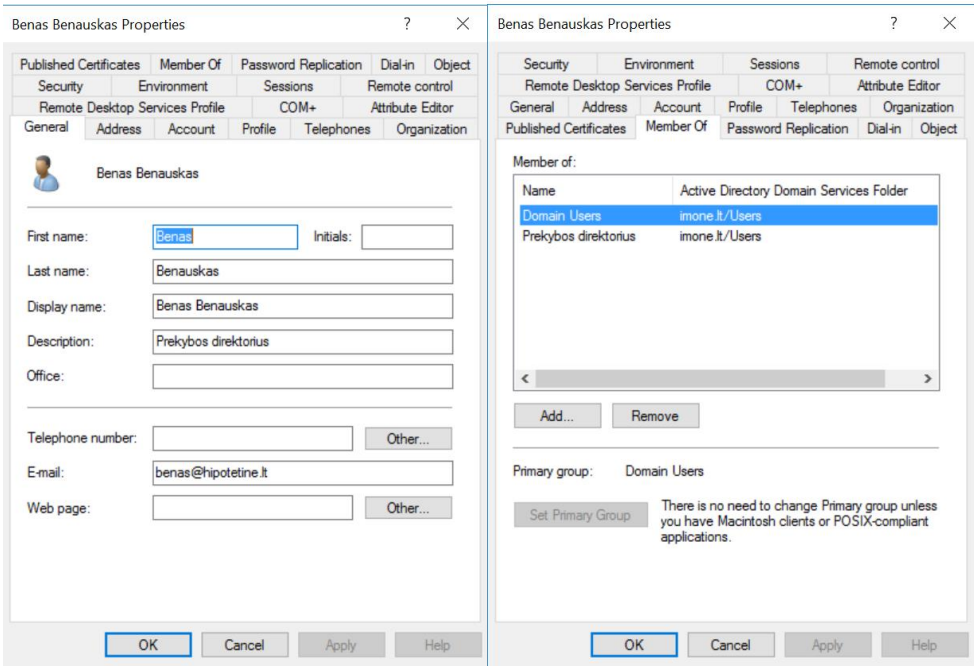
4.2.1. Bandymas Nr. 1

Sąlyga: Organizacijos prieigos valdymo politika numato, kad „Prekybos direktorius“ negali pasiekti katalogo „TEISE“, tačiau gali skaityti ir rašyti kataloge „PREKYBA“.

Taisyklė: Rolė „Prekybos direktorius“ turi būti priskirta funkcinei grupei „ACL_PREKYBA_MODIFY“ ir neturi priklausyti „ACL_TEISE_READ“, „ACL_TEISE_MODIFY“ arba „ACL_TEISE_FULL“ funkcinėms grupėms.

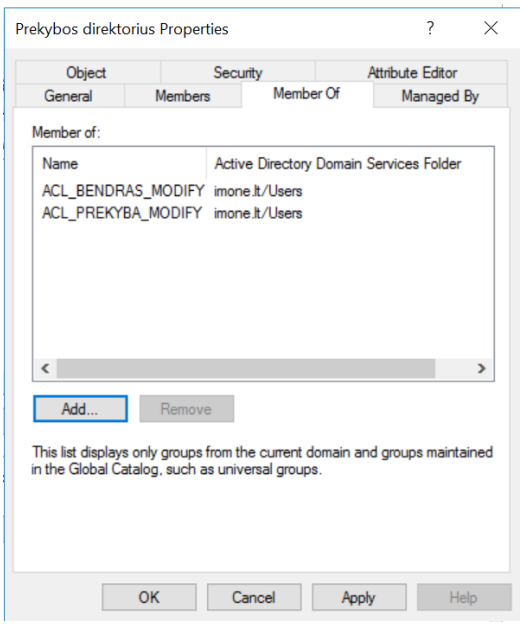
Rezultatas:

Prekybos direktoriaus pareigas įmonėje eina Benas Benauskas.



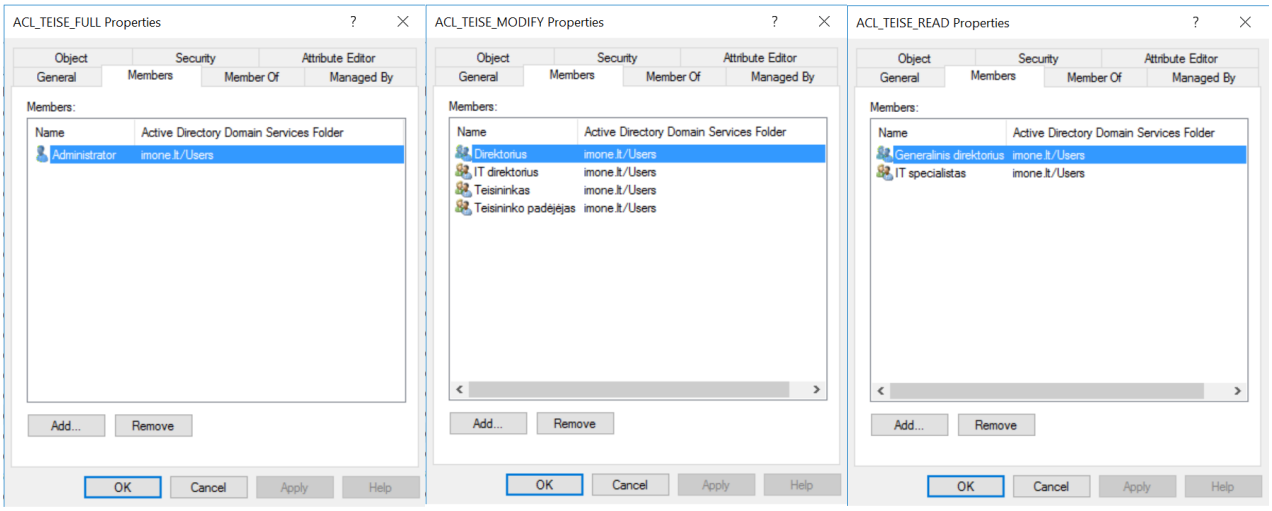
4.12 pav. Beno Benausko vartotojo duomenys.

Todėl jam buvo priskirta „Prekybos direktorius“ rolė, o pastaroji priklauso šioms funkcinėms grupėms (pav. žemiau).



4.13 pav. Prekybos direktoriaus funkcinės grupės.

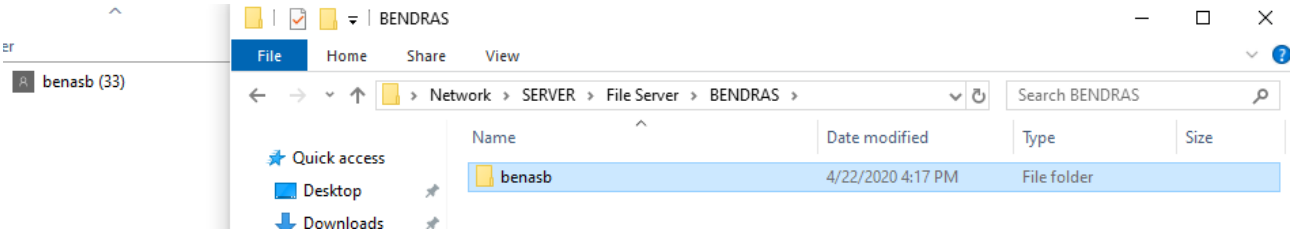
Šios grupės parodo, kad prekybos direktorius gali skaityti ir modifikuoti informaciją kataloge „BENDRAS“ ir „PREKYBA“. Visos kitos informacijos jis turėtų nepasiekti. Taip pat galima patikrinti mus dominančias grupes - „ACL_TEISE_READ“, „ACL_TEISE_MODIFY“ arba „ACL_TEISE_FULL“. Ten turėtų nebūti priskirtos rolės „Prekybos direktorius“.



4.14 pav. TEISE katalogo funkcinių grupių nariai.

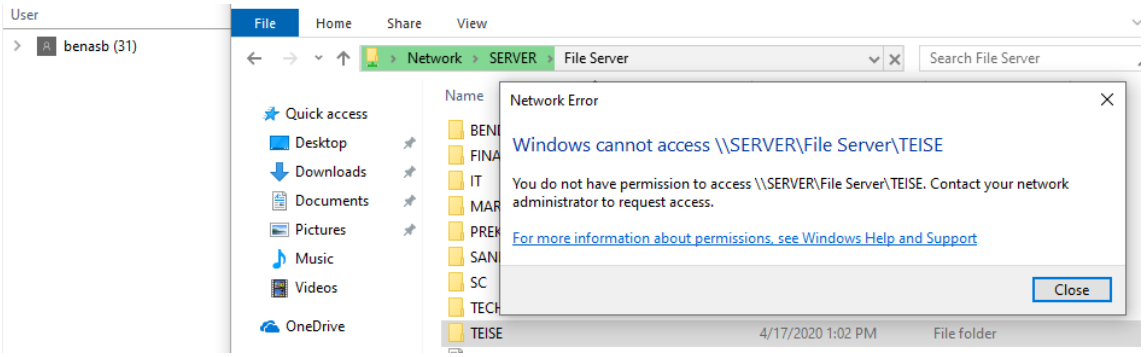
Taigi, panašu, kad viskas įvykdyta taip, kaip ir numatyta prieigos valdymo dokumente. Galiausiai, patikrinama bandant pasiekti duomenis iš vartotojo paskyros.

Leidžia pasiekti „BENDRAS“ katalogą ir ten sukurti naują.



4.15 pav. „BENDRAS“ katalogo modifikavimo teisė.

Draudžia pasiekti „TEISE“ katalogą.



4.16 pav. „TEISE“ katalogo nepasiekiamumas.

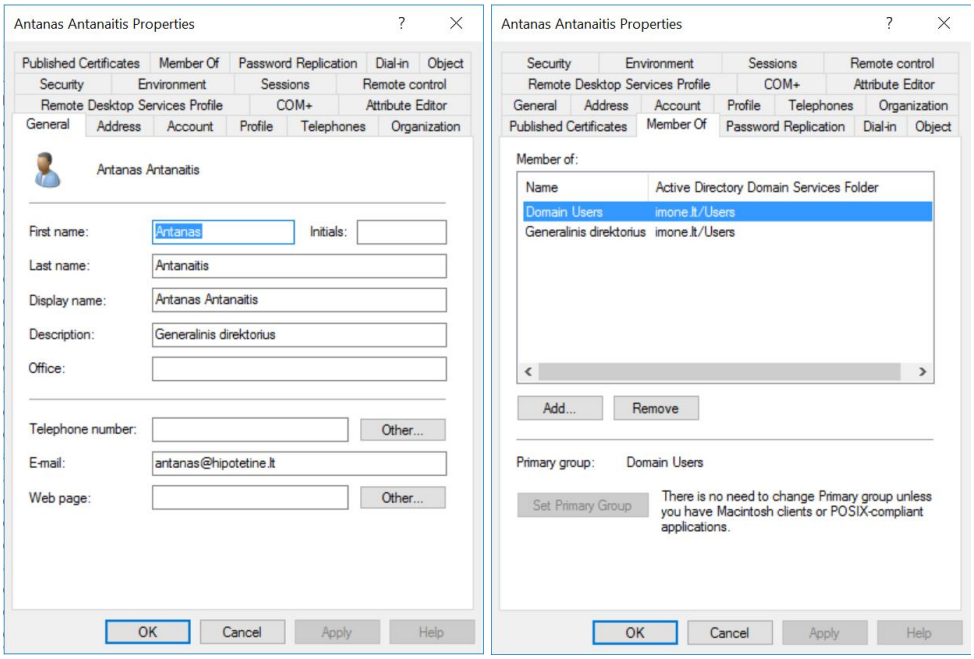
4.2.2. Bandymas Nr. 2

Sąlyga: Organizacijos prieigos valdymo politika numato, kad „Generalinis direktorius“ gali pasiekti visus katalogus, o „BENDRAS“ kataloge gali skaityti ir rašyti.

Taisyklė: Rolė „Generalinis direktorius“ turi būti priskirta visoms funkcinėms grupėms su žymeniu „*_READ“, išskyrus „ACL_BENDRAS_READ“ grupę. Rolė turi būti priskirta „ACL_BENDRAS_MODIFY“ grupei.

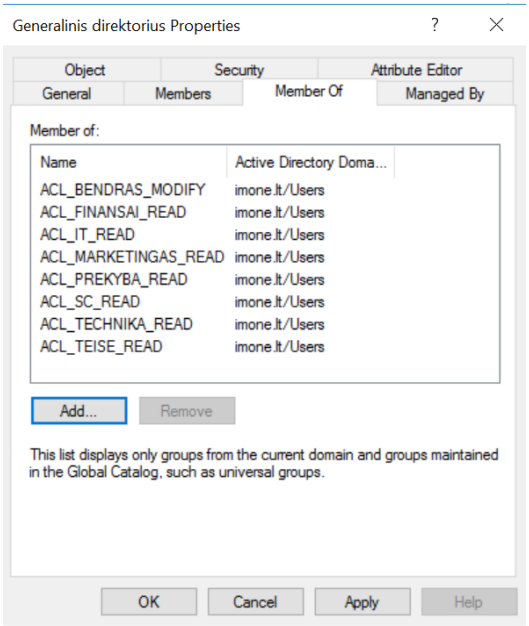
Rezultatas:

Generalinio direktoriaus pareigas įmonėje eina Antanas Antanaitis.



4.17 pav. Antano Antanaičio vartotojo duomenys.

Todėl jam buvo priskirta „Generalinis direktorius“ rolė, o pastaroji priklauso šioms funkcinėms grupėms (pav. žemiau).

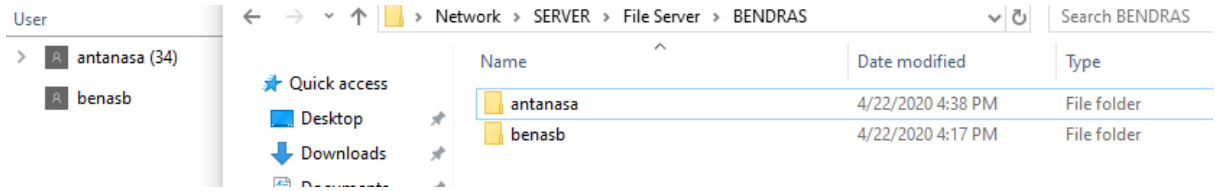


4.18 pav. Generalinio direktoriaus funkcinės grupės.

Šios grupės parodo, kad generalinis direktorius gali skaityti ir modifikuoti informaciją kataloge „BENDRAS“ ir visus kitus katalogus skaityti.

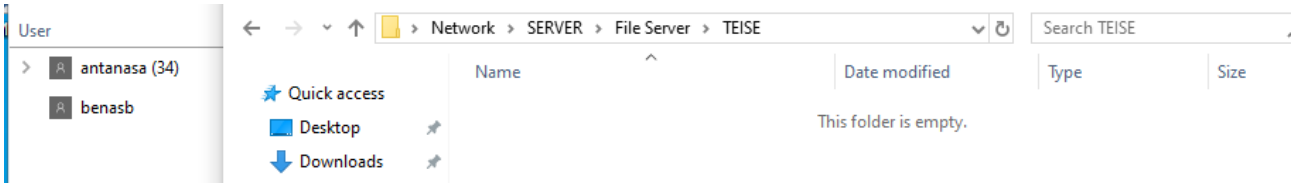
Vėl gi, panašu, kad viskas įvykdyta taip, kaip ir numatyta prieigos valdymo dokumente. Dar patikrinama bandant pasiekti duomenis iš vartotojo paskyros.

Leidžia pasiekti „BENDRAS“ katalogą ir ten sukurti naują.



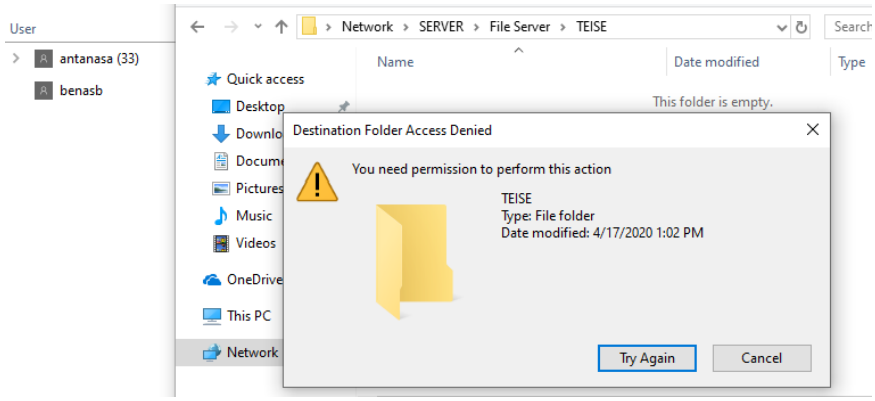
4.19 pav. „BENDRAS“ katalogo modifikavimo teisė.

Leidžia pasiekti „TEISE“ katalogą.



4.20 pav. „TEISE“ katalogo pasiekiamumas.

Bet neleidžia nieko modifikuoti.



4.21 pav. „TEISE“ katalogo „read-only“ teisės.

4.2.3. Apibendrinimas ir išvados

Nuosekliai atlikus visus programoje numatytus veiksmus sėkmingai įgyvendinamas rolėmis grįstas prieigos valdymas, panaudojant prieigos politikos dokumentą. Suformuotas metodas leidžia vartotojams priskirti jiems priklausančias roles, kurios per funkcines grupes suteikia prieigos politikoje aprašytas teises. *Powershell* programavimo kalba padeda visą proceso eigą automatizuoti, todėl administratoriui lieka tik kontroliuoti kiekvieno iš etapų sėkmingą atlikimą.

Šio tyrimo rezultatas – pilnai ir teisingai įgyvendinta prieigos valdymo politika. Visos suteiktos prieigos teisės atitinka politikoje aprašytąsias ir proceso eigoje nenustatyta nei viena klaida. Šį rezultatą pasiekti padėjo tinkamai suformuoti pradinės informacijos duomenų failai bei gerai paruošta infrastruktūra, todėl tai puikiai iliustruoja būtinybę laikytis nustatytų metodo reikalavimų.

4.3. Prieigos valdymo politikos įgyvendinimo trukmės tyrimas

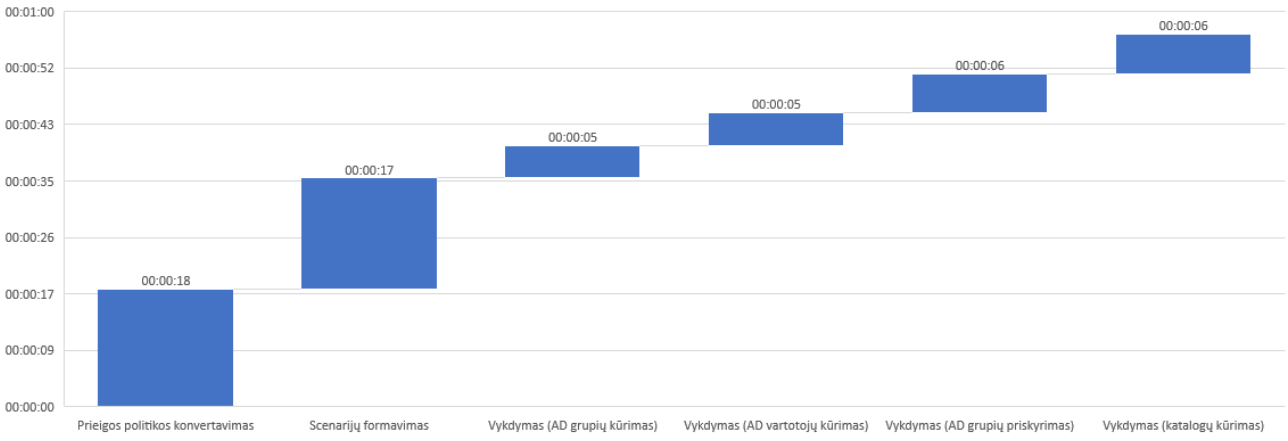
Šiam eksperimentui keliami tikslai:

1. Nustatyti prototipo laiko sąnaudos pilnam prieigos valdymui įgyvendinti;
2. Nustatyti administratoriaus laiko sąnaudas pilnam prieigos valdymui įgyvendinti;
3. Atlikti šių rodiklių palyginimą;
4. Identifikuoti priežastis, nulemiančias rezultatų skirtumus ar sutapimus.

Tyrimui panaudojamas aukščiau aprašytas prieigos valdymo politikos įgyvendinimo procesas, kurio atlikimo trukmė matuojama nuo programos paleidimo iki paskutinio etapo atlikimo. Visas procesas, tai:

- prieigos valdymo politikos dokumento konvertavimas į xml formatą:
  - 19 skirtingų pareigybių;
  - 8 informaciniai šaltiniai;
  - 3 teisių tipai;
- darbuotojų duomenų importavimas ir scenarijų generavimas:
  - 28 -ių darbuotojų duomenys duomenų faile;
- vartotojų kūrimas *Active Directory*;
- grupių kūrimas *Active Directory*;
- rolių priskyrimas vartotojams, funkcinių grupių priskyrimas rolėms;
- infrastruktūros paruošimas;
- funkcinių grupių priskyrimas informaciniams šaltiniams.

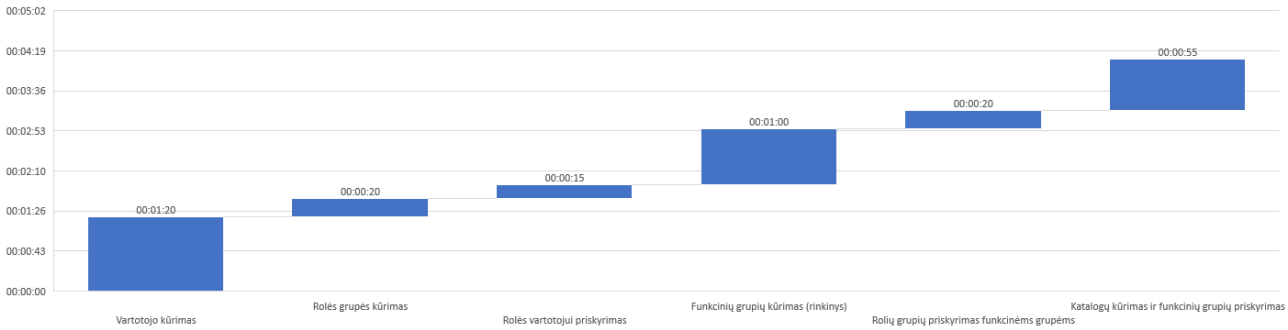
Išmatuota, kad visas procesas trunka šiek tiek mažiau nei minutę.



4.22 pav. Prototipo laiko sąnaudos prieigos valdymui įgyvendinti.

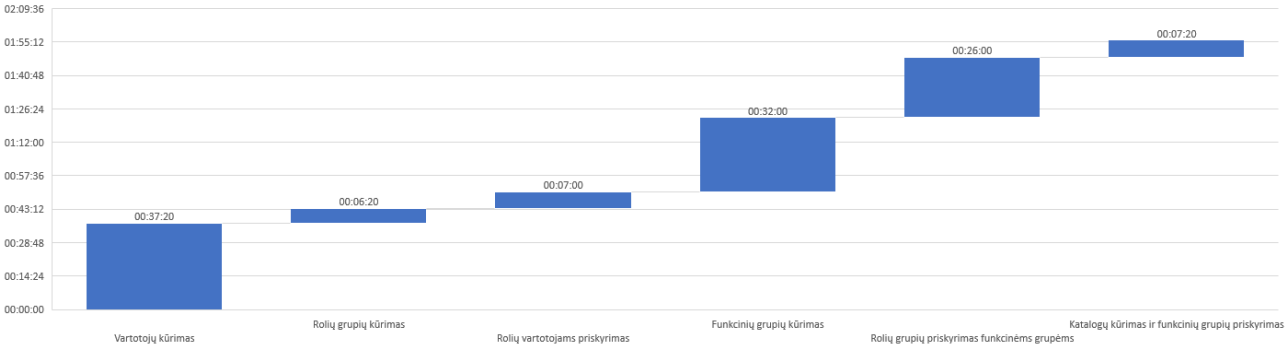
Siekiant išmatuoti, kiek užtruktų administratorius, kol pilnai įgyvendintų prieigos valdymo politiką, simuliuojama po vieną kiekvieno etapo procesą ir dauginama iš atitinkamo kiekio, kuris reikalingas pilnam atlikimui.

Žemiau pateikiamos diagramos, kurios parado, kiek apytiksliai administratorius sugaištų, jei kiekvieną iš etapų bandytų atlikti mechaniškai.



4.23 pav. Administratoriaus darbo laiko sąnaudos vienam ciklui atlikti.

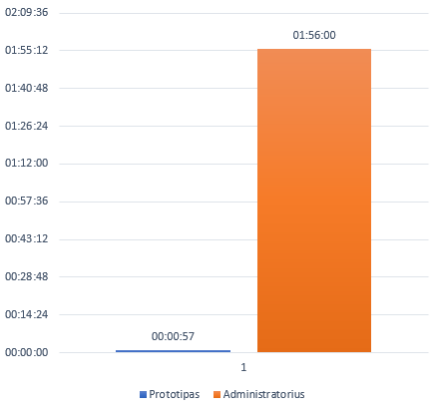
Vieno ciklo trukmė – apie 4 minutes ir 10 sekundžių. Tuo tarpu perskaičiavus preliminarų viso proceso atlikimo laiką gaunama apytikriai 1 valanda 56 minutės.



4.24 pav. Administratoriaus darbo laiko sąnaudos visam procesui atlikti.

4.3.1. Apibendrinimas ir išvados

Logiška, kad programinė įranga pranoko mechaninį administratoriaus darbą, tačiau be aukštos atlikimo spartos prototipas taip pat siūlo aukštą patikimumą, ko negalima pasakyti apie intensyviai tokį darbą dirbantį administratorių, kuris vienu metu turi naudoti kelis informacijos šaltinius, atlikinėti įvairias užduotis bei vesti skirtingus duomenis. Klaidos tikimybė itin aukšta.



4.25 pav. Trukmės palyginimas.

4.4. Didelių pradinių duomenų failų įtakos proceso trukmei tyrimas

Šiam eksperimentui keliami tikslai:

1. Nustatyti politikos dokumento kompleksiškumo įtaką prototipo darbo našumui;
2. Nustatyti kuriamų vartotojų kiekio įtaką prototipo darbo našumui;
3. Rezultatus palyginti.

Kaip nustatyta anksčiau aprašytame eksperimente, prieigos valdymo politikos įgyvendinimas, kur dokumente aprašyta 19 pareigybių, 8 informacijos šaltiniai kartu su darbuotojų duomenų faile pateikiamais 28 vartotojais, užtrunka apie minutę.

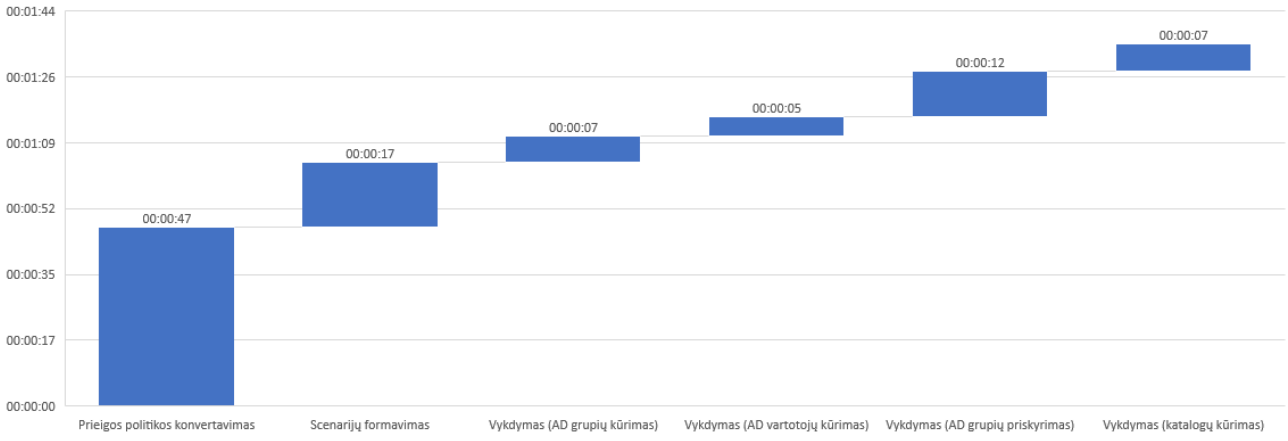
4.4.1. Prieigos politikos dokumento dydžio įtaka

Tyrimui prieigos valdymo politikos dokumente išplečiamas pareigybių sąrašas iki 50 vienetų, o informacijos šaltinių – iki 15 vienetų.

4.3 lentelė. Eksperimentui naudojamų duomenų palyginimas.

Duomenys	Eksperimentas nr. 1	Eksperimentas nr. 2	Skirtumas
Pareigybių kiekis, vnt.	19	57	200 %
Informacijos šaltinių kiekis, vnt.	8	16	100 %
Prieigos politikos dokumento dydis, baitais	6326	28311	348 %
Prieigos politikos dokumento eilučių skaičius, vnt.	240	1152	380 %
Darbuotojų įrašų kiekis faile, vnt.	28	28	0 %

Kelis kartus padidinus prieigos politikos dokumento turinį, didėja ir prototipui tenkanti skaičiavimo apkrova. Kiekvieno iš etapų atlikimo trukmės diagrama pateikiama žemiau.

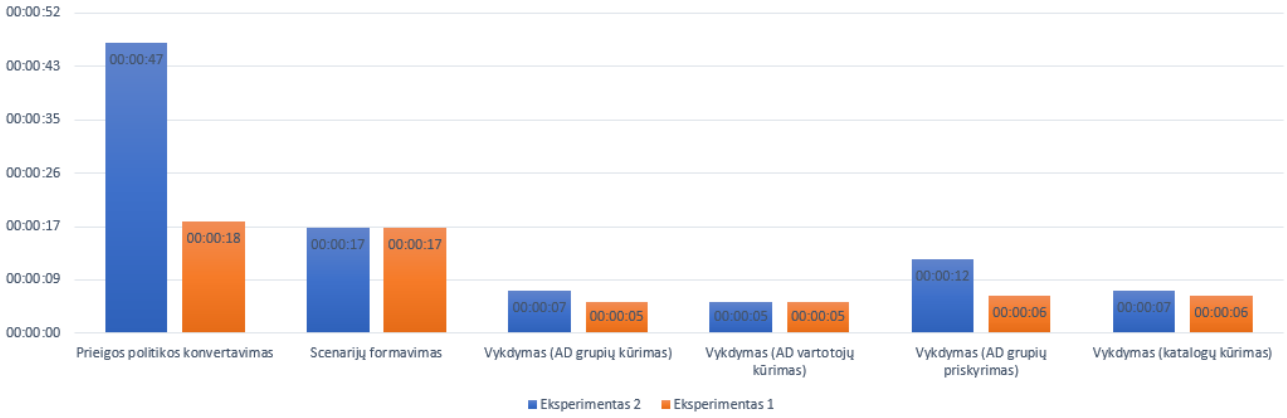


4.26 pav. Prototipo laiko sąnaudos prieigos politikos įgyvendinimui.

Bendra proceso trukmė sudarė 1 minutę ir 35 sekundes, kas yra tik 38 sekundėmis daugiau, nei pirmojo eksperimento metu.

4.4 lentelė. Eksperimento rezultatų palyginimas.

Etapai	Eksperimentas nr. 1	Eksperimentas nr. 2	Skirtumas
Prieigos politikos konvertavimas	00:00:18	00:00:47	161 %
Scenarijų formavimas	00:00:17	00:00:17	0 %
Vykdymas (AD grupių kūrimas)	00:00:05	00:00:07	40 %
Vykdymas (AD vartotojų kūrimas)	00:00:05	00:00:05	0 %
Vykdymas (AD grupių priskyrimas)	00:00:06	00:00:12	100 %
Vykdymas (katalogų kūrimas)	00:00:06	00:00:07	17 %
Bendra trukmė	**00:00:57**	**00:01:35**	**67 %**



4.27 pav. Rezultatų palyginimas.

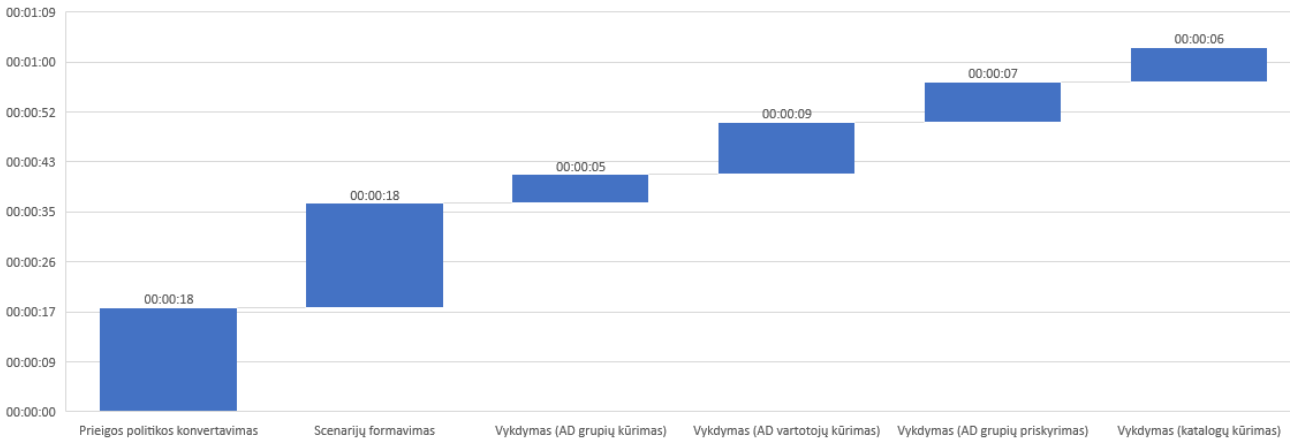
4.4.2. Darbuotojų duomenų failo įtaka

Šiam tyrimui darbuotojų duomenų failas išplečiamas nuo pirmajame eksperimente naudotų 28 įrašų iki 100 įrašų.

4.5 lentelė. Eksperimentui naudojamų duomenų palyginimas.

Duomenys	Eksperimentas nr. 1	Eksperimentas nr. 3	Skirtumas
Pareigybių kiekis, vnt.	19	19	0 %
Informacijos šaltinių kiekis, vnt.	8	8	0 %
Darbuotojų duomenų failo dydis, baitais	3663	12580	243 %
Darbuotojų įrašų kiekis faile, vnt.	28	100	257 %

Kiekvieno iš etapų atlikimo trukmės diagrama pateikiama žemiau.

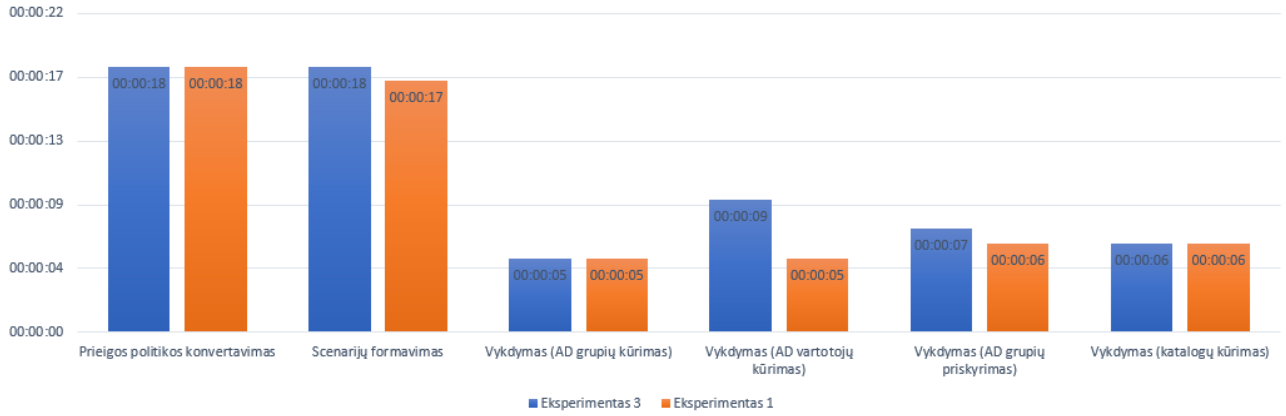


4.28 pav. Prototipo laiko sąnaudos prieigos politikos įgyvendinimui.

Bendra proceso trukmė sudarė 1 minutę ir 3 sekundes.

4.6 lentelė. Eksperimento rezultatų palyginimas.

Etapai	Eksperimentas nr. 1	Eksperimentas nr. 3	Skirtumas
Prieigos politikos konvertavimas	00:00:18	00:00:18	0 %
Scenarijų formavimas	00:00:17	00:00:18	6 %
Vykdymas (AD grupių kūrimas)	00:00:05	00:00:05	0 %
Vykdymas (AD vartotojų kūrimas)	00:00:05	00:00:09	80 %
Vykdymas (AD grupių priskyrimas)	00:00:06	00:00:07	17 %
Vykdymas (katalogų kūrimas)	00:00:06	00:00:06	0 %
Bendra trukmė	**00:00:57**	**00:01:03**	**11 %**



4.29 pav. Rezultatų palyginimas.

4.4.3. Apibendrinimas ir išvados

Atlikus šį tyrimą nustatyta, kad didžiausią įtaką prototipo spartai daro prieigos valdymo politikos dokumento kompleksiškumas. Kuo didesnis failas, tuo ilgiau užtrunka jo konvertavimas į xml formatą bei tam tikrų scenarijų vykdymas. Tačiau duomenų kiekio augimas ir proceso trukmės

pailgėjimas nėra susijęs tiesiogiai, nes iš eksperimento rezultatų matyti, kad padidinus duomenų failą net keturis kartus, jo apdorojimas pailgėja tik pusantro karto. Tokį poveikį sudaro proceso metu operacinės sistemos vykdomas resursų perskirstymas – programai suteikiama didesni skaičiavimo pajėgumai.

Dar mažesnę įtaką prototipo darbo našumui daro darbuotojų duomenų failo augimas. Įrašų skaičių jame padidinus beveik keturis kartus, bendra proceso trukmė pailgėjo tik 11 %. Tad galima daryti išvadą, kad prototipas gali būti panaudotas ir itin didelėms organizacijoms.

IŠVADOS

Šio projekto metu susipažinta su informacijos saugos politikos sudedamosiomis dalimis, jos projektavimu, derinimu ir įgyvendinimu. Taip pat gilintasi į prieigos valdymo saugos politikos ypatumus, egzistuojančius prieigos valdymo modelius, vyraujančias tendencijas ir iššūkius įgyvendinant. Taip pat pasiūlytas metodas daliai šių iššūkių spręsti procesą automatizuojant. Galiausiai, sukurtas prototipas.

Galima padaryti tokias išvadas:

1. Informacijos saugos politika yra neatsiejama sėkmingos ir sauga besirūpinančios organizacijos dalis. Įmonės, kuriose įgyvendinta informacijos saugos politika, visada bus pranašesnės kovoje su kibernetinėmis grėsmėmis, nei tos, kurios investuoja tik į technologinius sprendimus.
2. Informacijos saugos politika turi savo gyvavimo ciklą, tad reguliariai turi būti peržiūrima, tobulinama ir atnaujinama.
3. Viena svarbiausių visos saugumo politikos dalių yra prieigos valdymo politika, kuri įgyvendinama, siekiant apsaugoti kritinę infrastruktūrą ir informaciją nuo neautorizuoto atskleidimo ar modifikavimo - leidimai suteikiami tik toms sistemoms ar vartotojams, kurie yra autorizuoti pasiekti atitinkamus resursus.
4. Prieigos valdymo saugos politikos įgyvendinimo automatizavimas yra būtinas, norint, kad kuo daugiau organizacijų tinkamai valdytų prieigą prie savo informacinių šaltinių;
5. Prieigos valdymo saugos politikos dokumento formalizavimas į programoms suprantamą formatą yra svarbus žingsnis siekiant proceso automatizavimo;
6. Automatizavimas ženkliai sumažina politikos įgyvendinimo laiko sąnaudas, o tai reiškia, ir taupo finansus.

LITERATŪROS SĄRAŠAS

[1] „The CIA Triad - Assurance on Information Security,“ 2013. [Tinkle]. Available: https://www.slideshare.net/bharathraob/the-cia-triad-28739772?next_slideshow=1. [Kreiptasi 11 12 2017].

[2] M. Rhodes-Ousley, Information Security: Second Edition, JAV, 2013.

[3] „2017 Data Breach Investigation Report,“ 2017. [Tinkle]. Available: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/. [Kreiptasi 28 Gruodžio 2017].

[4] T. R. Peltier, Information security fundamentals: Second edition, JAV: CRC Press, 2014.

[5] T. R. Peltier, Information security policies and procedures: A Practitioner's Reference, JAV: CRC Press, 2004.

[6] K. J. Knapp, R. F. Morris, T. E. Marshall, T. A. Byrd, „Information security policy: An organizational-level,“ Elsevier, 2009.

[7] J. Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, JAV, 2013.

[8] „Cengage Learning, Introduction to Information Security,“ 2008. [Tinkle]. Available: https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf. [Kreiptasi 11 12 2017].

[9] T. Čepas, „Prieigos kontrolė ir jos vaidmuo sistemos saugumui užtikrinti,“ įtraukta *Mokslas – Lietuvos ateitis*, Vilnius, 2011.

[10] J.M. Stewart, E. Tittel, M. Chapple, Certified Information Systems Security Professional Study Guide: Fourth Edition, JAV: Wiley Publishing, 2008.

[11] A. Venčkauskas, E. Kazanavičius, Informacinių technologijų saugos metodai, Kaunas: TEV, 2011.

[12] D. Holme, Windows Administration. Productivity solutions for IT professionals., Washington: Microsoft Press, 2008.

[13] „Organizacijos struktūra,“ [Tinkle]. Available: http://www.mokslas.net/vadyba/organizacijos-struktura/. [Kreiptasi 26 gegužės 2018].

[14] G. Skersys, „Informacijos sauga,“ TEV, Kaunas, 2011.

[15] „CISSP Certification All-in-One Exam Guide,“ [Tinkle]. Available: http://media.techtarget.com/searchSecurity/downloads/29667C05.pdf. [Kreiptasi 02 Sausio 2018].

[16] „CISSP Exam Cram: Security Architecture and Models,“ 29 Lapkričio 2012. [Tinkle]. Available:

http://www.pearsonitcertification.com/articles/article.aspx?p=1998558&seqNum=4. [Kreiptasi 02 Sausio 2018].

[17] „Autentification & identification - Tinklu Saugumas,“ 29 Balandžio 2013. [Tinkle]. Available: http://www.tinklusaugumas.lt/Autentification%20%26%20identification. [Kreiptasi 2 Sausio 2018].

[18] „What ANSI RBAC is,“ [Tinkle]. Available: http://directory.apache.org/fortress/user-guide/1.3-what-rbac-is.html. [Kreiptasi 2 Sausio 2018].

[19] H. C. A. v. Tilborg, Encyclopedia of Cryptography and Security, USA: Springer, 2011.

[20] „Microsoft Azure,“ 19 kovo 2020. [Tinkle]. Available: https://docs.microsoft.com/en-us/azure/role-based-access-control/overview. [Kreiptasi 3 balandžio 2020].

[21] W3C, „Extensible Markup Language (XML) 1.0 (Fifth Edition),“ 2008.

PRIEDAI

1 priedas. Prieigos politikos dokumentas

Prieigos politikos dokumentas

2018.01.01

UAB "Įmonė" vadovybė, siekdama išsaugoti konkurencinį pranašumą, pelningumą, pinigų cirkuliaciją, teisinius ir sutartinius įsipareigojimus, bei įvaizdį, įsipareigoja užtikrinti organizacijos informacinių vertybių konfidencialumą, vientisumą ir prieinamumą. Reikalavimai informacijai ir jos apsaugai turi atitikti organizacijos veiklos tikslus. Informacijos saugumo valdymo sistema skirta užtikrinti informacijos sklaidą, apdorojimą, saugojimą, sumažinant informacijos saugumo rizikas iki priimtino lygio.

Viena iš saugą užtikrinančių priemonių yra prieigos prie informacijos resursų kontrolė ir valdymas. Šis formalus prieigos politikos įgyvendinimo dokumentas griežtai apibrėžia, kokias prieigos teises pagal priskirtas roles kiekvienas darbuotojas įgyja. Dokumentas yra reguliariai peržiūrimas ir redaguojamas už saugumą atsakingo asmens.

UAB "Įmonė"

Departamentas: Administracija
Pareigos: Generalinis direktorius
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Skaityti;
TEISE - Skaityti;
FINANSAI - Skaityti;
IT - Skaityti;
SC - Skaityti;
TECHNIKA - Skaityti;
MARKETINGAS - Skaityti;

Departamentas: Prekybos skyrius
Pareigos: Prekybos direktorius
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Skaityti/Rašyti;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: Prekybos skyrius
Pareigos: Regiono direktorius
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Skaityti;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: Prekybos skyrius
Pareigos: Prekybos atstovas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Skaityti;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: Teisės skyrius
Pareigos: Teisininkas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Skaityti;
TEISE - Skaityti/Rašyti;
FINANSAI - Skaityti;
IT - Skaityti;
SC - Skaityti;
TECHNIKA - Skaityti;
MARKETINGAS - Skaityti;

Departamentas: Teisės skyrius
Pareigos: Teisininko padėjėjas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Skaityti/Rašyti;

FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: Finansų skyrius
Pareigos: Vyr. finansininkas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Skaityti/Rašyti;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: Finansų skyrius
Pareigos: Finansininkas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Skaityti/Rašyti;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: IT skyrius
Pareigos: IT direktorius
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Skaityti/Rašyti;
TEISE - Skaityti/Rašyti;
FINANSAI - Skaityti/Rašyti;
IT - Skaityti/Rašyti;
SC - Skaityti/Rašyti;
TECHNIKA - Skaityti/Rašyti;
MARKETINGAS - Skaityti/Rašyti;

Departamentas: IT skyrius

Pareigos: IT projektų vadovas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Skaityti;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: IT skyrius
Pareigos: IT specialistas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Skaityti;
TEISE - Skaityti;
FINANSAI - Skaityti;
IT - Skaityti/Rašyti;
SC - Skaityti;
TECHNIKA - Skaityti;
MARKETINGAS - Skaityti;

Departamentas: IT skyrius
Pareigos: DB administratorius
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Skaityti;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: Klientų aptarnavimo skyrius
Pareigos: Klientu aptarnavimo vadovas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;

SC - Skaityti/Rašyti;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: Klientų aptarnavimo skyrius
Pareigos: Klientu aptarnavimo specialistas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Skaityti/Rašyti;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Nepasiekiama;

Departamentas: Technikos skyrius
Pareigos: Technikos direktorius
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Skaityti/Rašyti;
MARKETINGAS - Nepasiekiama;

Departamentas: Technikos skyrius
Pareigos: Inžinierius
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Skaityti/Rašyti;
MARKETINGAS - Nepasiekiama;

Departamentas: Marketingo skyrius
Pareigos: Marketingo vadovas
Prieiga:

BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Skaityti/Rašyti;

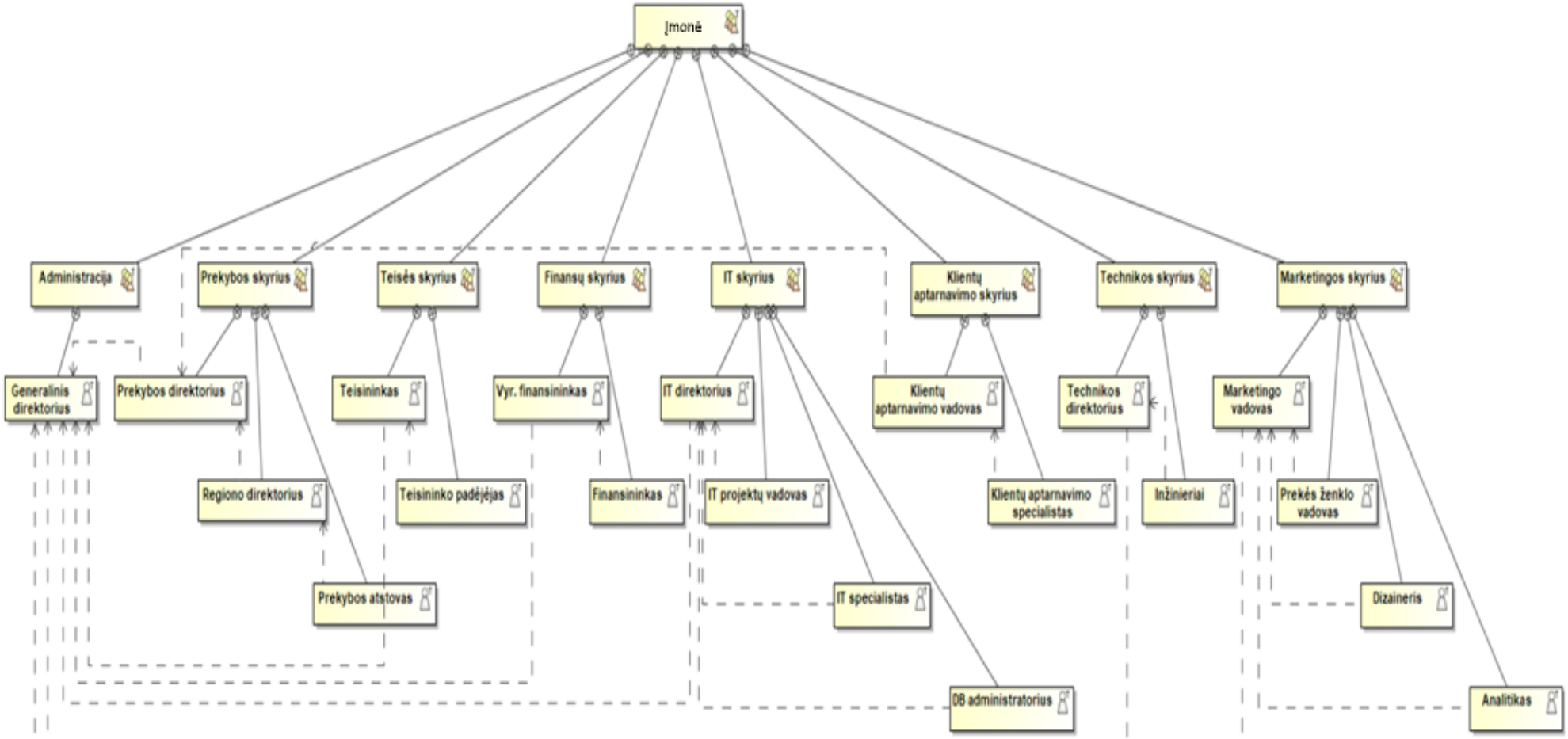
Departamentas: Marketingo skyrius
Pareigos: Dizaineris
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Skaityti/Rašyti;

Departamentas: Marketingo skyrius
Pareigos: Analitikas
Prieiga:
BENDRAS - Skaityti/Rašyti;
PREKYBA - Nepasiekiama;
TEISE - Nepasiekiama;
FINANSAI - Nepasiekiama;
IT - Nepasiekiama;
SC - Nepasiekiama;
TECHNIKA - Nepasiekiama;
MARKETINGAS - Skaityti/Rašyti;

IT direktorius yra šio dokumento valdytojas ir yra atsakingas už jo peržiūrą, pagal ISVS peržiūros reikalavimus.

Šį dokumentą elektroniniu būdu tvirtina organizacijos vadovas.

2 priedas. Įmonės organizacinė struktūra.



3 priedas. Prieigos saugos politikos formalizuotas dokumentas.

```
<?xml version="1.0"?>
<Imone>
 <Katalogas pav="BENDRAS">
  <Pareigos pav="Generalinis direktorius">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="Prekybos direktorius">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="Regiono direktorius">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="Prekybos atstovas">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="Teisininkas">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="Teisininko padėjėjas">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="Vyr. finansininkas">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="Finansininkas">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="IT direktorius">
   <SMBShare>ChangeAccess</SMBShare>
   <Teises>Modify</Teises>
   <Leidimas>allow</Leidimas>
   <Veiksmas>Add</Veiksmas>
  </Pareigos>
  <Pareigos pav="IT projektų vadovas">
```

```
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="IT specialistas">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="DB administratorius">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Klientu aptarnavimo vadovas">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Klientu aptarnavimo specialistas">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Technikos direktorius">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Inžinierius">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Marketingo vadovas">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Dizaineris">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Analitikas">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
  </Katalogas>
  <Katalogas pav="PREKYBA">
```

```
<Pareigos pav="Generalinis direktorius">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Prekybos direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Regiono direktorius">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Prekybos atstovas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininkas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininko padėjėjas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Vyr. finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT projektų vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT specialistas">
```

```
  <SMBShare>ReadAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>allow</Leidimas>
  <Veiksmas>Add</Veiksmas>
 </Pareigos>
 <Pareigos pav="DB administratorius">
  <SMBShare>NoAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>deny</Leidimas>
  <Veiksmas>Block</Veiksmas>
 </Pareigos>
 <Pareigos pav="Klientu aptarnavimo vadovas">
  <SMBShare>NoAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>deny</Leidimas>
  <Veiksmas>Block</Veiksmas>
 </Pareigos>
 <Pareigos pav="Klientu aptarnavimo specialistas">
  <SMBShare>NoAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>deny</Leidimas>
  <Veiksmas>Block</Veiksmas>
 </Pareigos>
 <Pareigos pav="Technikos direktorius">
  <SMBShare>NoAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>deny</Leidimas>
  <Veiksmas>Block</Veiksmas>
 </Pareigos>
 <Pareigos pav="Inžinierius">
  <SMBShare>NoAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>deny</Leidimas>
  <Veiksmas>Block</Veiksmas>
 </Pareigos>
 <Pareigos pav="Marketingo vadovas">
  <SMBShare>NoAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>deny</Leidimas>
  <Veiksmas>Block</Veiksmas>
 </Pareigos>
 <Pareigos pav="Dizaineris">
  <SMBShare>NoAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>deny</Leidimas>
  <Veiksmas>Block</Veiksmas>
 </Pareigos>
 <Pareigos pav="Analitikas">
  <SMBShare>NoAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>deny</Leidimas>
  <Veiksmas>Block</Veiksmas>
 </Pareigos>
</Katalogas>
<Katalogas pav="TEISE">
 <Pareigos pav="Generalinis direktorius">
  <SMBShare>ReadAccess</SMBShare>
  <Teises>Read</Teises>
  <Leidimas>allow</Leidimas>
  <Veiksmas>Add</Veiksmas>
 </Pareigos>
```

```
<Pareigos pav="Prekybos direktorius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Regiono direktorius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Prekybos atstovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininkas">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininko padėjėjas">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Vyr. finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT projektų vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT specialistas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="DB administratorius">
```

```
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Klientu aptarnavimo vadovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Klientu aptarnavimo specialistas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Technikos direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Inžinierius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Marketingo vadovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Dizaineris">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Analitikas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
  </Katalogas>
  <Katalogas pav="FINANSAI">
   <Pareigos pav="Generalinis direktorius">
    <SMBShare>ReadAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Prekybos direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
```

```
<Pareigos pav="Regiono direktorius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Prekybos atstovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininkas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininko padėjėjas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Vyr. finansininkas">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Finansininkas">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT projektų vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT specialistas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="DB administratorius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo vadovas">
```

```
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Klientu aptarnavimo specialistas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Technikos direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Inžinierius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Marketingo vadovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Dizaineris">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Analitikas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
  </Katalogas>
  <Katalogas pav="IT">
   <Pareigos pav="Generalinis direktorius">
    <SMBShare>ReadAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Prekybos direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Regiono direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
```

```
<Pareigos pav="Prekybos atstovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininkas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininko padėjėjas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Vyr. finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT projektų vadovas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT specialistas">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="DB administratorius">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo specialistas">
```

```
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Technikos direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Inžinierius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Marketingo vadovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Dizaineris">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Analitikas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
  </Katalogas>
  <Katalogas pav="SC">
   <Pareigos pav="Generalinis direktorius">
    <SMBShare>ReadAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Prekybos direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Regiono direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Prekybos atstovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
```

```
<Pareigos pav="Teisininkas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Teisininko padėjėjas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Vyr. finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT projektų vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT specialistas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="DB administratorius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo vadovas">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo specialistas">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Technikos direktorius">
```

```
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Inžinierius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Marketingo vadovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Dizaineris">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Analitikas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
  </Katalogas>
  <Katalogas pav="TECHNIKA">
   <Pareigos pav="Generalinis direktorius">
    <SMBShare>ReadAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Prekybos direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Regiono direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Prekybos atstovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Teisininkas">
    <SMBShare>ReadAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
```

```
<Pareigos pav="Teisininko padėjėjas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Vyr. finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT projektų vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT specialistas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="DB administratorius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo specialistas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Technikos direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="Inžinierius">
```

```
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Marketingo vadovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Dizaineris">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Analitikas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
  </Katalogas>
  <Katalogas pav="MARKETINGAS">
   <Pareigos pav="Generalinis direktorius">
    <SMBShare>ReadAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Prekybos direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Regiono direktorius">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Prekybos atstovas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
   <Pareigos pav="Teisininkas">
    <SMBShare>ReadAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Teisininko padėjėjas">
    <SMBShare>NoAccess</SMBShare>
    <Teises>Read</Teises>
    <Leidimas>deny</Leidimas>
    <Veiksmas>Block</Veiksmas>
   </Pareigos>
```

```
<Pareigos pav="Vyr. finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Finansininkas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT direktorius">
 <SMBShare>ChangeAccess</SMBShare>
 <Teises>Modify</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="IT projektų vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="IT specialistas">
 <SMBShare>ReadAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>allow</Leidimas>
 <Veiksmas>Add</Veiksmas>
</Pareigos>
<Pareigos pav="DB administratorius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo vadovas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Klientu aptarnavimo specialistas">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Technikos direktorius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Inžinierius">
 <SMBShare>NoAccess</SMBShare>
 <Teises>Read</Teises>
 <Leidimas>deny</Leidimas>
 <Veiksmas>Block</Veiksmas>
</Pareigos>
<Pareigos pav="Marketingo vadovas">
```

```
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Dizaineris">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
   <Pareigos pav="Analitikas">
    <SMBShare>ChangeAccess</SMBShare>
    <Teises>Modify</Teises>
    <Leidimas>allow</Leidimas>
    <Veiksmas>Add</Veiksmas>
   </Pareigos>
  </Katalogas>
</Imone>
```